Nebraska Administrative Services

RFP 5252 Z1

Independent Verification and Validation Services

May 18, 2016

TECHNICAL PROPOSAL

First Data®

5565 Glenridge Connector NE, Suite 1600
Atlanta, GA 30342
www.firstdata.com

May 16, 2016

First Data.

Jennifer Crouse/Robert Thompson
State Purchasing Bureau
1526 K Street, Suite 130
Lincoln, NE 68508

Subject: First Data's proposal in response to RFP #5252 Z1: Independent Verification and Validation (IV&V) Services

Dear Ms. Crouse and Mr. Thompson,

First Data Government Solution, LP is pleased to submit our proposal in response to the RFP #5252 Z1 to provide Independent Verification and Validation (IV&V) Services. We are confident that the State's evaluators will find our proposal fully compliant with the requirements outlined in the RFP. Further, we believe the Department will find that First Data Government Solutions, LP has submitted a proposal that represents the best solution for the IV&V services required by the State.

The State of Nebraska has undertaken the EES and DMA projects to support its vision of an interoperable solution that meets the needs of the State's HHS agencies both for now and the foreseeable future. Nebraska has demonstrated its understanding and recognition of the important role an IV&V Contractor can play in helping the State to identify and mitigate risks and issues. It is clear that the objective of these IV&V services is for Nebraska to benefit from independent and objective project oversight. These services must be provided by a firm that has a proven ability to deliver professional IV&V services, with uncompromising integrity and independence. **First Data is that partner**.

First Data offers an unmatched combination of experience and capability, including a proven IV&V methodology based on industry standards; a thorough understanding of integrated eligibility systems and supporting technologies, and unparalleled health and human services program experience.

First Data Has the Keys to Successful Projects

For more than 30 years, First Data has provided services to our government clients. We understand that successful project outcomes do not occur by chance. Rather, they are born of four keys to success:

- ***An Understanding of the Project's Goals and Objectives*** - with a clear understanding of the expected results.
- ***A Defined Project Plan*** - one that focuses and guides all project activities toward the achievement of the desired outcomes.

- ***The Right People*** - who bring the requisite expertise, knowledge, and experience.

- ***An Experienced Firm*** - one that is financially sound, with a history of successfully providing similar services.

First Data Understands the Project's Goals and Objectives

We know that your plan is to manage multiple initiatives as a portfolio of projects with staged implementation and are pleased to hear that this process will be managed by a single governance structure. Successfully achieving the DHHS and Division of Medicaid and Long Term Care (MLTC)'s long-term operational vision and objectives requires a partner with expertise, experience, and insight into current IV&V and quality assurance practices, coupled with a broad understanding of healthcare and human services program delivery. Nebraska also benefits from a partner that understands the State's complex technological and business environments and how it must integrate with various Medicaid stakeholders as well as internal state resources. **First Data is that partner**.

First Data will help identify and address issues and risks as early as possible throughout the project from initiation through certification. We fully understand what Nebraska is striving to achieve, and we recognize how critical this project is to the citizens you serve.

First Data Has a Proven Approach Tailored to the Portfolio of DHHS Projects

Our approach to IV&V services is founded upon the importance of following a consistent and disciplined approach emphasizing independence; objectivity; and the use of a methodology that is proven, rigorous, and based on industry standards. This approach provides First Data with the credibility to effectively evaluate and assess the implementation vendors' project management teams, as well as project plans, processes, procedures, controls, and the resulting outcomes/products. This disciplined approach is applied to all phases of the System Development Life Cycle (SDLC).

We recognize the critical importance of IV&V services. The complexity of the portfolio of projects is magnified by the number of work products to be reviewed; the velocity of day-to- day decisions on the project and certifications to be conducted. By utilizing our proven IV&V methodology we will help the State overcome these challenges by:

- ***Focusing on high-value, high-risk areas of the project:*** IV&V reviews require discipline and focused attention. Because of the size and complexity of the project, it may be easy to overlook the root causes of project risks and become distracted by the symptoms of the risks. Our approach emphasizes gaining an understanding of the true elements of risk to the project and providing meaningful analysis that the State and implementation vendors can use to guide the project and take corrective action as needed.

- ***Utilizing Proven Pre-Defined Checklists:*** Our approach includes tailored checklists, already in use in Nebraska to verify and validate project activities. The First Data checklists were developed using industry standards and have been refined over many years and numerous engagements, incorporating lessons learned. The checklists assist us in

performing assessments of project processes and products, and will be tailored to meet the specific needs of this project.

- ***Leveraging Recent IV&V Experience:*** First Data has proven experience in providing similar IV&V services to numerous other implementation projects across the country, as detailed in Section 2.8: Summary of Corporate Experience. As a result of these engagements, the First Data Team has an unmatched understanding of the risks, issues, and mitigation strategies associated with complex implementations in health and human services agencies.

- ***Deep understanding of the business:*** Projects such as the EES and DMA projects are more than just modernization efforts. They profoundly affect the business processes, policy, procedures, and operations of the delivery of critical services to citizens. Our consultants have deep and personal experience in operating many of these programs and truly understand the associated issues and challenges.

- ***Incorporating a 360-degree risk analysis perspective:*** The risks that will arise during the portfolio of DHHS projects will come from many sources. Our IV&V activities will be heavily focused on deliverables, work products, processes, procedures, and methodologies. At the same time our risk analysis will take into account a variety of perspectives including project risks stemming from the State, its divisions and program areas, and other stakeholders.

First Data Has the Experienced Project Team to Deliver "Day 1" Value

First Data is proposing a team of IV&V professionals who collectively address the specialized skills your project requires. Our team is led by Project Management Institute (PMI)-certified Project Managers supported by highly-skilled Cúram, Medicaid, Technical, ACA and Eligibility Certification Subject Matter Expert (SME) advisors, complemented with a pool of professional technical and business SMEs. The First Data IV&V Project Team represents a powerful lineup committed to providing a cost-effective IV&V solution for Nebraska. Our staff credentials are detailed in Section 3.2: Organizational Staffing. Specifically, First Data offers:

- Consultants with extensive experience and knowledge with all of the health and human services programs included within the scope of the portfolio of projects outlined in the RFP.

- A team that includes consultants currently performing IV&V services for similar projects across the United States, including other large-scale integrated eligibility implementation efforts.

- Proactive risk analysis methods developed through our long history of IV&V consulting engagements.

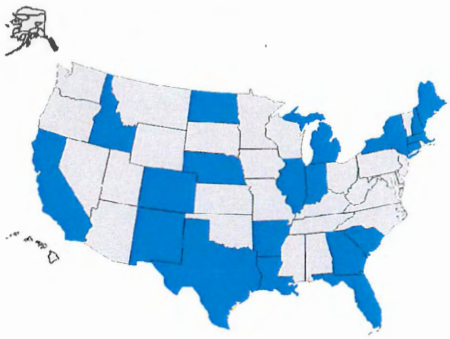
- Hands-on technical expertise with the technology listed in this RFP, including Cúram.

- A staffing approach that provides for expertise, continuity of resources, and the ability to efficiently add to our Team's capacity at key points in the project.

- A team of whom 100% of EES proposed staff has worked with you on the EES project and will mitigate any risks associated with selecting another vendor. Nebraska will not have to spend any resources on knowledge transfer or schedule slippage by selecting First Data to continue to provide IV&V services for EES, DMA and optional projects

First Data offers Outstanding Qualifications as an IV&V Vendor

First Data is a nationally recognized leader in health and human services systems IV&V consulting. We have been providing these services for our state partners' complex, statewide automation projects for the past 30 years. We bring a national perspective having provided these services on one or more, large, complex, statewide systems in multiple states. This significant level of real experience will provide IV&V services that meet the State's requirements and expectations.



Our methodology for performing IV&V on system implementations has been successful at all levels of government across multiple service areas. We have learned that most successful projects are a result of strong partnerships with our State clients. To develop cohesive working relationships, we provide our clients with quality service and outstanding personnel.

The First Data Value Proposition

Our proposal offers the State a unique combination of hands-on and Nebraska-specific experience, robust IV&V methods and tools and a deep understanding of health and human services programs. Nebraska is clearly making a significant investment in both time and resources with this portfolio of projects. The IV&V vendor must also be viewed as an investment in the success of this effort. Based on our extensive relevant experience, we offer the best value and lowest risk to support the ongoing EES effort and the upcoming DMA project. Our knowledge of State operations and our commitment to excellence in delivery will allow DHHS to achieve its vision.

First Data welcomes the opportunity to discuss our proposal should there be any questions that may arise. If you have any questions, please do not hesitate to contact Mr. Keith Schraad at 913-709-2262 or via email at keith.schraad@firstdata.com.

Regards,

Jacie Engle
Vice President

By signing this Request for Proposal for Contractual Services form, the bidder guarantees compliance with the provision stated in this Request for Proposal, agrees to the terms and conditions unless otherwise agreed to (see Section III) and certifies that bidder maintains a drug free work place environment.

Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat 73-603 DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Contractors. This information is for statistical purposes only and will not be considered for contract award purposes.

_X_ **NEBRASKA CONTRACTOR AFFIDAVIT**: Bidder hereby attests that bidder is a Nebraska Contractor. "Nebraska Contractor" shall mean any bidder who has maintained a bona fide place of business and at least one employee within this state for at least the six (6) months immediately preceding the posting of this RFP.

____ I hereby certify that I am a **Resident disabled veteran or business located in a designated enterprise zone** in accordance with Neb. Rev Stat 73-107 and wish to have preference, if applicable, considered in the award of this contract.

FIRM: First Data Government Solutions, LP

COMPLETE ADDRESS: 5565 Glenridge Connector NE Atlanta, Georgia 30342

TELEPHONE NUMBER: 404-890-2462 FAX NUMBER: 402-315-5105

SIGNATURE: Jacie Engle DATE: May 16, 2016

TYPED NAME AND TITLE OF SIGNER: Jacie Engle, Vice President

1.0 Request for Proposal Form

Preparation of Response Contact Information	
Bidder Name:	First Data Government Solutions, LP
Bidder Address:	5565 Glenridge Connector NE Atlanta, Georgia 30342
Contact Person and Title:	Keith Schraad, Sales Director
Email Address:	Keith.schraad@firstdata.com
Telephone Number (office):	913-709-2262
Telephone Number (cellular):	913-709-2262
Fax Number:	402-315-5105

Communication with the State Contact Information	
Bidder Name:	First Data Government Solutions, LP
Bidder Address:	5565 Glenridge Connector NE Atlanta, Georgia 30342
Contact Person and Title:	Keith Schraad, Sales Director
Email Address:	Keith.schraad@firstdata.com
Telephone Number (office):	913-709-2262
Telephone Number (cellular):	913-709-2262
Fax Number:	402-315-5105

TERMS AND CONDITIONS

By signing the "Request for Proposal for Contractual Services" form, the bidder guarantees compliance with the provisions stated in this Request for Proposal, agrees to the Terms and Conditions unless otherwise agreed to, and certifies bidder maintains a drug free work place environment.

Bidders are expected to closely read the Terms and Conditions and provide a binding signature of intent to comply with the Terms and Conditions; provided, however, a bidder may indicate any exceptions to the Terms and Conditions by (1) clearly identifying the term or condition by subsection, and (2) including an explanation for the bidder's inability to comply with such term or condition which includes a statement recommending terms and conditions the bidder would find acceptable. Rejection in whole or in part of the Terms and Conditions may be cause for rejection of a bidder's proposal. **Bidders must include completed Section III with their proposal response.**

The State of Nebraska is soliciting bids in response to the RFP. The State of Nebraska will not consider proposals that propose the substitution of the bidder's contract, agreements, or terms for those of the State of Nebraska's. Any License, Service Agreement, Customer Agreement, User Agreement, Bidder Terms and Conditions, Document, or Clause purported or offered to be included as a part of this RFP must be submitted as individual clauses, as either a counter-offer or additional language, and each clause must be acknowledged and accepted in writing by the State. If the Bidder's clause is later found to be in conflict with the RFP or resulting contract the Bidder's clause shall be subordinate to the RFP or resulting contract, unless the State has agreed in writing to incorporate the Bidder's clause into the resulting contract."

A. GENERAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
JC			

The contract resulting from this Request for Proposal shall incorporate the following documents:

1. Amendment to Contract Award with the most recent dated amendment having the highest priority;
2. Contract Award and any attached Addenda;
3. The Request for Proposal form and the Contractor's Proposal, signed in ink
4. Amendments to RFP and any Questions and Answers; and
5. The original RFP document and any Addenda.

These documents constitute the entirety of the contract.

Unless otherwise specifically stated in a contract amendment, in case of any conflict between the incorporated documents, the documents shall govern in the following order of preference with number one (1) receiving preference over all other documents and with each lower numbered document having preference over any higher numbered document: 1) Amendment to Contract Award with the most recent dated amendment having the highest priority, 2) Contract Award and any attached Addenda, 3) the signed Request for Proposal form and the Contractor's Proposal, 4) Amendments to RFP and any Questions and Answers, 5) the original RFP document and any Addenda.

Any ambiguity in any provision of this contract which shall be discovered after its execution shall be resolved in accordance with the rules of contract interpretation as established in the State of Nebraska.

Once proposals are opened they become the property of the State of Nebraska and will not be returned.

B. AWARD

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

All purchases, leases, or contracts which are based on competitive proposals will be awarded according to the provisions in the Request for Proposal. The State reserves the right to reject any or all proposals, in whole or in part, or to award to multiple bidders in whole or in part, and at its discretion, may withdraw or amend the Request for Proposal at any time. The State reserves the right to waive any deviations or errors that are not material, do not invalidate the legitimacy of the proposal, and do not improve the bidder's competitive position. All awards will be made in a manner deemed in the best interest of the State. The Request for Proposal does not commit the State to award a contract. If, in the opinion of the State, revisions or amendments will require substantive changes in proposals, the due date may be extended.

By submitting a proposal in response to this Request for Proposal, the bidder grants to the State the right to contact or arrange a visit in person with any or all of the bidder's clients.

Once intent to award decision has been determined, it will be posted to the Internet at:
http://das.nebraska.gov/materiel/purchasing.html

Grievance and protest procedure is available on the Internet at:
http://das.nebraska.gov/materiel/purchase_bureau/docs/vendors/protest/ProtestGrievanceProcedureForVendors.pdf

Any protests must be filed by a vendor within ten (10) business days after the intent to award decision is posted to the Internet.

C. COMPLIANCE WITH CIVIL RIGHTS LAWS AND EQUAL OPPORTUNITY EMPLOYMENT / NONDISCRIMINATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The Contractor shall comply with all applicable local, state, and federal statutes and regulations regarding civil rights laws and equal opportunity employment. The Nebraska Fair Employment Practice Act prohibits Contractors of the State of Nebraska, and their Subcontractors, from discriminating against any employee or applicant for employment, with respect to hire, tenure, terms, conditions, compensation, or privileges of employment because of race, color, religion, sex, disability, marital status, or national origin (Neb. Rev. Stat. §§ 48-1101 to 48-1125). The Contractor guarantees compliance with the Nebraska Fair Employment Practice Act, and breach of this provision shall be regarded as a material breach of contract. The Contractor shall insert a similar provision in all Subcontracts for services to be covered by any contract resulting from this Request for Proposal.

D. PERMITS, REGULATIONS, LAWS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
JE			

The Contractor shall procure and pay for all permits, licenses, and approvals necessary for the execution of the contract. The Contractor shall comply with all applicable local, state, and federal laws, ordinances, rules, orders, and regulations.

E. OWNERSHIP OF INFORMATION AND DATA

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response	NOTES/COMMENTS:
		JE	First Data requests an exception to provide that these rights and obligations are for deliverables provided under the contract. We request the addition of language protecting our rights to our intellectual property. We can agree to indemnify the State from claims for royalties and costs, which should make the guarantee unnecessary.

~~The State of Nebraska shall have the unlimited right to publish, duplicate, use, and disclose all information and data developed or derived by the Contractor pursuant to this contract.~~

~~The Contractor must guarantee that it has the full legal right to the materials, supplies, equipment, and other rights or titles (e.g. rights to licenses transfer or assign deliverables) necessary to execute this contract. The contract price shall, without exception, include compensation for all royalties and costs arising from patents, trademarks, and copyrights that are in any way involved in the contract. It shall be the responsibility of the Contractor to pay for all royalties and costs, and the State must be held harmless from any such claims.~~

The State of Nebraska shall have the unlimited right to publish, duplicate, use, and disclose all information and data developed or derived by the Contractor in the performance of this contract (the "Deliverables"). All of Contractor's pre-existing intellectual property, templates, methodologies and processes or intellectual property, methodologies and processes developed independently of this contract are and shall remain the sole and exclusive property of Contractor.

The Contractor agrees that it has the full legal right to license, transfer or assign the Deliverables. The contract price shall, without exception, include compensation for all royalties and costs arising from patents, trademarks, and copyrights to the Deliverables. It shall be the responsibility of the Contractor to pay for all royalties and costs for the Deliverables, and the State must be held harmless from any such claims.

F. INSURANCE REQUIREMENTS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
JE			

The Contractor shall not commence work under this contract until all the insurance required hereunder has been obtained and such insurance has been approved by the State. The Contractor shall maintain all required insurance for the life of this contract and shall ensure that the State Purchasing Bureau has the most current certificate of insurance throughout the life of this contract. If Contractor will be utilizing any Subcontractors, the Contractor is responsible for obtaining the certificate(s) of insurance required herein under from any and all Subcontractor(s). The Contractor is also responsible for ensuring Subcontractor(s) maintain the insurance required until completion of the contract requirements. The Contractor shall not allow any Subcontractor to commence work on any Subcontract until all similar insurance required of the Subcontractor has been obtained and approved by the Contractor. Approval of the insurance by the State shall not limit, relieve, or decrease the liability of the Contractor hereunder.

If by the terms of any insurance a mandatory deductible is required, or if the Contractor elects to increase the mandatory deductible amount, the Contractor shall be responsible for payment of the amount of the deductible in the event of a paid claim.

Insurance coverages shall function independent of all other clauses in the contract, and in no instance shall the limits of recovery from the insurance be reduced below the limits required by this section.

1. WORKERS' COMPENSATION INSURANCE

The Contractor shall take out and maintain during the life of this contract the statutory Workers' Compensation and Employer's Liability Insurance for all of the contactors' employees to be engaged in work on the project under this contract and, in case any such work is sublet, the Contractor shall require the Subcontractor similarly to provide Worker's Compensation and Employer's Liability Insurance for all of the Subcontractor's employees to be engaged in such work. This policy shall be written to meet the statutory requirements for the state in which the work is to be performed, including Occupational Disease. This policy shall include a waiver of subrogation in favor of the State. The amounts of such insurance shall not be less than the limits stated hereinafter.

2. COMMERCIAL GENERAL LIABILITY INSURANCE AND COMMERCIAL AUTOMOBILE LIABILITY INSURANCE

The Contractor shall take out and maintain during the life of this contract such Commercial General Liability Insurance and Commercial Automobile Liability Insurance as shall protect Contractor and any Subcontractor performing work covered by this contract from claims for damages for bodily injury, including death, as well as from claims for property damage, which may arise from operations under this contract, whether such operation be by the Contractor or by any Subcontractor or by anyone directly or indirectly employed by either of them, and the amounts of such insurance shall not be less than limits stated hereinafter.

The Commercial General Liability Insurance shall be written on an occurrence basis, and provide Premises/Operations, Products/Completed Operations, Independent Contractors, Personal Injury, and Contractual Liability coverage. The policy shall include the State, and others as required by the contract documents, as Additional Insured(s). This policy shall be primary, and any insurance or self-insurance carried by the State shall be considered excess and non-contributory. The Commercial Automobile Liability Insurance shall be written to cover all Owned, Non-owned, and Hired vehicles.

3. INSURANCE COVERAGE AMOUNTS REQUIRED

COMMERCIAL GENERAL LIABILITY	
General Aggregate	$2,000,000
Products/Completed Operations Aggregate	$2,000,000
Personal/Advertising Injury	$1,000,000 per occurrence
Bodily Injury/Property Damage	$1,000,000 per occurrence
Fire Damage	$50,000 any one fire
Medical Payments	$10,000 any one person
Damage to Rented Premises	$300,000 each occurrence
Contractual	Included
XCU Liability (Explosion, Collapse, and Underground Damage)	Included
Independent Contractors	Included
Abuse & Molestation	Included
WORKER'S COMPENSATION	
Employers Liability Limits	$500K/$500K/$500K

Statutory Limits- All States	Statutory - State of Nebraska
USL&H Endorsement	Statutory
Voluntary Compensation	Statutory
COMMERCIAL AUTOMOBILE LIABILITY	
Bodily Injury/Property Damage	$1,000,000 combined single limit
Include All Owned, Hired & Non-Owned Automobile liability	Included
Motor Carrier Act Endorsement	Where Applicable
UMBRELLA/EXCESS LIABILITY	
Over Primary Insurance	$5,000,000
SUBROGATION WAIVER	
"Workers' Compensation policy shall include a waiver of subrogation in favor of the State of Nebraska."	
LIABILITY WAIVER	
"Commercial General Liability & Commercial Automobile Liability policies shall be primary and any insurance or self-insurance carried by the State shall be considered excess and non-contributory."	

4. EVIDENCE OF COVERAGE

The Contractor should furnish the State, with their proposal response, a certificate of insurance coverage complying with the above requirements to the attention of the Buyer at 402-471-2089 (fax)

Administrative Services
State Purchasing Bureau
1526 K Street, Suite 130
Lincoln, NE 68508

These certificates or the cover sheet shall reference the RFP number, and the certificates shall include the name of the company, policy numbers, effective dates, dates of expiration, and amounts and types of coverage afforded. If the State is damaged by the failure of the Contractor to maintain such insurance, then the Contractor shall be responsible for all reasonable costs properly attributable thereto.

Notice of cancellation of any required insurance policy must be submitted to Administrative Services State Purchasing Bureau when issued and a new coverage binder shall be submitted immediately to ensure no break in coverage.

G. COOPERATION WITH OTHER CONTRACTORS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response	NOTES/COMMENTS:
JG			

The State may already have in place or choose to award supplemental contracts for work related to this Request for Proposal, or any portion thereof.

1.The State reserves the right to award the contract jointly between two or more potential Contractors, if such an arrangement is in the best interest of the State.
2.The Contractor shall agree to cooperate with such other Contractors, and shall not commit or permit any act which may interfere with the performance of work by any other Contractor.

H. INDEPENDENT CONTRACTOR

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

It is agreed that nothing contained herein is intended or should be construed in any manner as creating or establishing the relationship of partners between the parties hereto. The Contractor represents that it has, or will secure at its own expense, all personnel required to perform the services under the contract. The Contractor's employees and other persons engaged in work or services required by the contractor under the contract shall have no contractual relationship with the State; they shall not be considered employees of the State.

All claims on behalf of any person arising out of employment or alleged employment (including without limit claims of discrimination against the Contractor, its officers, or its agents) shall in no way be the responsibility of the State. The Contractor will hold the State harmless from any and all such claims. Such personnel or other persons shall not require nor be entitled to any compensation, rights, or benefits from the State including without limit, tenure rights, medical and hospital care, sick and vacation leave, severance pay, or retirement benefits.

I. CONTRACTOR RESPONSIBILITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The Contractor is solely responsible for fulfilling the contract, with responsibility for all services offered and products to be delivered as stated in the Request for Proposal, the Contractor's proposal, and the resulting contract. The Contractor shall be the sole point of contact regarding all contractual matters.

If the Contractor intends to utilize any Subcontractor's services, the Subcontractor's level of effort, tasks, and time allocation must be clearly defined in the Contractor's proposal. The Contractor shall agree that it will not utilize any Subcontractors not specifically included in its proposal in the performance of the contract without the prior written authorization of the State. Following execution of the contract, the Contractor shall proceed diligently with all services and shall perform such services with qualified personnel in accordance with the contract.

J. CONTRACTOR PERSONNEL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The Contractor warrants that all persons assigned to the project shall be employees of the Contractor or specified Subcontractors, and shall be fully qualified to perform the work required herein. Personnel employed by the Contractor to fulfill the terms of the contract shall remain under the sole direction and control of the Contractor. The Contractor shall include a similar provision in any contract with any Subcontractor selected to perform work on the project.

Personnel commitments made in the Contractor's proposal shall not be changed without the prior written approval of the State. Replacement of key personnel, if approved by the State, shall be with personnel of equal or greater ability and qualifications.

The State reserves the right to require the Contractor to reassign or remove from the project any Contractor or Subcontractor employee.

In respect to its employees, the Contractor agrees to be responsible for the following:

1. any and all employment taxes and/or other payroll withholding;
2. any and all vehicles used by the Contractor's employees, including all insurance required by state law;
3. damages incurred by Contractor's employees within the scope of their duties under the contract;
4. maintaining workers' compensation and health insurance and submitting any reports on such insurance to the extent required by governing State law; and
5. determining the hours to be worked and the duties to be performed by the Contractor's employees.

K. CONTRACT CONFLICTS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Contractor shall insure that contracts or agreements with sub-contractors and agents, and the performance of services in relation to this contract by sub-contractors and agents, does not conflict with this contract.

L. STATE OF NEBRASKA PERSONNEL RECRUITMENT PROHIBITION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to more narrowly define the extent of the prohibition. A more definite time period and more readily identifiable group of State employees will help us manage compliance with this restriction.

The Contractor shall not, at any time, during the term of this contract and for six (6) months thereafter, recruit or employ any State employee or agent ~~who has worked on the Request for Proposal or project, or who had any influence on decisions affecting the Request for Proposal or project.~~

M. CONFLICT OF INTEREST

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

By submitting a proposal, bidder certifies that there does not now exist any relationship between the bidder and any person or entity which is or gives the appearance of a conflict of interest related to this Request for Proposal or project.

The bidder certifies that it shall not take any action or acquire any interest, either directly or indirectly, which will conflict in any manner or degree with the performance of its services hereunder or which creates an actual or appearance of conflict of interest.

The bidder certifies that it will not employ any individual known by bidder to have a conflict of interest.

Any contractor (and its subcontractors) serving in the role of independent validation and verification (IV&V) service contractor to the State is prohibited from soliciting, proposing, or being awarded any project management, quality assurance, software design, development, or other manner of planning, design, development, or implementation phase activity on the projects for which these IV&V services are being procured.

This exclusion likewise extends to any other project within the State that may interact with or otherwise provide services to the projects or to the State during the full term of this contract. This exclusion is executed in accordance with federal regulations at 45 CFR 95.626, which require that this IV&V effort, "... be conducted by an entity that is independent from the State".

IV&V is the set of verification and validation activities performed by an agency not under the control of the organization developing the software. IV&V services must be provided and managed by an organization that is technically and managerially independent of the subject software development project. This independence takes two mandatory forms.

First, technical independence requires that the IV&V services provider organization, its personnel, and subcontractors are not and have not been involved in the software development or implementation effort or in the project's initial planning and/or subsequent design. Technical independence helps ensure that IV&V review reports are free of personal or professional bias, posturing, or gold plating.

Second, managerial independence is required to make certain that the IV&V effort is provided by an organization that is departmentally and hierarchically separate from the software development and program management organizations. Managerial independence helps ensure that the IV&V service provider can deliver findings and recommendations to state and federal executive leadership and management without restriction, fear of retaliation, or coercion (e.g., reports being subject to prior review or approval from the development group before release to outside entities, such as the federal government).

N. PROPOSAL PREPARATION COSTS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The State shall not incur any liability for any costs incurred by bidders in replying to this Request for Proposal, in the demonstrations and/or oral presentations, or in any other activity related to bidding on this Request for Proposal.

O. ERRORS AND OMISSIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The bidder shall not take advantage of any errors and/or omissions in this Request for Proposal or resulting contract. The bidder must promptly notify the State of any errors and/or omissions that are discovered.

P. BEGINNING OF WORK

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The bidder shall not commence any billable work until a valid contract has been fully executed by the State and the successful Contractor. The Contractor will be notified in writing when work may begin.

Q. ASSIGNMENT BY THE STATE

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The State shall have the right to assign or transfer the contract or any of its interests herein to any agency, board, commission, or political subdivision of the State of Nebraska. There shall be no charge to the State for any assignment hereunder.

R. ASSIGNMENT BY THE CONTRACTOR

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to provide that the State' prior written consent will not be required to an affiliate or in the event of a change of control. We need this flexibility in order to have control of our own business decisions.

The Contractor may not assign, voluntarily or involuntarily, the contract or any of its rights or obligations hereunder (including without limitation rights and duties of performance) to any third party, without the prior written consent of the State, which will not be unreasonably withheld, provided, however, the State's consent is not required for the Contractor to assign this contract to an affiliate or in connection with a merger, acquisition, or sale of all or substantially all of the Contractor's assets or of a controlling equity interest.

S. DEVIATIONS FROM THE REQUEST FOR PROPOSAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The requirements contained in the Request for Proposal become a part of the terms and conditions of the contract

resulting from this Request for Proposal. Any deviations from the Request for Proposal must be clearly defined by the bidder in its proposal and, if accepted by the State, will become part of the contract. Any specifically defined deviations must not be in conflict with the basic nature of the Request for Proposal, mandatory requirements, or applicable state or federal laws or statutes. "Deviation", for the purposes of this RFP, means any proposed changes or alterations to either the contractual language or deliverables within the scope of this RFP. The State discourages deviations and reserves the right to reject proposed deviations.

T. GOVERNING LAW

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The contract shall be governed in all respects by the laws and statutes of the State of Nebraska. Any legal proceedings against the State of Nebraska regarding this Request for Proposal or any resultant contract shall be brought in the State of Nebraska administrative or judicial forums as defined by State law. The Contractor must be in compliance with all Nebraska statutory and regulatory law.

U. ATTORNEY'S FEES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

In the event of any litigation, appeal, or other legal action to enforce any provision of the contract, the Contractor agrees to pay all expenses of such action, as permitted by law, including attorney's fees and costs, if the State is the prevailing party.

V. ADVERTISING

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The Contractor agrees not to refer to the contract award in advertising in such a manner as to state or imply that the company or its services are endorsed or preferred by the State. News releases pertaining to the project shall not be issued without prior written approval from the State.

W. STATE PROPERTY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The Contractor shall be responsible for the proper care and custody of any State-owned property which is furnished for the Contractor's use during the performance of the contract. The Contractor shall reimburse the State for any loss or damage of such property; normal wear and tear is expected.

X. SITE RULES AND REGULATIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
JE			

The Contractor shall use its best efforts to ensure that its employees, agents, and Subcontractors comply with site rules and regulations while on State premises. If the Contractor must perform on-site work outside of the daily operational hours set forth by the State, it must make arrangements with the State to ensure access to the facility and the equipment has been arranged. No additional payment will be made by the State on the basis of lack of access, unless the State fails to provide access as agreed to between the State and the Contractor.

Y. NOTIFICATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
JE			

During the bid process, all communication between the State and a bidder shall be between the bidder's representative clearly noted in its proposal and the buyer noted in Section II.A. Procuring Office and Contact Person, of this RFP. After the award of the contract, all notices under the contract shall be deemed duly given upon delivery to the staff designated as the point of contact for this Request for Proposal, in person, or upon delivery by U.S. Mail, facsimile, or e-mail. Each bidder should provide in its proposal the name, title, and complete address of its designee to receive notices.

1.Except as otherwise expressly specified herein, all notices, requests, or other communications shall be in writing and shall be deemed to have been given if delivered personally or mailed, by U.S. Mail, postage prepaid, return receipt requested, to the parties at their respective addresses set forth above, or at such other addresses as may be specified in writing by either of the parties. All notices, requests, or communications shall be deemed effective upon personal delivery or three (3) calendar days following deposit in the mail.

2.Whenever the Contractor encounters any difficulty which is delaying or threatens to delay its timely performance under the contract, the Contractor shall immediately give notice thereof in writing to the State reciting all relevant information with respect thereto. Such notice shall not in any way constitute a basis for an extension of the delivery schedule or be construed as a waiver by the State of any of its rights or remedies to which it is entitled by law or equity or pursuant to the provisions of the contract. Failure to give such notice, however, may be grounds for denial of any request for an extension of the delivery schedule because of such delay.

Either party may change its address for notification purposes by giving notice of the change, and setting forth the new address and an effective date.

For the duration of the contract, all communication between Contractor and the State regarding the contract shall take place between the Contractor and individuals specified by the State in writing. Communication about the contract between Contractor and individuals not designated as points of contact by the State is strictly forbidden.

Z. EARLY TERMINATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to the State's right to immediately terminate the contract if the Contractor intentionally discloses confidential information. We ought to be able to intentionally disclose confidential information to our subcontractors or as required by law. The right to terminate should only apply if the disclosure violates the contract.

The contract may be terminated as follows:
1.The State and the Contractor, by mutual written agreement, may terminate the contract at any time.

2.The State, in its sole discretion, may terminate the contract for any reason upon thirty (30) calendar day's written notice to the Contractor. Such termination shall not relieve the Contractor of warranty or other service obligations incurred under the terms of the contract. In the event of termination the Contractor shall be entitled to payment, determined on a pro rata basis, for products or services satisfactorily performed or provided.

3.The State may terminate the contract immediately for the following reasons:

a.if directed to do so by statute;
b.Contractor has made an assignment for the benefit of creditors, has admitted in writing its inability to pay debts as they mature, or has ceased operating in the normal course of business;
c.a trustee or receiver of the Contractor or of any substantial part of the Contractor's assets has been appointed by a court;
d.fraud, misappropriation, embezzlement, malfeasance, misfeasance, or illegal conduct pertaining to performance under the contract by its Contractor, its employees, officers, directors, or shareholders;
e.an involuntary proceeding has been commenced by any party against the Contractor under any one of the chapters of Title 11 of the United States Code and (i) the proceeding has been pending for at least sixty (60) calendar days; or (ii) the Contractor has consented, either expressly or by operation of law, to the entry of an order for relief; or (iii) the Contractor has been decreed or adjudged a debtor;
f.a voluntary petition has been filed by the Contractor under any of the chapters of Title 11 of the United States Code;
g.Contractor intentionally discloses confidential information in violation of Contractor's obligations of confidentiality under this contract.
h.Contractor has or announces it will discontinue support of the deliverable;
i.second or subsequent documented "vendor performance report" form deemed acceptable by the State Purchasing Bureau; or
j.Contractor engaged in collusion or actions which could have provided Contractor an unfair advantage in obtaining this contract.

AA. FUNDING OUT CLAUSE OR LOSS OF APPROPRIATIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The State may terminate the contract, in whole or in part, in the event funding is no longer available. The State's obligation to pay amounts due for fiscal years following the current fiscal year is contingent upon legislative appropriation of funds for the contract. Should said funds not be appropriated, the State may terminate the contract with respect to those payments for the fiscal years for which such funds are not appropriated. The State will give the Contractor written notice thirty (30) calendar days prior to the effective date of any termination, and advise the Contractor of the location (address and room number) of any related equipment. All obligations of the State to make payments after the termination date will cease and all interest of the State in any related equipment will terminate. The Contractor shall be entitled to receive just and equitable compensation for any authorized work which has been satisfactorily completed as of the termination date. In no event shall the Contractor be paid for a loss of anticipated profit.

BB. BREACH BY CONTRACTOR

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to provide that the State must provide at least a thirty (30) day cure period.

The State may terminate the contract, in whole or in part, if the Contractor fails to perform its obligations under the contract in a timely and proper manner. The State ~~may~~ shall by providing a written notice of default to the Contractor, allow the Contractor to cure a failure or breach of contract within a period of at least thirty (30) calendar days (or longer at State's discretion considering the gravity and nature of the default). Said notice shall be delivered by Certified Mail, Return Receipt Requested, or in person with proof of delivery. Allowing the Contractor time to cure a failure or breach of contract does not waive the State's right to immediately terminate the contract for the same or different contract breach which may occur at a different time. In case of default of the Contractor, the State may contract the service from other sources and hold the Contractor responsible for any excess cost occasioned thereby.

CC. ASSURANCES BEFORE BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

If any document or deliverable required pursuant to the contract does not fulfill the requirements of the Request for Proposal/resulting contract, upon written notice from the State, the Contractor shall deliver assurances in the form of additional Contractor resources at no additional cost to the project in order to complete the deliverable, and to ensure that other project schedules will not be adversely affected.

DD. ADMINISTRATION – CONTRACT TERMINATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

1.Contractor must provide confirmation that upon contract termination all deliverables prepared in accordance with this agreement shall become the property of the State of Nebraska; subject to the ownership provision (section E) contained herein, and is provided to the State of Nebraska at no additional cost to the State.

2.Contractor must provide confirmation that in the event of contract termination, all records that are the property of the State will be returned to the State within thirty (30) calendar days. Notwithstanding the above, Contractor may retain one copy of any information as required to comply with applicable work product documentation standards or as are automatically retained in the course of Contractor's routine back up procedures.

EE. PENALTY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

In the event that the Contractor fails to perform any substantial obligation under the contract, the State may withhold all monies due and payable to the Contractor, without penalty, until such failure is cured or otherwise adjudicated. Failure to meet the dates for the deliverables as agreed upon by the parties may result in an assessment of penalty due the State of $500.00 dollars per day, until the deliverables are approved. Contractor will be notified in writing when penalty will commence.

FF. FORCE MAJEURE

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Neither party shall be liable for any costs or damages resulting from its inability to perform any of its obligations under the contract due to a natural disaster, or other similar event outside the control and not the fault of the affected party ("Force Majeure Event"). A Force Majeure Event shall not constitute a breach of the contract. The party so affected shall immediately give notice to the other party of the Force Majeure Event. The State may grant relief from performance of the contract if the Contractor is prevented from performance by a Force Majeure Event. The burden of proof for the need for such relief shall rest upon the Contractor. To obtain release based on a Force Majeure Event, the Contractor shall file a written request for such relief with the State Purchasing Bureau. Labor disputes with the impacted party's own employees will not be considered a Force Majeure Event and will not suspend performance requirements under the contract.

GG. PROHIBITION AGAINST ADVANCE PAYMENT

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Payments shall not be made until contractual deliverable(s) are received and accepted by the State.

HH. PAYMENT

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

State will render payment to Contractor when the terms and conditions of the contract and specifications have been satisfactorily completed on the part of the Contractor as solely determined by the State. Payment will be made by the responsible agency in compliance with the State of Nebraska Prompt Payment Act (See Neb. Rev. Stat. §§ 81-2401 through 81-2408). The State may require the Contractor to accept payment by electronic means such as ACH deposit. In no event shall the State be responsible or liable to pay for any services provided by the Contractor prior to the Effective Date, and the Contractor hereby waives any claim or cause of action for any such services.

II. INVOICES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Invoices for payments must be submitted by the Contractor to the agency requesting the services with sufficient detail to support payment. The terms and conditions included in the Contractor's invoice shall be deemed to be solely for the convenience of the parties. No terms or conditions of any such invoice shall be binding upon the State, and no action by the State, including without limitation the payment of any such invoice in whole or in part, shall be construed as binding or estopping the State with respect to any such term or condition, unless the invoice term or condition has been previously agreed to by the State as an amendment to the contract.

JJ. RIGHT TO AUDIT

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Contractor shall establish and maintain a reasonable accounting system that enables the State to readily audit contract. The State and its authorized representatives shall have the right to audit, to examine, and to make copies of or extracts from all financial and related records (in whatever form they may be kept, whether written, electronic, or other) relating to or pertaining to this contract kept by or under the control of the Contractor, including, but not limited to those kept by the Contractor, its employees, agents, assigns, successors, and Subcontractors. Such records shall include, but not be limited to, accounting records, written policies and procedures; all paid vouchers including those for out-of-pocket expenses; other reimbursement supported by invoices; ledgers; cancelled checks; deposit slips; bank statements; journals; original estimates; estimating work sheets; contract amendments and change order files; back charge logs and supporting documentation; insurance documents; payroll documents; timesheets; memoranda; and correspondence.

Contractor shall, at all times during the term of this contract and for a period of five (5) years after the completion of this contract, maintain such records, together with such supporting or underlying documents and materials. The Contractor shall at any time requested by the State, whether during or after completion of this contract and at Contractor's own expense make such records available for inspection and audit (including copies and extracts of

records as required) by the State. Such records shall be made available to the State during normal business hours at the Contractor's office or place of business. In the event that no such location is available, then the financial records, together with the supporting or underlying documents and records, shall be made available for audit at a time and location that is convenient for the State. Contractor shall ensure the State has these rights with Contractor's assigns, successors, and Subcontractors, and the obligations of these rights shall be explicitly included in any subcontracts or agreements formed between the Contractor and any Subcontractors to the extent that those Subcontracts or agreements relate to fulfillment of the Contractor's obligations to the State.

Costs of any audits conducted under the authority of this right to audit and not addressed elsewhere will be borne by the State unless certain exemption criteria are met. If the audit identifies overpricing or overcharges (of any nature) by the Contractor to the State in excess of one-half of one percent (.5%) of the total contract billings, the Contractor shall reimburse the State for the total costs of the audit. If the audit discovers substantive findings related to fraud, misrepresentation, or non-performance, the Contractor shall reimburse the State for total costs of audit. Any adjustments and/or payments that must be made as a result of any such audit or inspection of the Contractor's invoices and/or records shall be made within a reasonable amount of time (not to exceed 90 days) from presentation of the State's findings to Contractor.

KK. TAXES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to provide that the price quoted is in addition to and not in lieu of any taxes.

~~The State is not required to pay taxes of any kind and assumes no such liability as a result of this solicitation. Any property tax payable on the Contractor's equipment which may be installed in a state-owned facility is the responsibility of the Contractor.~~

The State will pay, or reimburse Contractor for, any and all applicable sales, use, excise, franchise or other taxes (collectively, "Taxes"), whether federal, state or local, however designated, which are levied or imposed with respect to the services; excluding, however, income or employment taxes imposed upon or separately payable by Contractor with respect to its employees, agents, contractors or affiliates, and property taxes payable by Contractor on property owned by Contractor. The price quoted by Contractor is in addition to, and not in lieu of any Taxes. If the State claims exemption from any Taxes it will provide a certificate upon request

LL. INSPECTION AND APPROVAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Final inspection and approval of all work required under the contract shall be performed by the designated State officials. The State and/or its authorized representatives shall have the right to enter any premises where the Contractor or Subcontractor duties under the contract are being performed, and to inspect, monitor or otherwise evaluate the work being performed. All inspections and evaluations shall be at reasonable times and in a manner that will not unreasonably delay work.

MM. CHANGES IN SCOPE/CHANGE ORDERS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The State may, upon the written agreement of Contractor, make changes to the contract within the general scope of the RFP. The State may, at any time work is in progress, by written agreement, make alterations in the terms of work as shown in the specifications, require the Contractor to make corrections, decrease the quantity of work, or make such other changes as the State may find necessary or desirable. The Contractor shall not claim forfeiture of contract by reasons of such changes by the State. Changes in work and the amount of compensation to be paid to the Contractor shall be determined in accordance with applicable unit prices if any, or a pro-rated value.

Corrections of any deliverable, service or performance of work required pursuant to the contract shall not be deemed a modification. Changes or additions to the contract beyond the scope of the RFP are not permitted.

NN. SEVERABILITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

If any term or condition of the contract is declared by a court of competent jurisdiction to be illegal or in conflict with any law, the validity of the remaining terms and conditions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the contract did not contain the particular provision held to be invalid.

OO. CONFIDENTIALITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to more narrowly define confidential information. We also request modifications to this section to make it consistent with our privacy and information security policies and procedures. It is not feasible for us to follow different policies and procedures for each one of our many clients.

~~All materials and information provided by the State or acquired by the Contractor on behalf of the State shall be regarded as confidential information. All materials and information provided by the State or acquired by the Contractor on behalf of the State shall be handled in accordance with federal and state law, and ethical standards. The Contractor must ensure the confidentiality of such materials or information. Should said confidentiality be breached by a Contractor; Contractor shall notify the State immediately of said breach and take immediate corrective action.~~

~~It is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a (i)(1), which is made applicable to Contractors by 5 U.S.C. 552a (m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.~~

All materials and information provided by the State or acquired by the Contractor on behalf of the State shall be regarded as confidential information ("Confidential Information"). Confidential Information does not include information which: (i) is or becomes part of the public domain; (ii) was already known to the receiving party prior to its disclosure; (iii) is lawfully obtained from a third party without obligations of confidentiality; (iv) is independently developed by the receiving party; or (v) must be communicated in response to a valid law, regulation or court order, provided the disclosing party uses reasonable efforts to notify the other party prior to disclosure (unless such notification is prohibited by law, regulation or court order) so such party may seek a protective order or otherwise prevent or limit such disclosure. The Contractor will take commercially reasonable steps to prevent disclosure of Confidential Information, including, at a minimum, such steps it would take to protect its own Confidential Information. A "Security Incident" means any unauthorized or unlawful access to, use, disclosure or alteration of non-public or personally identifiable information ("Personal Information"). In the event of a Security Incident, the contractor will promptly (i) assess the nature and scope of the Security Incident; (ii) identify the Personal Information involved, if any; (iii) take appropriate steps to contain, control and stop the Security Incident; and (iv), in the event Personal Information was compromised and it is reasonably suspected that misuse will result, notify the other party of the Security Incident, subject to any request by law enforcement or other government agency to withhold such notice pending the completion of an investigation.

Contractor's employees and officers are informed through annual privacy, security, and related training programs (as well as Privacy Standard Operating Procedures) about civil and criminal penalties that may be imposed under federal and state laws for unauthorized use or disclosure of confidential information

PP. PROPRIETARY INFORMATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Data contained in the proposal and all documentation provided therein, become the property of the State of Nebraska and the data becomes public information upon opening the proposal. If the bidder wishes to have any information withheld from the public, such information must fall within the definition of proprietary information contained within Nebraska's public record statutes. **All proprietary information the bidder wishes the State to withhold must be submitted in a sealed package, which is separate from the remainder of the proposal, and provide supporting documents showing why such documents should be marked proprietary**. The separate package must be clearly marked PROPRIETARY on the outside of the package. **Bidders may not mark their entire Request for Proposal as proprietary**. Bidder's cost proposals may not be marked as proprietary information. Failure of the bidder to follow the instructions for submitting proprietary and copyrighted information may result in the information being viewed by other bidders and the public. Proprietary information is defined as trade secrets, academic and scientific research work which is in progress and unpublished, and other information which if released would give advantage to business competitors and serve no public purpose (see Neb. Rev. Stat. § 84-712.05(3)). In accordance with Attorney General Opinions 92068 and 97033, bidders submitting information as proprietary may be required to prove specific, named competitor(s) who would be advantaged by release of the information and the specific advantage the competitor(s) would receive. Although every effort will be made to withhold information that is properly submitted as proprietary and meets the State's definition of proprietary information, the State is under no obligation to maintain the confidentiality of proprietary information and accepts no liability for the release of such information.

QQ. CERTIFICATION OF INDEPENDENT PRICE DETERMINATION/COLLUSIVE BIDDING

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

By submission of this proposal, the bidder certifies that it is the party making the foregoing proposal and that the proposal is not made in the interest of, or on behalf of, any undisclosed person, partnership, company, association, organization, or corporation; that the proposal is genuine and not collusive or sham; that the bidder has not directly or indirectly induced or solicited any other bidder to put in a false or sham proposal, and has not directly or indirectly colluded, conspired, connived, or agreed with any bidder or anyone else to put in a sham proposal, or that anyone shall refrain from bidding; that the bidder has not in any manner, directly or indirectly, sought by agreement, communication, or conference with anyone to fix the proposal price of the bidder or any other bidder, or to fix any overhead, profit, or cost element of the proposal price, or of that of any other bidder, or to secure any advantage against the public body awarding the contract of anyone interested in the proposed contract; that all statements contained in the proposal are true; and further that the bidder has not, directly or indirectly, submitted the proposal price or any breakdown thereof, or the contents thereof, or divulged information or data relative thereto, or paid, and will not pay, any fee to any corporation, partnership, company association, organization, proposal depository, or to any member or agent thereof to effectuate a collusive or sham proposal.

RR. STATEMENT OF NON-COLLUSION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The proposal shall be arrived at by the bidder independently and be submitted without collusion with, and without any direct or indirect agreement, understanding or planned common course of action with, any person; firm; corporation; bidder; Contractor of materials, supplies, equipment or services described in this RFP. Bidder shall not collude with, or attempt to collude with, any state officials, employees or agents; or evaluators or any person involved in this RFP. The bidder shall not take any action in the restraint of free competition or designed to limit independent bidding or to create an unfair advantage.

Should it be determined that collusion occurred, the State reserves the right to reject a bid or terminate the contract and impose further administrative sanctions.

SS. PRICES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to delete the second paragraph of this section. Since this project is being bid competitively, these obligations should be unnecessary. We are offering our most competitive pricing.

All prices, costs, and terms and conditions outlined in the proposal shall remain fixed and valid commencing on the opening date of the proposal until an award is made or the Request for Proposal is cancelled.

~~Prices quoted on the Cost Proposal form shall remain fixed for the first year of the contract period. Any request for a price increase must be submitted in writing to the State Purchasing Bureau a minimum of 120 days prior to the price increase effective date, and be accompanied by documentation justifying the price increase. Further documentation may be required by the State to justify the increase. The State reserves the right to deny any requested price increase. No price increases are to be billed to any State Agencies prior to written amendment of the contract by the parties.~~

The State will be given full proportionate benefit of any price decrease during the term of the contract. Contractor represents and warrants that all prices for services, now or subsequently specified, are as low as and no higher than prices which the Contractor has charged or intends to charge customers other than the State for the same or similar products and services of the same or equivalent quantity and quality for delivery or performance during the same periods of time. If, during the term of the contract, the Contractor shall reduce any and/or all prices charged to any customers other than the State for the same or similar products or services specified herein, the Contractor shall make an equal or equivalent reduction in corresponding prices for said specified products or services.

Contractor also represents and warrants that all prices set forth in the contract and all prices in addition, which the Contractor may charge under the terms of the contract, do not and will not violate any existing federal, state, or municipal law or regulations concerning price discrimination and/or price fixing. Contractor agrees to hold the State harmless from any such violation. Prices quoted shall not be subject to increase throughout the contract period unless specifically allowed by these specifications.

TT. BEST AND FINAL OFFER

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The State will compile the final scores for all parts of each proposal. The award may be granted to the highest scoring responsive and responsible bidder. Alternatively, the highest scoring bidder or bidders may be requested to submit best and final offers. If best and final offers are requested by the State and submitted by the bidder, they will be evaluated (using the stated criteria), scored, and ranked by the Evaluation Committee. The award will then be granted to the highest scoring bidder. However, a bidder should provide its best offer in its original proposal. Bidders should not expect that the State will request a best and final offer.

UU. ETHICS IN PUBLIC CONTRACTING

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

No bidder shall pay or offer to pay, either directly or indirectly, any fee, commission compensation, gift, gratuity, or anything of value to any State officer, legislator, employee or evaluator based on the understanding that the receiving person's vote, actions, or judgment will be influenced thereby. No bidder shall give any item of value to any employee of the State Purchasing Bureau or any evaluator.

Bidders shall be prohibited from utilizing the services of lobbyists, attorneys, political activists, or consultants to secure the contract. It is the intent of this provision to assure that the prohibition of state contact during the procurement process is not subverted through the use of lobbyists, attorneys, political activists, or consultants. It is the intent of the State that the process of evaluation of proposals and award of the contract be completed without

external influence. It is not the intent of this section to prohibit bidders from seeking professional advice, for example consulting legal counsel, regarding terms and conditions of this Request for Proposal or the format or content of their proposal.

If the bidder is found to be in non-compliance with this section of the Request for Proposal, they may forfeit the contract if awarded to them or be disqualified from the selection process.

VV. INDEMNIFICATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to (a) limit Contractor's indemnification obligation to infringement by the products or services and (b) exclude the Contractor's indemnification obligations when the intellectual property ("IP") infringement is due to the State's use of the IP in a manner not authorized by the Contract or in combination with other IP not provided by the Contractor. We request the removal of the State's right to withhold its consent to a settlement for any reason. We expect that the State may withhold its consent but only if there are reasonable grounds for withholding it. We also request that the second paragraph be deleted. This paragraph gives the State additional remedies that duplicate and overlap the indemnification provision. We believe that these are additional remedies are not necessary given the indemnification provision.

1.GENERAL

The Contractor agrees to defend, indemnify, hold, and save harmless the State and its employees, volunteers, agents, and its elected and appointed officials ("the indemnified parties") from and against any and all claims, liens, demands, damages, liability, actions, causes of action, losses, judgments, costs, and expenses of every nature, including investigation costs and expenses, settlement costs, and attorney fees and expenses ("the claims"), sustained or asserted against the State, arising out of, resulting from, or attributable to the willful misconduct, negligence, error, or omission of the Contractor, its employees, Subcontractors, consultants, representatives, and agents, except to the extent such Contractor liability is attenuated by any action of the State which directly and proximately contributed to the claims.

2.INTELLECTUAL PROPERTY

The Contractor agrees it will, at its sole cost and expense, defend, indemnify, and hold harmless the indemnified parties from and against any and all claims, to the extent such claims arise out of, result from, or are attributable to, the actual or alleged infringement or misappropriation of any patent, copyright, trade secret, trademark, or confidential information of any third party ~~by the Contractor or its employees, Subcontractors, consultants, representatives, and agents~~ by products or services provided by the Contractor, except to the extent such claim is caused by, relates to or arises out of (a) the State's failure to use the Deliverables as permitted under the contract or (b) the State's configuration or use of the Deliverables in combination with other software, equipment, services, processes, elements, components or systems that are not provided by the Contractor; provided, however, the State gives the Contractor prompt notice in writing of the claim. The Contractor may not settle any infringement claim that will affect the State's use of the Licensed Software without the State's prior written consent, ~~which consent may be withheld for any reason.~~

~~If a judgment or settlement is obtained or reasonably anticipated against the State's use of any intellectual property for which the Contractor has indemnified the State, the Contractor shall, at the Contractor's sole cost and expense, promptly modify the item or items which were determined to be infringing, acquire a license or licenses on the State's behalf to provide the necessary rights to the State to eliminate the infringement, or provide the State~~

~~with a non-infringing substitute that provides the State the same functionality. At the State's election, the actual or anticipated judgment may be treated as a breach of warranty by the Contractor, and the State may receive the remedies provided under this RFP.~~

3.PERSONNEL
The Contractor shall, at its expense, indemnify and hold harmless the indemnified parties from and against any claim with respect to withholding taxes, worker's compensation, employee benefits, or any other claim, demand, liability, damage, or loss of any nature relating to any of the personnel provided by the Contractor.

4.SELF-INSURANCE
The State of Nebraska is self-insured for any loss and purchases excess insurance coverage pursuant to Neb. Rev. Stat. § 81-8,239.01 (Reissue 2008). If there is a presumed loss under the provisions of this agreement, Contractor may file a claim with the Office of Risk Management pursuant to Neb. Rev. Stat. §§ 81-8,829 – 81-8,306 for review by the State Claims Board. The State retains all rights and immunities under the State Miscellaneous (Section 81-8,294), Tort (Section 81-8,209), and Contract Claim Acts (Section 81-8,302), as outlined in Neb. Rev. Stat. § 81-8,209 *et seq.* and under any other provisions of law and accepts liability under this agreement to the extent provided by law.

5.ALL REMEDIES AT LAW
Nothing in this agreement shall be construed as an indemnification by one party of the other for liabilities of a party or third parties for property loss or damage or death or personal injury arising out of and during the performance of this lease. Any liabilities or claims for property loss or damages or for death or personal injury by a party or its agents, employees, contractors or assigns or by third persons, arising out of and during the performance of this lease shall be determined according to applicable law.

WW. NEBRASKA TECHNOLOGY ACCESS STANDARDS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Contractor shall review the Nebraska Technology Access Standards, found at http://nitc.nebraska.gov/standards/2-201.html and ensure that products and/or services provided under the contract are in compliance or will comply with the applicable standards to the greatest degree possible. In the event such standards change during the Contractor's performance, the State may create an amendment to the contract to request the contract comply with the changed standard at a cost mutually acceptable to the parties.

XX. ANTITRUST

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The Contractor hereby assigns to the State any and all claims for overcharges as to goods and/or services provided in connection with this contract resulting from antitrust violations which arise under antitrust laws of the United States and the antitrust laws of the State.

YY. DISASTER RECOVERY/BACK UP PLAN

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to clarify that we can provide an executive summary of our disaster recovery plan, subject to receipt of a non-disclosure agreement. For security reasons, we must keep our disaster recovery plan confidential.

~~The Contractor shall have a disaster recovery and back-up plan, of which a copy should be provided to the State, which includes, but is not limited to equipment, personnel, facilities, and transportation, in order to continue services as specified under the specifications in the contract in the event of a disaster.~~

The contractor shall have a disaster recovery and back-up plan, an executive summary of which will be provided to the State upon request and subject to receipt of a non-disclosure agreement from the State. The executive summary will summarize the plan which addresses, but is not limited to, equipment, personnel, facilities, and transportation, in order to continue services as specified under the specifications in the contract in the event of a disaster.

ZZ. TIME IS OF THE ESSENCE

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to clarify that this provision is subject to the contract's force majeure provision and to provide that the Contractor will not be responsible for delays that are due to delays in performance by the State or its contractors.

Subject to Section FF., Force Majeure, Time is of the essence in this contract. The Contractor will not be liable for any delays in performance that are due to delays in performance by the State or its contractors. The acceptance of late performance with or without objection or reservation by the State shall not waive any rights of the State nor constitute a waiver of the requirement of timely performance of any obligations on the part of the Contractor remaining to be performed.

AAA. RECYCLING

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Preference will be given to items which are manufactured or produced from recycled material or which can be readily reused or recycled after their normal use as per Neb. Rev. Stat. § 81-15,159.

BBB. DRUG POLICY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Contractor certifies it maintains a drug free work place environment to ensure worker safety and workplace integrity. Contractor agrees to provide a copy of its drug free workplace policy at any time upon request by the State.

CCC. EMPLOYEE WORK ELIGIBILITY STATUS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The Contractor is required and hereby agrees to use a federal immigration verification system to determine the work eligibility status of employees physically performing services within the State of Nebraska. A federal immigration verification system means the electronic verification of the work authorization program authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 U.S.C. 1324a, known as the E-Verify Program, or an equivalent federal program designated by the United States Department of Homeland Security or other federal agency authorized to verify the work eligibility status of an employee.

If the Contractor is an individual or sole proprietorship, the following applies:

1.The Contractor must complete the *United States Citizenship Attestation Form*, available on the Department of Administrative Services website at http://das.nebraska.gov/materiel/purchasing.html

The completed United States Attestation Form should be submitted with the Request for Proposal response.

2.If the Contractor indicates on such attestation form that he or she is a qualified alien, the Contractor agrees to provide the US Citizenship and Immigration Services documentation required to verify the Contractor's lawful presence in the United States using the Systematic Alien Verification for Entitlements (SAVE) Program.

3.The Contractor understands and agrees that lawful presence in the United States is required and the Contractor may be disqualified or the contract terminated if such lawful presence cannot be verified as required by Neb. Rev. Stat. § 4-108.

DDD. CERTIFICATION REGARDING DEBARMENT, SUSPENSION AND INELIGIBILITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The Contractor, by signature to this RFP, certifies that the Contractor is not presently debarred, suspended,

proposed for debarment, declared ineligible, or voluntarily excluded by any federal department or agency from participating in transactions (debarred). The Contractor also agrees to include the above requirements in any and all Subcontracts into which it enters. The Contractor shall immediately notify the Department if, during the term of this contract, Contractor becomes debarred. The Department may immediately terminate this contract by providing Contractor written notice if Contractor becomes debarred during the term of this contract.

Contractor, by signature to this RFP, certifies that Contractor has not had a contract with the State of Nebraska terminated early by the State of Nebraska. If Contractor has had a contract terminated early by the State of Nebraska, Contractor must provide the contract number, along with an explanation of why the contract was terminated early. Prior early termination may be cause for rejecting the proposal.

EEE. POLITICAL SUB-DIVISIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The Contractor may extend the contract to political sub-divisions conditioned upon the honoring of the prices charged to the State. Terms and conditions of the Contract must be met by political sub-divisions. Under no circumstances shall the State be contractually obligated or liable for any purchases by political sub-divisions or other public entities not authorized by Neb. Rev. Stat. § 81-145, listed as "all officers of the state, departments, bureaus, boards, commissions, councils, and institutions receiving legislative appropriations." A listing of Nebraska political subdivisions may be found at the website of the Nebraska Auditor of Public Accounts.

FFF. OFFICE OF PUBLIC COUNSEL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to clarify that the Contractor will not be providing health and human services. This section should not apply.

If it provides, under the terms of this contract and on behalf of the State of Nebraska, health and human services to individuals; service delivery; service coordination; or case management, Contractor shall submit to the jurisdiction of the Office of Public Counsel, pursuant to Neb. Rev. Stat. §§ 81-8,240 et seq. This section shall survive the termination of this contract and shall not apply if Contractor is a long-term care facility subject to the Long-Term Care Ombudsman Act, Neb. Rev. Stat. §§ 81-2237 et seq. The parties agree that the Contractor will not provide health and human services to individuals on behalf of the State under the terms of this contract.

GGG. LONG-TERM CARE OMBUDSMAN

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			First Data requests an exception to clarify that we are not a long-term care facility. This section should not apply.

If it is a long-term care facility subject to the Long-Term Care Ombudsman Act, Neb. Rev. Stat. §§ 81-2237 et seq., Contractor shall comply with the Act. This section shall survive the termination of this contract. The parties agree that the Contractor is not a long-term care facility.

2
Corporate Overview

2.0 Corporate Overview

First Data is pleased to offer our independent verification and validation (IV&V) services to Nebraska in support of the Eligibility and Enrollment Solution (EES) and Data Management and Analytics (DMA) projects, as well as any optional projects implemented, to support the transition to a Medicaid enterprise driven by data and analytics. First Data's culture is founded on continuous improvement principles. In addition, based on our experience on the Nebraska EES Project, and our understanding of the culture and environment of the Department of Health and Human Services (DHHS) we focused our response to highlight tools, techniques and program and industry expertise on DHHS specific requirements. We will continue to be flexible in our efforts to address DHHS' needs. Our flexibility and attention to your needs is what DHHS can depend on from First Data for this engagement.

The First Data Team brings a strong knowledge of Medicaid enterprise solutions and emerging changes through our Medicaid consulting practice, which follows the trends in Medicaid, anticipates changes, and analyzes impacts to our clients and future projects. Our Medicaid Subject Matter Experts (SMEs) work collaboratively with our State Medicaid clients and the Centers for Medicare & Medicaid Services (CMS) regional directors to confirm that planning and upcoming activities will align with CMS' direction to streamline review and approval processes. Our research, analysis, and communications support ongoing alignment with CMS.

First Data also maintains a personal interest in making Nebraska successful in this effort. Not only do we have experience working with your team, but First Data has a strong connection to Nebraska with over 5,000 current employees and over 45 years of presence operating in the State. We have a vested interest in this project and genuinely care about the success of this important program. Our employees and their families stand to benefit from your success.

First Data Government Solutions, LP is the government facing business component of First Data Corporation. First Data Government Solutions, LP was formed to bring business and technical expertise in IT solutions and consulting services to government and has been performing high-profile government projects for more than 30 years. We bring a team of consultants dedicated solely to helping government clients effectively perform their mission by providing a seamless approach to business, technology, and consulting services. Our professionals – subject matter specialists, business analysts, technical analysts, project

managers, quality assurance analysts, and application developers – combine world-class business experience with strong technical expertise.

Understanding of the Project

We know your plan is to manage multiple initiatives as a portfolio of projects with staged implementation, and are pleased to hear that this process will be managed by a single governance structure. Successfully achieving the DHHS and Division of Medicaid and Long Term Care (MLTC)'s long-term operational vision and objectives requires a partner with expertise, experience, and insight into current IV&V and quality assurance practices, coupled with a broad understanding of healthcare and human services program delivery. Partnering with First Data, Nebraska also benefits from a partner that understands the State's complex technological and business environments and how it must integrate with various Medicaid stakeholders as well as internal state resources. **First Data is that partner**. We bring a unique combination of extensive IV&V expertise, experience collaborating with states to successfully manage multiple projects, strong Medicaid credentials, and an intimate understanding of Nebraska's technological and business landscape.

As Nebraska continues to evolve further toward managed care, adding behavioral health to the delivery system, First Data has the right team to help guide you to achieve your goals of improved health outcomes, better integration and quality of care and reduced program costs. We offer the State an extremely qualified team of experts with knowledge of Medicaid enterprise systems, CMS certifications and the State of Nebraska human services operations. We stand ready to assist you as your partner for the years to come.

First Data is intimately aware of the challenges and complex considerations facing DHHS because of our history with Nebraska, and other states in the strategic planning, development, implementation, and operations of large, complex healthcare systems. Some of these challenges include:

- **Effectively meeting all federally mandated requirements while also implementing a new Medicaid Eligibility and Enrollment System** – We are fully aware of CMS requirements and can provide confiramtion that the new Medicaid Eligibility and Enrollment System meets these federal standards.
- **Increasing pressures to improve efficiency of operations and provide better service to the public** – We understand the business needs driving this project and the need to provide operational improvements. We realize the Department is looking to do this by aligning with the MITA 3.0 standards and the Seven Standards and Conditions to promote the interoperability between State systems, and desiring to progress to target MITA maturity levels. We will leverage the MECT v.2.0 as a tool to report progress on the integrity and functionality of Medicaid enterprise system development to CMS.
- **Need for flexibility in business operations** – We understand the challenges faced by agencies in today's rapidly changing program environments. Systems must be

able to quickly respond to legislative or programmatic changes, such as Health Care Reform, otherwise cumbersome work arounds may be required to correctly determine and administer Medicaid enterprise systems and processes.

- **Coordinating project efforts with many stakeholders involved** – Because we have worked with other states that are undergoing wide-spread system changes, we appreciate the importance of working closely with all stakeholders across multiple organizations that service the same clients. We already have the established relationships required with the project stakeholders and federal partners to foster expediency in the review process. In addition, the project must manage input from multiple legislative initiatives and be accountable by providing timely and accurate information as the legacy replacement project progresses. We want the IV&V experience to include lessons learned across all initiatives and for the State to actualize the benefit of having a consolidated IV&V provider to support accountability.

- **Securing project success** – Historically, IT projects across the country tend to experience schedule slippages, budget overruns, and failure to meet end-user expectations. As a result, we have gained a deep appreciation for the long-term implications of the decisions that are made early in the process and can help the Department while enforcing the processes and standards that work well. As with the current First Data EES IV&V Team, we will continue to focus each project implementation on achieving stated outcomes. In addition, we will align objective based assessments to DHHS strategic goals via program oversight.

First Data has a long history of partnering with government clients in their efforts to plan and manage the replacement of large legacy eligibility systems, including several recent, large-scale, complex HHS projects, examples of which are included as project samples in our summary of corporate experience section. Below we highlight some of the advantages our extensive experience brings to the EES and DMA Projects:

- **We know more than any other vendor about Nebraska's EES implementation** - Having been Nebraska's trusted IV&V vendor for the last two years, we are uniquely poised to resume our responsibilities---on Day One, thus mitigating any scope, schedule or cost risk Nebraska might experience through transitioning to another vendor. We have worked with the State, Wipro and CMS through the requirements and design phases and understand the risks, rewards, and strategic imperatives set forth by DHHS. Our knowledge and experience is augmented by staffing *100% of the EES team with skilled practitioners who have practical Cúram implementation experience*. In addition, our Executive Oversight (Kelly Tinsley), Privacy and Security SME (Albert Decker) and our Center of Excellence (COE) staff have participated in multiple Cúram implementations for integrated eligibility.

- **We understand Medicaid Enterprise Systems** – First Data has helped many Medicaid agencies plan, procure, and implement complex systems, providing a deep and broad understanding of various Medicaid enterprise administrations, the

corresponding programs, and the interrelations between the programs and various interfaces.

- **We understand the programs *AND* the data** – First Data has worked with all of the major health and human services programs, and while the EES Project supports Medicaid eligibility, we understand how the various related programs intersect and support DHHS's overarching vision. We have a very good understanding of the programs, policies, and business processes associated with all of these programs and can bring best practices from other states. Our proposed team brings the right skills and experience to support your vision. We also understand how the data intersects between all of the programs, and we will bring that knowledge to bear during the development of the Data Management and Analytics system.

- **We are fiercely independent** – First Data has extensive experience as an independent advisor on system development and implementation projects. First Data does not prefer any solution or solution provider, but has worked with most of the current systems or approaches in an independent capacity. We will have no agenda other than the successful design, development and implementation of DHHS Projects.

- **We are industry leaders in IV&V** – The First Data Team has a long list of successful IV&V projects involving government information systems. **Our list of clients includes 50 government QA/IV&V projects.** This has included some of the largest and highest-profile projects in the country and has enabled us to gain valuable lessons learned from other states that can help the State as it makes this significant transformation. As a result, we have seen what works well and we know things to watch out for as the project progresses. Our role has taken many different forms and responsibilities over the lifecycle of the projects, depending on the specific milestone or work product developed, but we have always maintained our commitment to meeting the needs of the project with dedicated staff and proven tools and methodologies.

- **We have a history of successful projects** – Perhaps the greatest testament to the quality of our work is the number of clients that have asked us to continue supporting their project after the conclusion of our original contract. Twenty (20) of First Data's large system projects have involved an IV&V role after performing the initial planning/procurement, or have involved a significant contract extension in order to increase the scope of the effort. We recognize that states have options when selecting a partner for their projects, and we are honored that so many of them have continued to select us after working with us. The long-term nature of our client engagements and the re-selection of the First Data

First Data's methodology brings the IV&V framework Nebraska needs:

- ✓ *Accommodates a portfolio of projects*
- ✓ *Identifies cross-project risks*
- ✓ *Streamlines review processes*
- ✓ *Reinforces relationships with Stakeholder agencies*

Team through multiple re-procurements demonstrate the trust our clients have in us as a partner that delivers on its commitments.

First Data has carefully reviewed and understands the requirements set forth and looks forward to working with you to verify that Nebraska's IT vendors are making systematic, steady progress toward implementing the necessary tools and technology for the DHHS. The First Data Team is uniquely qualified to be the partner Nebraska needs to help DHHS achieve its objectives. Given the opportunity, we believe our involvement will be a key element of success for all your projects. We bring an integrated IV&V methodology previously applied to the largest system integrators in the country (Accenture, Deloitte, Xerox) which we have adapted to manage a program portfolio of interdependent projects such as those proposed. In addition, you will benefit from our position as a national leader in the area of Medicaid systems, allowing us to bring many years of experience and project success to your program.

Corporate qualifications are important, and while we are proud of ours, we know that the qualifications of the people on the ground working with you to actually deliver the project are the most important. From our pool of accomplished resources, we will bring to you a skilled team with the right mix of Nebraska knowledge, Cúram implementation expertise, Medicaid program expertise, deep technical knowledge and an accomplished track record helping states implement complex health and humans services systems. Our team's current support of the EES Project will be leveraged to minimize any transition to a new implementation contractor, allowing DHHS management to continue to focus on implementation activities.

First Data's Nebraska roots run deep and we very much appreciate the opportunity to partner with you on this program that is so vital to the health and welfare of the people of Nebraska. In the pages to follow, we clearly demonstrate why First Data is the best choice for making the DHHS enterprise improvement programs a success for all Nebraskans.

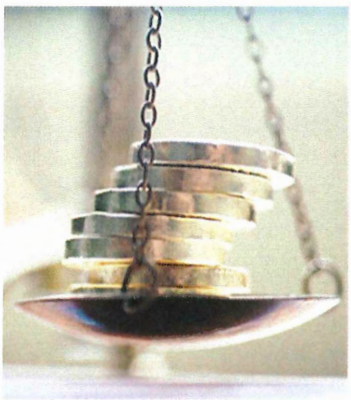
2.1 Bidder Identification and Information

The table below documents our company information.

Requirement	First Data's Information
Full company or corporate name	First Data Government Solutions, LP
Address of company's headquarters	5565 Glenridge Connector NE Atlanta, Georgia 30342
Entity organization	Limited partnership
State of incorporation	Delaware
Year of incorporation	2004
Has name and form of organization changed since first organized?	No

Table 2.1 – First Data's Bidder Information

2.2 Financial Statements



First Data Government Solutions, LP is the government facing business component of First Data Corporation, a Fortune 500 company ranked #1 in Financial Data Services. As the global leader in transaction processing and services for financial institutions, retailers, and government organizations, Nebraska and DHHS can trust that in addition to being a well-rounded and highly qualified company, First Data is also a financially stable organization. In October 2015, First Data became a publicly traded company. The company has strong financial backing, solid revenue growth, ample liquidity, and significant headroom to fund all its operations. We continue to be confident in our business model, well-balanced revenue base and market-leading position.

We have provided last year's audited financial statements as Appendix 1.

Our financial organization representative is:

Mr. Shane McCullough
6802 Pine Street Omaha, NE 68106
402-222-3397
shane.mccullough@firstdata.com

First Data has had no judgments, litigation, or financial reversals which might materially affect the viability or stability of our organization.

2.3 Change of Ownership

First Data Government Solutions, LP does not anticipate any change in ownership or control during the twelve (12) months following this proposal's due date. We understand that the State should be notified of any change or ownership to an awarded vendor.

2.4 Office Location

First Data's corporate headquarters is located in Atlanta, Georgia. We also have a large office location in Omaha Nebraska, as well as Cincinnati Ohio, Roseville California, and Englewood Colorado. If a contract is awarded for this project, our location responsible for performance of the contract would be the Omaha office, located at 6902 Pine Street.

2.5 Relationships with the State

First Data Government Solutions, LP was awarded a contract with Nebraska's Department of Health and Human Services for Eligibility and Enrollment Solution (EES) Independent Verification and Validation (IV&V) Services in January 2014. The contract number is 58755 O4. This contract will expire on June 30, 2016.

In addition to the contract referenced above, First Data has a large presence in Omaha, Nebraska. First Data opened an office in Omaha in 1971. We currently have 8 buildings, totally 1.5 million square feet of real estate. First Data employs over 5,400 employees in these Omaha locations. Our long history and presence demonstrates our commitment to the State and its various projects and endeavors.

2.6 Bidder's Employee Relations to State

To the best of our knowledge, no party named in our proposal response is or was an employee of the State within the past 24 months.

To the best of our knowledge, no employee of First Data Government Solutions, LP is an employee of any agency of the State of Nebraska.

2.7 Contract Performance

First Data has not had a contract terminated for default during the past five (5) years.

First Data Government Solutions, LP has had two (2) contracts terminated for convenience during the past five (5) years:

- **Louisiana Department of Health and Hospitals**: The Government Product Solution Division of First Data Government Solutions contracted with the State of Louisiana to implement First Data's Whole Healthcare product (AuthentiCare®). The State decided not to implement AuthentiCare ® as its EVV services, and stayed with their legacy vendor of 10 years. *(Termination for convenience – September 2015)*

- **New Mexico Human Services Department**: The State of New Mexico decided to terminate for convenience the Fixed Price PMO contract for both Medicaid and Child Support Enforcement system replacement. The State is utilizing a Time & Materials, Staff Augmentation model for the Medicaid PMO services and, due to budget constraints, is reevaluating next steps for the State's Child Support Enforcement system replacement strategy. *(Termination for convenience – April 2016)*

2.8 Summary of Corporate Experience

First Data provides the following three (3) projects to demonstrate our experience on projects similar to the EES and DMA projects.

Arkansas Department of Human Services (ADHS)	
Arkansas Eligibility Independent Verification and Validation (IV&V) Project	
Project Overview	First Data monitored and assessed the Software Development Life Cycle (SDLC) and the products that defined the Eligibility and Enrollment Framework (EEF) Project to

Arkansas Department of Human Services (ADHS)			
Arkansas Eligibility Independent Verification and Validation (IV&V) Project			
	make sure it fulfilled Federal and State project requirements.		
Planned Contract Dates	March 2013 – December 2015	**Actual Contract Dates**	March 2013 – December 2015
Planned Project Budget	$3,026,925	**Actual Project Budget**	$2,958,750
Summary of Services	• Quality Assurance • BPR	• IV&V • CMS Grant Support	
Project Description	First Data monitored and assessed the Software Development Life Cycle (SDLC) and the products that defined the Eligibility and Enrollment Framework (EEF) Project to make sure it fulfilled Federal and State project requirements. Utilizing IBM's Cúram Framework, First Data worked with DHS and the Enterprise Program Management Team (EPMT) to navigate the Center for Medicare and Medical Services (CMS) attestation and gate review processes. Services provided included the following: **Quality Assurance/IV&V** • Assessed the quality of the product as it was developed by formal review and assessment of design deliverables to identify potential discrepancies from established requirements and standards. • Reviewed testing procedures and results from the DDI and State testing teams to determine completeness and compliance with pre-defined test criteria, identify deficiencies and confirm cohesive interaction between required project teams. • Collaborated with ADHS and the EPMT to prepare for and navigate through CMS required system attestations and gate review process successfully by following the CMS Enterprise Life Cycle. **Technical Quality Assurance Support** First Data provided dedicated resources to observe the EEF project technical team operation by: • Monitoring Affordable Care Act (ACA) compliance and attainment of ADHS functional requirements. • Providing consultative input to the Enterprise Program Management Team (EPMT) / Project Management Office (PMO) and ADHS project leadership, as deemed necessary. • Confirming that risks were identified and managed in a timely manner. • Providing specialized assessment focused on: 1) security compliance and 2) test planning and test management. **Business Process Reengineering Quality Assurance Support** First Data provided dedicated resources to observe the EEF project teams by: • Concentrating on rapidly reengineering operational service delivery processes to monitor ACA compliance and adherence to the business architecture selected by the governance board.		

Arkansas Department of Human Services (ADHS)		
Arkansas Eligibility Independent Verification and Validation (IV&V) Project		
		• Providing consultative input to the EPMT / PMO and ADHS project leadership, as deemed necessary. • Verifying that risks were identified and managed in a timely manner. • Providing specialized independent assessment focused on: 1) Client and User Support Contact Center design and implementation and 2) Organization Change Management (OCM) implementation. **Project Integration IV&V / Quality Assurance Support** First Data provided dedicated resources to support IV&V and enhanced program management level Quality Assurance support to ADHS that: • Monitored effective integration between the Eligibility and Enrollment Framework, Arkansas Health Insurance Partnership Exchange and the Health Care Independence Act Medical Frailty determination and Shopping Experience projects. • Worked collaboratively with CMS to verify that federal and state stakeholder interests were addressed promptly.
Client Contact	Name	Tim Lampe, Arkansas DHS
	Position	Project Director, Program Management Office Department of Human Services
	Address	Donaghey Plaza North, Slot 5401 P.O. Box 1437 Little Rock, AR 72203-1437
	Phone	(501)320-3988
	Email	Tim.Lampe@dhs.arkansas.gov

Connecticut Department of Social Services (DSS)			
Connecticut Modernization Consulting Services for Project Management and Quality Assurance			
Project Overview	Connecticut DSS delivers public assistance and employment services for Medicaid, TANF, Food Stamps, and related Child Care Programs and services. The Department serves a caseload of 390,000 and 3,000 staff in 25+ locations. The Eligibility Management System (EMS) has been supporting the Department for over 20 years and is constrained by its technology. DSS embarked on a Modernization effort utilizing First Data to provide Strategic Planning and Procurement services. The planning and procurement was successfully completed with the design, development, and implementation phase initiated November 2011. First Data continues to provide Quality Assurance services throughout the implementation phase. Estimated completion is end of 2017.		
Planned Contract Dates	November 2011 – October 2017	**Actual Contract Dates**	November 2011 - Present
Planned Project Budget	$18.4 million	**Actual Project Budget**	Project is currently on budget

Connecticut Department of Social Services (DSS)	
Connecticut Modernization Consulting Services for Project Management and Quality Assurance	
Summary of Services	• Project Management • Quality Assurance / Quality Control • Business Process and Technical Architecture • Telephony / Call Center / IVR
Project Description	First Data provides project management and quality assurance during the design, development and implementation phase of the Modernization project. This includes: ***Deliverable Management*** • Verify Deliverable Expectation Document (DED) for each deliverable captures the State and the Prime Vendor's mutual understanding of the scope, objectives, content, and format of each deliverable. • Support the client during Contractor walkthroughs of each deliverable, to clarify content, answer questions, or to familiarize the project team with the deliverable. • Provide formal review and written comments on deliverables by key project stakeholders, with the use of a standardized matrix to document comments. • Confirm Contractor submittal of draft and final versions of each deliverable accommodate appropriate revisions, corrections, or other changes requested by the Department. • Confirm formal written acceptance of project deliverables by the State Project Manager, IT Technical Program Manager, and the Modernization Project Sponsor. • Archive all project deliverables in the State's project library and verify adherence to all configuration management processes. ***Risk and Issue Management*** • Risk and Issue Identification and Assessment - Assist in the identification, assessment, and prioritization of all project and project-related risks and issues. Assist in developing the coordinated and effective/efficient application of resources to minimize, monitor, and control the probability and/or impact of each risk and issue. • Risk Mitigation - Assist in the development of mitigation measures, formulated according to one or more of the following major risk options: ✓ Design a new business process with adequate built-in risk control and containment measures from the start. ✓ Periodically re-assess risks that are accepted in ongoing processes as a normal feature of business operations and modify mitigation measures. ✓ Avoid risk altogether (e.g. by closing down a particular high-risk business approach). • Review and Evaluation of the Risk Management Plan - Confirm applicable and effective security controls for managing the risks. Throughout the life of the Project evaluate whether the previously selected security controls

Connecticut Department of Social Services (DSS)

Connecticut Modernization Consulting Services for Project Management and Quality Assurance

are still applicable and effective; and evaluate the possible risk level changes in the business environment.

Requirements Validation

- Assist in mapping functional, technical and interface requirements to high-level Proposal requirements and project objectives; and in the identification of other related elements, for example, constraints, schedules, multiple system dependencies, etc.
- Verify documented requirements and supporting documentation have included each of the appropriate types of requirements.
- Assess verification of each requirement, identifying the verification technique and facilities and equipment required.
- Level requirements according to system and system sub-divisions, confirming that all requirements are written at the right level and can be traced back to their origins.
- Verify all relevant assumptions are clearly documented and agreed upon.

Requirements Traceability, Quality Assurance / Quality Control

- Review and Evaluation of Requirements Traceability Process and Artifacts - Confirm both the process and traceability matrix will properly document the life of a requirement and provide bi-directional traceability between various associated requirements. Confirm the process and artifact (s) enables the client and/or sponsor to find the origin of each requirement and tracks all changes made to all requirements.
- Traceability Quality Assurance - Verify all requirements are properly included and documented at the appropriate level. Identify items that do not trace, incorrectly trace, or do not sufficiently trace. Identify any missing, additional or ambiguous requirement to avoid future problems in design. Confirm traceability artifacts are maintained and used as designed during all project phases; requirements, design, testing and closeout.
- Tracing Issues - Confirm any tracing issues, problems, or questions generated by the traceability analysis have an agreed upon resolution. If appropriate, verify documentation (or requirement) updates are completed to prevent future issues and confirm documentation of the resolution points to or resides with the traceability analysis.

System Test Quality Assurance / Quality Control

- Review System Test Deliverable, all work plans, test plans, requirements documents, use case documents, test scenarios, etc., to confirm full documentation of the procedures to be used in System Test.
- Verify exit criteria is agreed upon and clearly documented. Confirm the

Connecticut Department of Social Services (DSS)

Connecticut Modernization Consulting Services for Project Management and Quality Assurance

scope of the test method is clearly defined, and any aspect included in the scope is accurate and repeatable through validation. Confirm all test plans have been properly traced back to business and technical requirements. Execute environment validation and smoke test and verify technical defects have been fixed. Confirm documented results are reviewed and reflect actual testing outcomes.

- Facilitate the System Test Go/No-Go session as the promotion to the User Acceptance Test environment is finalized.

User Acceptance Test (UAT) Planning, Execution and Management

- Verify product is Green Light and User Acceptance Sign Off ready at UAT completion, that all defects are fixed prior to production release or have an agreed upon plan to fix, and that Executive Management is fully informed of progress and issues at all times.
- Monitor the completion and delivery of all post-implementation fixes.
- Develop the draft *Project User Acceptance Test Plan* deliverable for review and approval. Including management reporting requirements and report templates.
  - ✓ Develop the draft *User Acceptance Test Business Scenario*.
  - ✓ Track development of the test caseload to completion and verify proper coverage for testing.
  - ✓ Develop the UAT Kick Off deck, training materials, roster, schedule, test process templates and instructions, and technical supporting documentation.
  - ✓ Identify the tester skill set and representation required to verify the composition of the team adequately reflect a cross section of the end user community.
  - ✓ Review the Production Cutover Plan to verify its adequacy.
- Conduct UAT Process, Incident Tracking Tool, and Application Training for the UAT team to verify team members understand the function and use of all templates.
- Initiate scenario assignments, confirm documented results reflect actual testing outcomes, monitor percent to completion, including re-tests, and track to overall completion of plan.
- Confirm timely, accurate and complete defect and change request reporting in project Incident Tracking Tool and facilitate daily testing debrief with UAT Team and the developer.
- Compile nightly UAT Management Reports, as agreed upon in the Approved *Project User Acceptance Plan*.
- Facilitate the UAT Change Prioritization session and verify the application changes recommended by the UAT Team are prioritized by mutual consensus.

Connecticut Department of Social Services (DSS)

Connecticut Modernization Consulting Services for Project Management and Quality Assurance

- Upon the successful completion of UAT, facilitate the UAT Green Light (Go/No-Go) session.

Implementation Planning and Support

- Assist the client in the planning and logical sequencing of implementation events as determined by the Project Work Plan phases and milestones. Assist in the identification of implementation risks and mitigation strategies. Assist in planning management brainstorming sessions, communication and event planning and development of presentation materials. Participate in stakeholder informing sessions, both internal and external, as requested. Review all project system training deliverables to confirm adherence to Approved Project Management Plan and proper integration and consideration of overall Project development schedule.
- Assist the client in the identification of change management impacts, especially those high impact areas, and the prioritization of the associated process mapping. Assist in the planning required for prioritizing the development and approval of all process changes. Assist in the identification of affected stakeholders (internal and external), and related training and communication requirements.

Project Closeout Support

- Review the Project Close Out Report and confirm the report properly documents the turnover of all project deliverables, closes out all financials, certifies all project records are updated, completed and properly archived, project successes and lessons learned are well documented, and the completed Project Close Out and Transitions Check List is included.
- Verify support for the development and approval of the Post Implementation Evaluation Report (PIER), as necessary.

Additional Services

Business Process Re-Engineering Support and Quality Assurance Outcomes

- Identify, prioritize and develop all required Maintenance and Operations (M&O) project procedures.
- Establish an on-going Change Control process for all items subject to configuration management.
- Developing corrective action plans.

Call Center Telephony Systems Engineering Support and Quality Assurance

- Call Center and IVR Planning - Support the planning of the Project Interactive Voice Response (IVR) and Call Center telephony architecture

Connecticut Department of Social Services (DSS)		
Connecticut Modernization Consulting Services for Project Management and Quality Assurance		
		and application: ✓ Perform special studies, assessments and/or surveys. ✓ Support bid specifications process, including statement of work reviews. ✓ Research and compile Call Center and IVR technical information. • Call Center and IVR Design - Support the design of the Project Interactive Voice Response (IVR) and Call Center telephony architecture and application. ✓ Support all business and technical requirements and design sessions. ✓ Review system business requirements and design documentation. ✓ Review technical architecture requirements and design documentation. ✓ Participate in all business continuity planning and provide technical architecture performance assessments. ✓ Determination of appropriate Telco/Data equipment. ✓ Determination of appropriate power requirements. • Call Center Space Planning; Site Preparation and Installation Planning and Management Support - Support the steps required to select Call Center facility locations. ✓ Facilitate site selection evaluation process. ✓ Planning and development of Call Center staffing plans. ✓ Development/management of the Site Preparation/Installation Plan. ✓ Coordination of all site preparation and installation activities. ✓ Development of Call Center Operational Procedures Guide. ✓ Identification of post implementation corrective action initiatives. ✓ Review system reports to identify trends and anomalous data. ✓ Analyze information and draw valid conclusions.
Client Contact	Name	Vance Dean
	Position	CIO, CT Department of Social Services
	Address	25 Sigourney Street Hartford, CT 06106
	Phone	860-424-5508
	Email	Vance.dean@ct.gov

Indiana Family and Social Services Administration	
Indiana Eligibility Determination Services System (IEDSS) IV&V	
Project Overview	The Family & Social Services Administration (FSSA) is a health care and social service financing agency that delivers a variety of services to its citizens in need. There are over one million Hoosiers that receive services from FSSA. This represents

Indiana Family and Social Services Administration

Indiana Eligibility Determination Services System (IEDSS) IV&V

about 1/6th of the State's population.

The agency has initiated a project to modify and then replace its eligibility system in two phases:

- Phase 1 involves implementation of a business rules engine and modification of the legacy system to support Medicaid MAGI eligibility determination and other ACA requirements by October 2016
- Phase 2 includes replacement of the legacy system, incorporation of full functionality, and achieving federal certification by December 2017

The new IEDSS will be a custom, web-based portal solution that is accessible by external applicants, social service agencies, caseworkers and other stakeholders, integrated with approved support tools to support State and county staff, processing, and communication to the various related State and federal systems. The Federal and State programs in the scope of the IEDSS solution include:

- Cash Assistance
  - ✓ Temporary Assistance for Needy Families (TANF)
  - ✓ Refugee Cash Assistance (RCA)
- Healthcare Assistance
  - ✓ Medicaid
  - ✓ Children's Health Insurance Program (CHIP)
  - ✓ Hoosier Healthwise
  - ✓ Healthy Indiana Plan (HIP)
  - ✓ Presumptive Eligibility for Pregnant Women
- Supplemental Assistance Programs
  - ✓ Residential Care Assistance Program (RCAP)
  - ✓ Supplemental Assistance for Personal Needs payments (SAPN)
- Indiana Manpower and Comprehensive Training (IMPACT)
- Supplemental Nutrition Assistance Program (SNAP)

First Data is a prime contractor on this project, and Logic House is a subcontractor.

Planned Contract Dates	December 2012 – December 2017	**Actual Contract Dates**	December 2012 - Present
Planned Project Budget	$4.64MM	**Actual Project Budget**	$7.67MM (expanded services and project extension)
Summary of Services	• IV&V • UAT Support	• Federal Review Support	

Project Description

First Data is providing IV&V services during the design, development and implementation of the IEDSS project. This includes:

Project Planning

- Verify that DDI Contractor Project Management plans are in place and maintained under an appropriate level of control.

Indiana Family and Social Services Administration

Indiana Eligibility Determination Services System (IEDSS) IV&V

- Validate that the DDI Contractor Project Management plans address requirements traceability, escalation procedures, risk analysis, issue management which follow appropriate standards and are aligned with RFP requirements.
- Verify that appropriate system environments are in place and are maintained in accordance with the appropriate RFP technical foundation requirements, as updated through requirements validation and design phases of the project
- Verify that the DDI Contractor's Detailed Project Work Plan addresses each phase of the System Development Life Cycle (SDLC).
- Verify the DDI Contractor's Work Breakdown Structure (WBS) facilitates verifying and controlling project scope.
- Verify that decisions are documented, archived, and manageable for future reference.
- Verify status reporting mechanism is in place which presents various levels of detail appropriate for the various Agency and federal management tiers, including the Project Management Office, DFR, OMPP, FSSA Executives, FNS, and CMS.

Requirements Validation

- Verify that the processes and procedures for managing requirements are in place and appropriate.
- Verify that requirements can be traced through design, code, configuration and test.
- Validate that requirements of the system satisfy State and Federal regulations, including but not limited to CMS MITA 3.0 requirements.
- Verify that all business and technical requirements have been allocated to the appropriate DDI Contractor sub-system or business area.

System Design Verification

- Verify that the DDI Contractor's design and analysis process is in place and used to develop the design.
- Verify data interfaces and integration with the overall system design.
- Verify that business and technical requirements can be traced forward to system and business area design elements.
- Verify that required processes and tools are in place in accordance with the appropriate RFP business and technical requirements, as updated through requirements validation and design phases of the project.
- Verify that all DDI Contractor design products are under configuration control.
- Verify DDI Contractor design standards, methodology and tools used to develop the design are in place and appropriate for the tasks at hand.
- Validate the project policies and procedures for verifying that the system is

Indiana Family and Social Services Administration

Indiana Eligibility Determination Services System (IEDSS) IV&V

secure meets the State's IT security requirements, and verify that the privacy of client data is maintained through these policies and procedures.

- Verify the DDI Contractor's project security plan and risk analysis processes comply with the State's IT security requirements.
- Verify that the DDI Contractor's processes and equipment are in place to back up client and project data and files and archive them safely at appropriate intervals,
- Verify that the agency hosting the IEDSS system (Indiana Office of Technology - IOT) is implementing IT security processes as required, and that there are no deficiencies in IOT's security processes for the IEDSS where Federal (e.g. HIPAA) and State laws might impose security requirements.

Construction and Testing

- Verify that the Master Test Plan meets IEDSS requirements, is appropriate for the IEDSS project, and is being used by the DDI Contractor to actively guide the DDI Contractor's approach to testing throughout the life cycle of the project.
- Verify the software artifacts, system documentation, test data, and the test plan confirms a robust and complete migration capability.
- Validate that the results of the test are providing solutions as expected.
- Verify adherence to Application Architecture Standards as outlined in the RFP.
- Verify the contractor is monitoring activities during the Construction and Unit Testing task using technical reviews and audits.
- Verify the contractor's prepared comprehensive set of test scenarios, with applicable test cases and expected test results to test the migration, and conversion of all data and files.

Data Conversion Verification

- Verify that DDI Contractor has demonstrated that all data required to support processing is available, accurate, and ready for operations.

Integration and System Testing

- Validate the plans, requirements, environment, tools, and procedures used for unit, integration and system testing of system modules.

User Acceptance Testing

- Provide the knowledge and staff to plan, execute and assess the results of user acceptance tests including:

✓ Planning the acceptance test strategy and process
✓ Developing use cases

Indiana Family and Social Services Administration		
Indiana Eligibility Determination Services System (IEDSS) IV&V		
		✓ Creating test data ✓ Executing user acceptance tests ✓ Tracking actual test results to expected results ✓ Monitoring software defect correction ✓ Iterative execution of appropriate tests and regression testing, as necessary ✓ Reporting on test results from appropriate test cycles ✓ Validate that the system design and system functionality agree with the Stakeholder expectations as expressed at the conclusion of Requirements Validation and Design approval ✓ Validate that the operational environment delivers its services in accordance with the agreed upon requirements, design and applicable key performance measures ✓ Validate that the business functions are supported by the system in accordance with the agreed upon requirements, design and testing documentation ✓ Verify the functional area checklist for Operational Readiness has been applied and go/no-go criteria have been met **Pilot and Implementation Validation** • Validate the DDI Contractor has demonstrated and verified physical security, data security, and fire and disaster prevention and recovery procedures. **Federal Review Support** • Verify the DDI Contractor is utilizing all appropriate federal guidelines for Medicaid technology and systems projects, including but not limited to, the Enhanced Funding Requirements: Seven Conditions and Standards Medicaid IT Supplement (MITS-11-01-v1.0) throughout the DDI lifecycle. • Develop Federal Review Plan in coordination with the State and the DDI Contractor to outline the processes and procedures that will be used to manage system review activities. • Define requirements for all federal review guidelines during and after system implementation. • Verify the system solution meets criteria for federal compliance by reviewing and providing a written assessment of all gate review and compliance materials produced by the DDI Contractor in advance of federal gate reviews and post-implementation review activities. • Verify documentation for federal gate reviews and system compliance activities, including a Compliance Validation Report validating that all federal requirements have been met and documented.
Client Contact	Name	Sunshine Beam
	Position	FSSA/DFR Manager of Eligibility Systems

Indiana Family and Social Services Administration		
Indiana Eligibility Determination Services System (IEDSS) IV&V		
	Address	402 W. Washington Street, Room W392 Indianapolis, IN 46207
	Phone	317-650-0819
	Email	sunshine.beam@fssa.in.gov

Additional Relevant Experience

One of the key focus areas of the First Data professional services team is health care, with particular emphasis on the Medicaid program and its systems. As a result, we have a very good understanding of the programs, policies, processes, and types of systems involved in this project. For this project, First Data brings a strong combination of eligibility and IV&V expertise with hands-on MITA and Medicaid experience. The following table highlights the services provided by First Data in support of health care programs.

First Data's Health Care Experience		
Project Type	**Description Of Work Performed**	**Where Performed**
Health Insurance Exchange	Conduct system planning, analysis, requirements development, RFP development, grant writing, and procurement support, project management, quality assurance and technical support for a state health insurance exchange.	• Arkansas • California • Colorado • Connecticut • Idaho • Illinois • Indiana • Oregon
MMIS-Related Projects	Assisted several states in their efforts to replace their legacy Medicaid Management Information System, implement new system components, or oversee fiscal agent operations. Services provided include: • Alternatives analysis/feasibility studies • Requirements development • RFP development and procurement support • Business Transformation IV&V/QA during design, development, and implementation • Operational Quality Assurance	• Indiana • Florida • Louisiana • Maine • Massachusetts • Michigan • Nebraska • New Mexico • North Dakota • Ohio • Texas
Medicaid Policy and Program Analysis	Provided independent analysis of current Medicaid policies, rules, and regulations, including recommendations for process improvements.	• Alabama • Michigan
Medicaid Eligibility	Supported multiple eligibility system projects by performing activities that cover the entire system	• Arizona • Arkansas

First Data's Health Care Experience		
Project Type	**Description Of Work Performed**	**Where Performed**
Projects	lifecycle: • Alternatives analysis/business case development • Business process analysis and reengineering • Requirements development and analysis • RFP development and procurement support • Independent testing • Project Management • Training • Implementation support • IV&V/QA during design, development, and implementation • Operational Quality Assurance	• California Welfare System Consortiums: ✓ LEADER ✓ CalWIN ✓ C-IV ✓ ISAWS • Colorado • Connecticut • Indiana • Nebraska • New York • Ohio • Oklahoma • South Dakota • Virginia • Washington
Health Care Payment Reform	Conducted studies with health insurers and state government to explore opportunities for using health information technology to achieve real-time eligibility verification and claim adjudication.	• Vermont • Cerner (health insurer) payment reform pilot
Medicaid/ Consumer Directed Care Time & Attendance Tracking Systems	Implemented automated point-of-service IVR/Web tracking and billing systems for home and community-based services. The systems are used in support of case managers, program administrators, and providers that provide direct electronic billing to Medicaid and other third party payers.	• Florida • Kansas • Michigan • Oklahoma • South Carolina
Medicaid IVR/Web Systems	Performed multiple projects involving Medicaid eligibility Interactive Voice Response (IVR) systems. The projects include designing, developing, implementing, and maintaining eligibility IVRs. Also conducted analysis of a Medicaid provider call center.	• Georgia • Minnesota • Ohio • South Carolina
Public Health Systems	Conduct system planning, analysis, requirements development, RFP development, procurement support, project management, quality assurance and technical support for a statewide project to implement the CDC's National Electronic Disease Surveillance System (NEDSS) in compliance with the Public Health Information Network (PHIN) architecture and recommendations.	• Maine
Public Health IVR Systems	Interactive Voice Response (IVR) system for a state Immunization Program. The project included	• Ohio

First Data's Health Care Experience		
Project Type	**Description Of Work Performed**	**Where Performed**
	designing, developing, implementing, and maintaining the IVR.	
Health Care Provider Payment Processing	Payment processing for health care providers and card processing for health care flexible spending accounts.	• First Data currently works with approximately 150,000 providers

Table 2.2 – First Data's Healthcare Experience

2.9 Summary of Proposed Personnel and Management Approach

Beyond the tools, methodologies, and approaches, it is clearly the quality of the team members that will help determine success on the project. First Data prides itself on being able to offer a unique combination of business processing acumen and government programmatic subject matter expertise in order to confirm our solutions fit with the appropriate context of business needs, financial constraints, and client services.

For this particular agency initiative, First Data will assemble a team that represents the real, hands-on, practical knowledge, experience and expertise required by the specific project. Our team brings methodologies, best practices, and tools from some of the latest projects in the country. As a result, we understand what it takes to be successful and how to help DHHS implement the EES and DMA projects successfully.

All First Data consulting projects are led by Mr. David Sodergren, Vice President for First Data Government Solutions. Mr. Sodergren provides oversight and executive decision-making on project progress, resources, and budget. He also confirms DHHS' project needs are being met and that DHHS leadership is satisfied with our efforts.

Assisting Mr. Sodergren will be Ms. Kelly Tinsley, who will serve as Executive Oversight for this specific project. Ms. Tinsley's responsibility is to oversee the management of the professional services projects, specifically for Nebraska and DHHS. Ms. Tinsley will be responsible for monitoring client satisfaction and verifying adequate resource coverage to meet and exceed DHHS expectations. The organizational chart below outlines our proposed staffing for the EES and DMA projects.

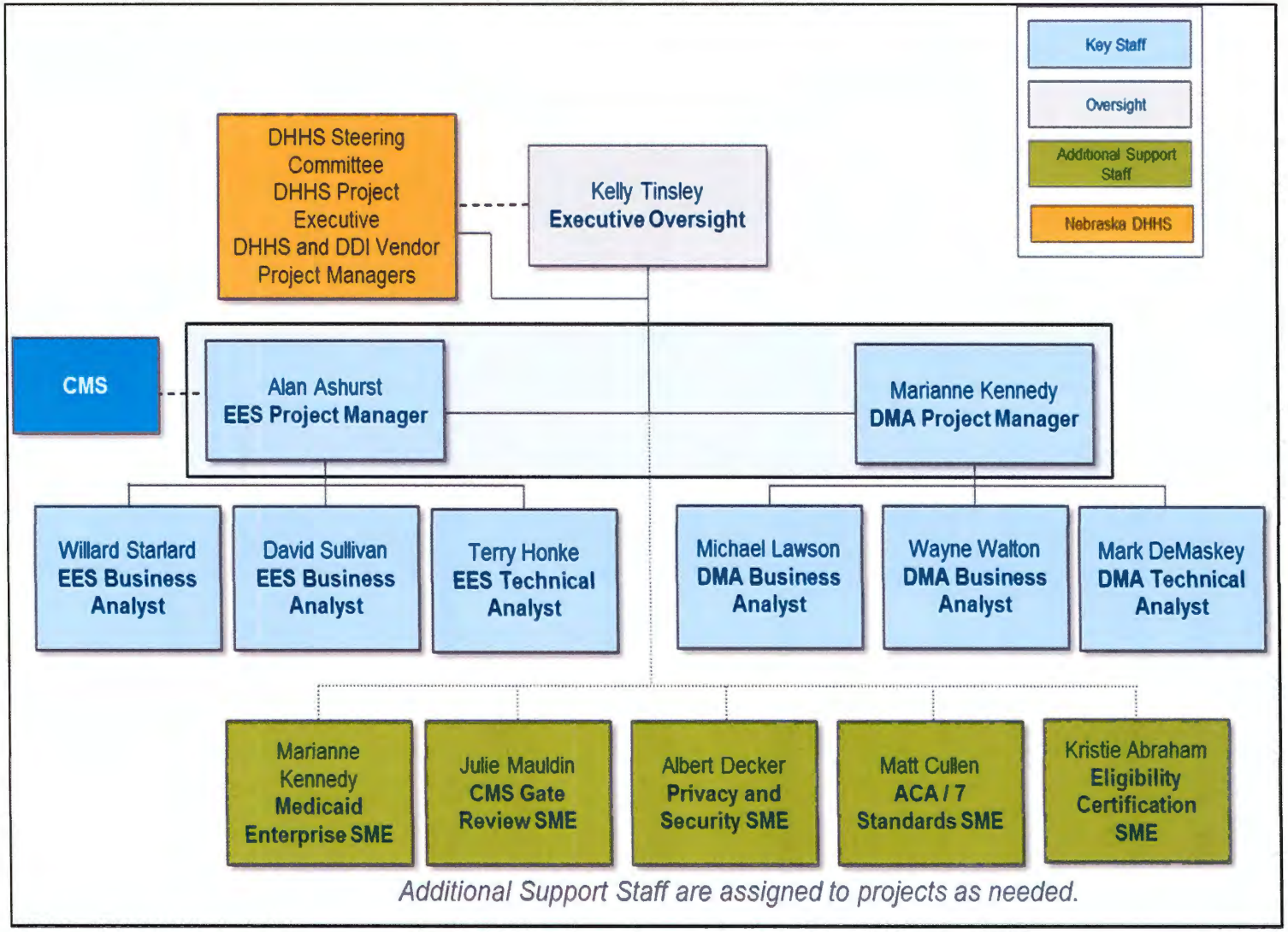


Figure 2.1: The First Data Team brings deep program and system implementation knowledge to support Nebraska's vision.

The relevant qualifications, expertise, and experience of the staff at First Data are truly unique, particularly in the areas of project management and IV&V services. Specifically, working with state government is where a vast amount of our experience lies, and we are providing an EES Team where all staff has Cúram experience. The table below details our proposed staff and their responsibilities on the EES and DMA projects. In addition, First Data understands that DHHS is considering a number of optional projects, yet to be fully defined. As outlined in the optional cost proposal, we will provide candidates aligned with project needs based on our understanding and experience that will collaborate with the EES and DMA Teams as needed.

Name	Title	Reporting To	Primary Work and Responsibility
Kelly Tinsley	Executive Oversight	David Sodergren	• Executive oversight of projects • Escalation point for client issues/concerns • Oversight of staffing • Contract management
Alan Ashurst	EES Project Manager	Kelly Tinsley	• Management of EES IV&V project schedule • Production of weekly EES status reports • Contributor to monthly status reports • Attendance at weekly project management and planning meetings
David Sullivan	EES Business Analyst	Alan Ashurst	• Assessment lead of the implementation contractor's ability to meet EES requirements • Contributor to EES-related IV&V deliverables • Support of assessment of functional work products that support business process • Support for validation of requirements • Attendance at required meetings
Willard Starlard	EES Business Analyst	Alan Ashurst	• Contributor to EES-related IV&V deliverables • Support of assessment of functional work products that support business process • Support for validation of requirements • Attendance at required meetings
Terry Honke	EES Technical Analyst	Alan Ashurst	• Validation of technical architecture for consistency with state and federal requirements, including CMS-7 and MITA 3.0 • Identification of technical risks • Contributor to implementation contractor deliverable reviews and technical portions of IV&V deliverables • Review of technical artifacts against

Name	Title	Reporting To	Primary Work and Responsibility
			enterprise architecture standards
Marianne Kennedy	DMA Project Manager	Kelly Tinsley	• Management of DMA IV&V project schedule • Production of weekly DMA status reports • Contributor to monthly status reports • Attendance at weekly project management and planning meetings
Michael Lawson	DMA Business Analyst	Marianne Kennedy	• Assessment lead of the implementation contractor's ability to meet DMA requirements • Contributor to DMA-related IV&V deliverables • Support of assessment of functional work products that support the business process. • Support for validation of requirements. • Attendance at required meetings.
Wayne Walton	DMA Business Analyst	Marianne Kennedy	• Assessment lead of the implementation contractor's ability to meet DMA requirements • Contributor to DMA related IV&V deliverables • Support of assessment of functional work products that support the business process. • Support of validation of requirements. • Attendance at required meetings.
Mark DeMaskey	DMA Technical Analyst	Marianne Kennedy	• Validation of technical architecture for consistency with state and federal requirements, including CMS-7 and MITA 3.0 • Identification of technical risks • Contributor to implementation contractor deliverable reviews and technical portions of IV&V deliverables • Review of technical artifacts against enterprise architecture standards
Albert Decker	Privacy and Security SME	Alan Ashurst and Marianne Kennedy	• Provision of all security, privacy, and HIPAA deliverables and reports.
Marianne Kennedy	Medicaid/MMIS SME	Alan Ashurst	• Advisor to IV&V teams, State and implementation contractors on enterprise architecture concerns.
Julie Mauldin	CMS Gate Review SME	Alan Ashurst	• Support to IV&V teams, State, and implementation contractors in CMS gate

Name	Title	Reporting To	Primary Work and Responsibility
			review planning • Advisor to all parties on CMS gate review expectations • Certification lead on behalf of CMS
Matt Cullen	ACA/7 Standards SME	Alan Ashurst	• Review of project materials for conformance with ACA rules, including 7 Standards and Conditions • Support to IV&V teams, implementation contractors and State in CMS gate review planning
Kristie Abraham	Eligibility Certification SME	Alan Ashurst	• Support to IV&V teams, implementation contractors and State in supporting EES Project and eligibility certification

Table 2.3 – First Data's Proposed Staff

2.9.1 Resumes

We have provided resumes for each of the personnel proposed for these projects. Resumes can be found in Appendix 2.

2.10 Subcontractors

First Data will not be utilizing any subcontractors for the EES and DMA projects.

3
Technical Approach

3.0 Technical Approach

Our Understanding of DHHS Requirements

First Data understands that DHHS is seeking a qualified independent verification and validation (IV&V) vendor to provide IV&V services for the entirety of the projects in flight and those on the near horizon that support transition to the vision expressed by DHHS. First Data assumes complete responsibility for timely performance of contractual responsibilities in accordance with federal and state laws, regulations, policies, and procedures. We anticipate that the new MECT2 standards from CMS will apply to the EES Project, and we are prepared to assist the Department with navigating this new process. We understand there is a phased approach toward achieving DHHS' Medicaid enterprise vision. While multiple projects are identified on the current roadmap, and we have provided a menu of staff to support these future projects, we understand there are two primary projects: Eligibility and Enrollment Solution (EES) and Data Management and Analytics (DMA) as described below.

First Data understands the EES Project is in the design phase, with Wipro providing DDI (design, development, and implementation) services as the prime contractor. The DDI phase is currently estimated to take longer than expected to complete, which means the Department needs flexibility from their IV&V provider. The modernized EES solution will provide real-time eligibility determinations and support the business processes for eligibility and enrollment in Nebraska Medicaid programs using modern and lasting technologies. Upon completion of the DDI phase, we know the State wants to actualize the following outcomes:

- Improved health outcomes.
- Enhanced integration of services and quality of care.
- Emphasis on person-centered care, including enhanced preventive and care management services.
- Reduced rate of costly and avoidable care.
- Improved financially sustainable system.

First Data also understand that the DMA module will receive data from supporting systems to facilitate robust analytics initiatives including case tracking, health outcome reporting and fraud detection. We recognize this effort is in the procurement stage and have planned our IV&V efforts to coincide with the start of the DMA implementation contractor.

First Data knows...

*IV&V is making sure the implementation contractors **DO** the right things, not **JUST** do things right.*

As a leader in providing IV&V services to state health and human services agencies, including the State of Nebraska, First Data brings a proven, disciplined approach to the IV&V services for the EES and DMA projects. Like other IV&V vendors, we base our approach on industry standards, including the Institute of Electrical and Electronics Engineers (IEEE) Standard for System and Software Verification and Validation. We also bring a team of talented and experienced consultants, with broad and deep experience in systems implementation, to apply our disciplined approach. Beyond our proven approach and talented team, however, we bring something more: a commitment to helping DHHS deliver these mission-critical systems on time and in budget.

The Strength of First Data

The following table provides insight into First Data's core strengths and how these can be leveraged to support Nebraska initiatives:

First Data Team Core Strengths	Applied Actions	Benefits to Nebraska
Best in Class IV&V Methodology and Toolset	• Completed assessment scorecards for critical MMIS checkpoints – within and across business functions • Comprehensive coverage of improvement initiative work areas, both anticipated and unanticipated • Tools and methods compatibility with common systems engineering practices inside and outside the Medicaid vendor community • Maximized efficiency of the First Data IV&V Team	• Comprehensive, consistent, professional and high-value IV&V work products created and delivered by certified professionals • Understandable IV&V findings and recommendations, fit for both leadership and technical consumption • Actionable IV&V findings and recommendations that are feasible, practical and effective • Reduction in any disruption that IV&V activities may have on the project team
Federal Requirements and Relationship Management	• Delivery of clear MITA compliance and strategy scorecard work products • Delivery of clear Seven Standards & Conditions scorecard work products • Cost Allocation Strategy Alternatives guidance • Partnership with Nebraska providing strategic guidance and communication support with CMS and other stakeholders	• Proven service competence and value with CMS: they know and trust First Data • Itemized regulatory compliance guidance, founded on proven strategies • Maximized federal funding participation for Nebraska • Reduced anxiety about federal oversight, federal strategies, and federal expectations

Table 3.1 – First Data's IV&V Core Strengths

To provide benefits such as these, First Data brings a mature and disciplined approach to providing IV&V services to confirm the compliance of all software-related items as consistent with the defined requirements. This begins with the maturation to an enterprise architecture approach, which will guide the conformance of EES, DMA, and other components to approved technologies, policies, procedures, and standards which are in alignment with the CMS Seven Conditions and Standards, such as the Modularity Condition. The First Data Team will plan, execute, and monitor all IV&V activities to run in parallel with each component's software development life cycle, and other support activities. This will maximize the realization of intended benefits sought by DHHS.

First Data understands this approach is envisioned to provide for a Medicaid ecosystem that improves the ability of DHHS to continue improving the health and wellness of Medicaid members by increasing their access to comprehensive health services in a cost effective manner and helping to reach the desired project goals of responding to the changing needs of applicants, enrollees and partners, while complying with all federal and state requirements, in a more agile manner.

First Data has a proven track record in the delivery of IV&V services for human services customers over the past 30 years. We understand our role, and how it relates to other major roles on the EES and DMA projects. We provide an ongoing, independent assessment of key elements of the projects, so State and Federal executive stakeholders have a clear, current and unbiased view of the projects' progress. Where we find areas of potential improvement, we will make the appropriate recommendations to DHHS, and work with DHHS and its selected contractors to implement them. We view the role of the IV&V consultant as an important partner to the overall success of these projects.

We align our IV&V methodology to the following Project Management standards:

- **Standard project processes as defined by the Project Management Body of Knowledge (PMBOK)** – *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Fifth Edition* reflects the collaboration and knowledge of working project managers and provides the fundamentals of project management as they apply to a wide range of projects. This internationally recognized standard gives project managers the essential tools to practice project management and deliver organizational results.

- **The phases as defined in the System Development Life Cycle (SDLC)** – A key to successful IT management is a solid project management methodology that incorporates the best government and commercial practices through a consistent and repeatable process, and provides a standard structure for planning, managing, and overseeing IT projects over their entire life cycle.

As with all of our service offerings, we align our method of delivering IV&V services with the PMBOK process groups and the CMS Expedited Life Cycle (XLC). Consistent with these processes, we initiate our IV&V services; we plan our IV&V services (create an IV&V Management Plan); we execute and control our IV&V services; and finally we conduct

proper closure of our IV&V services to verify all contractual obligations have been met. We will execute all phases of the PMBOK for each part of our IV&V engagement.

The SDLC framework provides a guide to project managers, business owners, IT executives, other stakeholders, and critical partners throughout the life of the project. This framework consists of ten life cycle phases, as shown in Figure 3.1.

As part of the Execute and Control PMBOK processes, we execute the IV&V tasks in alignment with the SDLC Phases 4 through 9. Generally, the First Data Team comes onboard after the Planning Phase has been completed by the HHS organization. However, the Project Manager should review the IV&V Statement of Work (SOW) to determine if Phases 1, 2, 3 or 10 are applicable to the current engagement and tailor our methodology to the proposal's request.

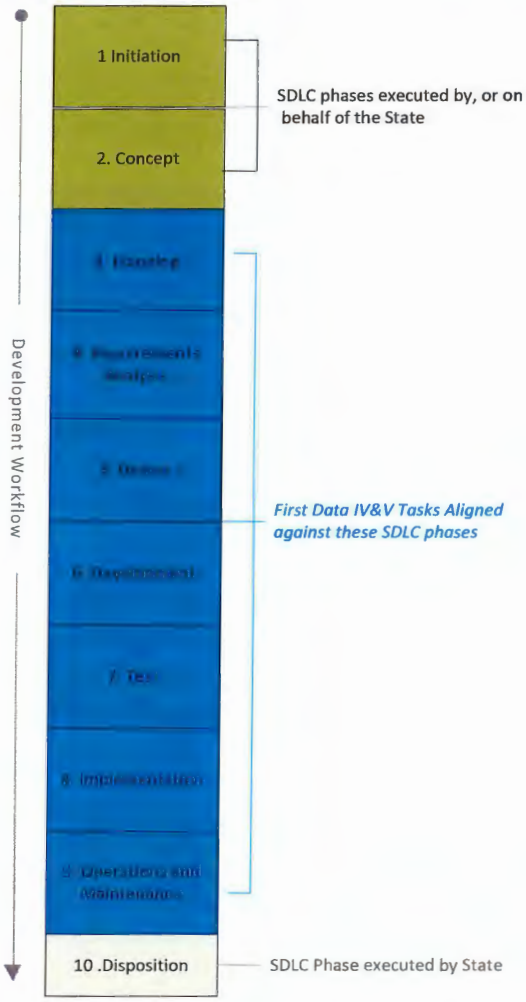


Figure 3.1: First Data aligned to the SDLC

Mitigating DHHS Transition Risks

Since February 3, 2014 the First Data Team has stood by DHHS to support the MLTC ACA Phase II implementation (EES). During these twenty-seven months we have formed invaluable relationships with the State team, with Wipro, and with the State's CMS representatives. We have collaborated throughout the engagement with the team and have adapted the delivery of IV&V services based on knowledge we have obtained and tailored to your requests. We have continually focused on the project's objectives and continue to advocate for attainment of project goals. As examples of First Data's commitment to Nebraska, we have provided valuable services beyond the scope of our contract for no charge (2 DSH and 3 PERM attestations). We know firsthand the unique challenges you have experienced, the hidden risks within the project and the technology, and the strengths and weaknesses of the project, teams and individuals. This First Data Team who you know well will remain in place and will be enhanced with staff expertise to see the EES project through to its successful completion. First Data will be able to leverage its commitment to DHHS to economize the initiation of the DMA and optional projects when they start.

A continued partnership with First Data will sustain the momentum the project currently has and will significantly mitigate risks that introducing a new IV&V vendor could introduce, including but not limited to:

- **A new Vendor will lack the understanding and knowledge of the complex architecture and systems.**

  Why First Data: Our team understands firsthand the complexity inherent in a Cúram implementation. We understand the data model, rules engine and underlying processes to guide DHHS through the remaining phases of the SDLC and we know the approach you are taking with your implementation. We know the nuances of Cúram; in fact, 100% of the EES team has conducted IV&V services on Cúram engagements. In addition, our Executive Oversight Manager (Kelly Tinsley), our Privacy and Security SME (Albert Decker) are experienced with Cúram. Further, we have worked alongside DHHS and Wipro and have a keen understanding of the strengths, weaknesses and risks associated with this complex solution.

- **A new vendor would cause a business disruption by having to orient them to the project.**

  Why First Data: We will "hit the ground running" on Day One which makes us uniquely qualified to continue to perform these services. We have established relationships with the State, vendors and CMS. There will be no "learning curve" with our team. Our team is trained, experienced and has the tools at hand to address DHHS' needs- Day One.

- **Vendor performance uncertainty.**

  Why First Data: The First Data Team, led by Alan Ashurst, is performing to the levels of quality DHHS expects. As design efforts continue for EES and DMA begins its planning phases, our known team members (David Sullivan, Terry Honke, Kristie Abraham) will work with DHHS and the expanded First Data Team to provide quality driven service in the realization of your goals.

- **High Lead Time (time and cost).**

  Why First Data: First Data understands the multiple delays that have occurred during the EES implementation. We understand the "how's," why's and basis of the Department's decisions. We also understand DHHS' focus on "getting it done right and on time." As an IV&V vendor our purpose is to provide independent and objective analysis on how well implementation vendors conduct their activities. Not having to "learn" (2-3 months conservatively) about the current project will afford DHHS an expedited process to continue the work at hand.

First Data is the partner to assist you in your continued efforts toward an interoperable state. We understand the business and technical architectures, the cultural landscape, the strategic imperatives of DHHS and the people charged with seeing this modernization to

fruition. Your schedule, scope and cost risks will be effectively mitigated through the selection of the First Data team.

The following sections provide a detailed description of our approach to delivering IV&V services to DHHS. The technical proposal is organized as illustrated as follows:

Section Number	Responses	Page
3.1	IV&V Responsibilities	58
3.1.1	Project Management	66
3.1.2	Independent Assessment and Quality Assurance	75
3.1.3	IV&V Status Meetings and Reporting	91
3.1.4	CMS and MITA Compliance	99
3.1.5	Operational and System Readiness	114
3.1.6	IV&V Deliverables and Work Products	122
3.2	Organizational Staffing	127
3.3	Logistics	149
3.4	Privacy and Security	150

Table 3.2 – Technical Proposal Organization

3.1 IV&V Responsibilities

Achieving the Nebraska DHHS and Division of Medicaid and Long Term Care (MLTC)'s vision of an enhanced, person-centered, integrated health services through the implementation of interoperable and responsive technology requires a partner with expertise, experience, insight, and a commitment to working hand-in-hand with DHHS to continue to deliver the ongoing EES Project, the pending DMA Project, and complementary optional projects. Nebraska needs a partner that understands the Medicaid program, both broadly and deeply. It requires a partner that understands the complex technology environment across today's health and human services agencies. It requires a partner with a proven record of accomplishment in helping health and human services agencies design and implement multiple large systems successfully. It requires a partner who is well versed in Medicaid eligibility, and comes to the project equipped with tools to expedite the delivery of IV&V services across DHHS's projects. Most importantly, it requires a partner that

First Data's IV&V framework for Nebraska:

- ✓ *Focuses on independent review*
- ✓ *Brings an experienced team with:*
  - *Practical Medicaid enterprise systems and CMS certifications knowledge*
  - *System implementation acumen in multiple COTS and custom human service solutions, including IBM Cúram*
  - *Understanding and commitment to DHHS*

understands DHHS's vision for the EES Project, the pending DMA Project and any optional projects and a partner that is committed to focusing on attainment of that vision across the multiple projects that are to attain it. **The First Data Team remains that partner**!

Through our IV&V services, the First Data Team brings a knowledge base that enables us to verify that the right system is built and to validate the system is built correctly throughout project. This knowledge and our understanding of CMS's Medicaid Enterprise Certification Toolkit (MECT) helps us to understand Nebraska's program and project-specific needs and how to partner in oversight of the management of projects.

First Data will review work products and deliverables that are outcomes of design, development, and implementation activities to verify that DHHS and CMS requirements are met. With this understanding, First Data is able to provide recommendations aimed at enhancing the overall quality and robustness of the deliverables to meet project goals. At critical points in time on similar projects, such as the completion of major activities, our understanding has helped us to update and examine the Requirements Traceability Matrix (RTM) to confirm there are no orphans, missing or incomplete requirements. To accurately measure progress and adherence to timeframes, the First Data Team may also analyze work plans, schedules, test plans and test results First Data's knowledge and understanding enables us to verify that the system adheres to the stakeholder's expectations for each project.

As an IV&V vendor whose proven processes and best practices scale to the enterprise level, we recognize this dynamic environment must be reflected in our methodology and approach, so that DHHS does not sacrifice quality in order to achieve the aggressive schedule. We accomplish this by working with the State and its partners in a team environment to help support a high quality product without bottlenecks. By integrating IV&V processes throughout the life cycle, rather than reviewing the results after completion of deliverables, DHHS can save time and effort through less rework. We also focus on identifying risks early and establishing response plans so that when issues do arise, the project can continue moving forward. In this approach, we measure our success as an IV&V vendor not by the number of deficiencies we identify, but by the success of the projects we support. Thus, we continue to view our role as an important partner to the overall success of the ongoing EES Project, the pending DMA Project, and complementary projects intended to achieve DHHS's business objectives.

To support our enterprise level approach, each project is staffed with a core team focused on that project's needs. In addition, in each project's core team there will be a team of subject matter experts who can work with each project team on an as-needed basis to confirm each project receives necessary and timely support. Each First Data Project Team will be led by a Project Manager, with business analysts and a Technical Analyst/Enterprise Architect in place.

The First Data Team also recognizes that not all IV&V projects are the same. In fact, the requirements, implementation methodology, and technologies used for one project may vary greatly between projects given the timing of the tasks, the level of true independence

required, and, at times, the need to couple IV&V services with QA services/planning and operational support through subject matter experts. With this in mind, we have developed a team structure and methodology that provides flexibility for our clients to verify the specific needs and requirements of each project are met. For each engagement, we also assign staff that has the appropriate subject matter expertise to perform comprehensive assessments.

The IV&V service contractor will review project and system processes and progress in areas including, but not limited to, the following: project management and modular development.

The First Data IV&V approach addresses the recommended items below.

Project Management	
Task Description	**Approach to Verification and Validation**
Progress against budget and schedule	• Monitor the Project's progress, resources, budget, schedules, workflow, and reporting to identify any issues, risks, or deficiencies, and make recommendations to address them. • Verify management involvement with scope and schedule management. • Validate resource loading, planned vs. actual completion, budget expenditures, and progress to plan. • Attention to the coordination and communication among teams, agencies, and departments to confirm everyone is working together, consistent with the overall project plan. • Verify stakeholder cooperation among project teams and escalate any communication risks identified.
Risk Management	• Verify and validate the Risk Management process is documented in a Risk Management Plan. • Review the risk management approach with a focus on identification, analysis of probability, impact and level of control, prioritization, assignment, mitigation planning, tracking, and monitoring. • Verify the project has well-developed technical and operational contingency plans in place to address the risk of failure of critical dependencies, such as a component or service from another state or CMS (for example, the data services hub). • Assess compliance with the Risk Management Plan by evaluating risks identified, the mitigation plans developed, and the risk resolution process.
Inclusion of state goals / objectives and all federal MMIS requirements in requests for proposal and contracts	• Analyze the requirements to validate that they adhere to State and Federal guidelines, regulations and conditions, meet the expectations of project and agency stakeholders and include DHHS and system performance standards. This includes verifying that various stakeholder groups have provided input to and/or participated in usability prototyping and testing of the system look and feel and have validated the interface requirements. • Validate the project requirements against First Data's proprietary Health and Human Services Business Architecture (HHSBA) to verify that there

Project Management	
Task Description	**Approach to Verification and Validation**
	are no gaps in the requirements.
Adherence to the state's software development lifecycle (SDLC)	• Validate that hardware, software, system development and project management standards are adhered to including but not limited to: ✓ NE IT Standards, current and planned ✓ NE IT Plan • Make recommendations for any additional standards that may be needed
Incorporation of the Seven Standards and Conditions into design and development	• Validate that hardware, software, system development and project management standards are adhered to the CMS Seven Standards and Conditions
Reasonability, thoroughness, and quality of MITA self-assessment, concept of operations, information architecture, and data architecture	• First Data will review the most recent state self-assessment, confirm that the following are addressed and identify gaps to the State: ✓ Review the As-Is business architecture description accurately reflects the reality of the environment as of2016. ✓ Evaluate the proposed To-Be business architecture environment is a quantifiable improvement over the As-Is environment and aligns with the anticipated maturity as published. ✓ Confirm that the As-Is technical architecture description accurately reflects the reality of the environment in 2016. ✓ Evaluate whether the proposed To-Be technical architecture environment incorporates the necessary technical enhancements currently being developed in order to achieve the anticipated maturity as published. ✓ Confirm that the As-Is information architecture description accurately reflects the reality of the environment in 2016. ✓ Evaluate whether the proposed To-Be information architecture environment incorporates the necessary capture, retention and transmission enhancements currently being developed in order to achieve the anticipated maturity as published. • Review if MITA 3.0 Business, Information and Technical Architecture and how NE meets 7 Standards and conditions are appropriately addressed. The State will update the SS-A as appropriate.
Reflection of the State's MITA goals and plans into actual MMIS design and development	• First Data reviews the most recent self-assessment and confirms that the published goals and objectives are still relevant. The First Data Team will meet with leadership to confirm the goals are still relevant, given the potential of multi-phase development, and the fact that goals and objectives may change since the original completion of the self-assessment. The State will update the SS-A as appropriate. • The First Data Team will compare solutions found in various design documents to the published and agreed-upon state goals and objectives. As part of design review responsibilities, the First Data Team will identify

Project Management	
Task Description	**Approach to Verification and Validation**
	gaps between what is being proposed and what is expected by the client in terms of goals and objectives. The IV&V Team may need to escalate their concern to the appropriate leadership forum if time or severity dictates.
Configuration management that is robust and includes state or developer configuration audits against configuration baseline	• Evaluate the configuration management (CM) plans and procedures to confirm they appropriately identify and control the functional and physical design characteristics of the implementation contractor. • Verify the CM plans and procedures and describe what items will be placed under configuration management control and how those items will be managed throughout the SDLC. This must include software code promotion and documentation version control for all environments: development, training, system test, user acceptance test, and production. • Include a list of all functional and physical items (configuration items) included in the scope of configuration management, which includes requirements, hardware, software, design, business rules, code, settings and configurations, and services • Identify the configuration management processes and tools are being documented, being adhered to, and contain the ability to rebuild system configurations from source code. • Validate that the configuration management processes and tools support the CMS standard and condition for reuse of services in a SOA model. • Validate the configuration management processes and understood throughout the project by monitoring code promotions.
Change Management	• Evaluate the Change Management Plan and procedures to verify they are comprehensive, follow industry standards and are monitored for adherence and effectiveness. • Review the scope change management approach to verify it is consistent with vision of the State. A robust scope management approach should be tightly coupled to the requirements management function and contains defined processes for modifying the Work Plan once scope changes have been approved by the change control board. • Confirm that the change management approach encompasses clear processes for identifying, documenting, reviewing and assessing the impact of the potential change on the project schedule, budget and past and future deliverables and milestones, whether there is training or other user related impacts and that formal change control board meetings are conducted with designated approvers. • Confirm that the Change Management Plan includes cross-project dependencies, requirements for all projects involved with the dependent requirements and that any changes to scope evaluate impacts across projects.
Adherence to service level agreements	• Validate system performance requirements are clearly defined and measurable (e.g. timing, response time and throughout) and satisfy user

Project Management	
Task Description	**Approach to Verification and Validation**
	needs. We provide recommendations regarding Service Level Objectives (SLO) and Agreements (SLA) that are appropriate based on the solution whether it is a development project, COTS product or outsourced business process.

Table 3.3 – Project Management Approach

Modular Development	
Task Description	**Approach to Verification and Validation**
Completeness and reasonability of MMIS concept of operations, architecture, and designs	• Analyze the requirements to validate that they adhere to MMIS guidelines, regulations, and conditions. • Analyze that the requirements and the timeframe for delivery meet new CMS rules that will be effective at delivery. • Validate the project requirements against First Data's proprietary Health and Human Services Business Architecture (HHSBA) to verify that there are no gaps in the overall component solution design or redundancy.
Accuracy of capture of interfaces and data sharing requirements with systems external to the MMIS	• Verify the project has well-developed technical and operational contingency plans in place to address the critical dependencies, such as a component or service from another project in the NE roadmap for MMIS replacement, other State Agency, other State or Federal service (e.g., the data services hub). • Verify that all system interfaces requirements comply with preferred approach per CMS 7 standards and conditions for SOA and interoperability, Federal standards for data exchange, security and privacy, and include operational, input/output controls, and error recovery. • Verify data interfaces and integration with the overall systems design, comply with preferred approach per CMS 7 standards and conditions for SOA and interoperability, Federal standards for data exchange, security and privacy, and include operational, input/output controls, and error recovery. Verify that approved interface documents are available, maintained and published to the appropriate projects, vendors and organizations to verify compliance to the standards and documented requirements for delivery and maintenance of interfaces and system / component integrations.
Viability and completeness of the data transition plan	• Suggest improvements to the conversion database designs to improve data integrity and system performance, including required data timeframes for conversion, data formats for archive of older data, data mapping plans, data backup at points in the conversion process and data validation in the ETL process. • Review the Conversion Data Dictionary and make recommendations regarding source locations, data normalization and/or data

Modular Development	
Task Description	**Approach to Verification and Validation**
	transformations. • Validate the conversion database design for maintainability, scalability, refresh ability, concurrence, normalization and other factors affecting performance and data integrity. • Evaluate the test plans of the data transition for completeness, appropriate data sets required for testing, testing scenarios, data modification scripts post data load, end to end testing for potential business rules or database trigger executions and complete validation through reports and user interfaces. • Evaluate the test results for the conversion database, including ETL reports and errors, operational reports against the data, i.e. ledgers, aging reports, and successful completion of the test case results defined in the data transition plan
Traceability of requirements through design, development, and testing	• Assess the existence of a Requirements Management Plan and validate that it is followed. Requirements will be validated during design, development, testing and implementation. • Evaluate and assess the SI proposed RTM tool for requirements management and provide a formal response specifically indicating whether the tool is appropriate for the project, works in conjunction with other related tools used by other teams on the project, and meets the requirements of the requirements tool in specific areas (i.e., traceability, tracking, reporting, escalation). • Confirm that the requirements follow the SMART (specific, measurable, achievable, traceable, and testable) rules. • Verify that requirements are tracked in an RTM for future traceability through design, code, test and implementation. The RTM enables forward and backward traceability from Solicitation through UAT and Project completion. • Verify that the requirements in the RTM are consolidated at an enterprise level in a multi-project approach and that cross project dependency requirements are identified and linked to verify deliverables will function as defined. • Confirm both the process and traceability matrix will properly document the life of a requirement and provide bi-directional traceability between various associated requirements. Verify the process and artifact(s) enables the State to find the origin of each requirement and tracks all changes made to all requirements. • Confirm all requirements are properly included and documented at the appropriate level. Identify items that do not trace, incorrectly trace, or do not sufficiently trace. Identify any missing, additional or ambiguous requirement to avoid future problems in design. Verify traceability artifacts are maintained and used as designed during all project phases.

Modular Development	
Task Description	**Approach to Verification and Validation**
	• Verify any tracing issues, problems, or questions generated by the traceability analysis have an agreed upon resolution. If appropriate, confirm documentation (or requirement) updates are completed to prevent future issues and confirm documentation of the resolution points to or resides with the traceability analysis.
Adequacy of system security and privacy policies, plans, technical designs, and implementations	• Evaluate and make recommendations on project policies and procedures to confirm that the system is secure and that the privacy of client data is maintained to specific, defined standards (NIST, HIPAA, MARS-E 2.0). • Assess the approach and tools mentioned in the design and development deliverables that include network security, security of data, access or physical security, and the security of the application software. • Review of the Site Preparation Plan, includes checking the results of detail modeling to operations facilities to verify the proposed network design contains adequate bandwidth for transmission to meet specifications. • Monitor that the SI is using redacted data whenever possible during testing, training and conversion validation. Verify appropriate access as required for PHI and PII. Review these work products and confirm they adequately address security requirements for the Equipment, Software, Network and Facility. • In order to determine what areas within the Eligibility System would be likely targets of potential threats, we will analyze the conceptual technical architecture and business requirements with a focus on the known security threat landscape to identify risks for each of the functional and architectural areas identified.
Coverage and integrity of all system testing, including stress testing and testing of interfaces between modules and with external partner systems	• Review schedules to verify that adequate time and resources are assigned for planning, development, review, testing and rework. • Review the SI's Performance test plan to validate it is measuring performance of appropriate scenarios, volumes of transactions and will provide output measurements consistent with the defined performance requirements. • Review the SI's performance testing results to include the review of new and existing system hardware configurations to determine if their performance is adequate to meet existing and proposed system requirements. • Evaluate the planned hardware configurations and infrastructure architecture to verify it is scalable, maintainable, and upgradeable, and will meet the demands of the planned Eligibility System. Where the First Data Team finds deficiencies, we will make recommendations for changes to the hardware design and, if applicable, any cloud configurations. • Review the State's hardware configuration management plans and procedures to identify any potential issues, such as the sun setting of support for a hardware component.

Modular Development	
Task Description	**Approach to Verification and Validation**
	• Evaluate volume and stress testing results, and evaluate the capacity planning program to verify its ability to support future growth. • Identify issues, risks, or deficiencies, we will make recommendation to improve system performance and accommodate future growth. • Validate that the testing of the software will simulate operational conditions. • Validate that daily, month end, and month beginning conditions exist for batch testing.
Capacity management, including consideration of future vendors' support and release plans for underlying databases, software, and hardware	• Evaluate program changes and impacts that may produce significant spikes in system demand such as open enrollment periods, changes to MAGI requirements for Medicaid eligibility, month end, quarterly and annual processing volumes. • We will evaluate growth plans, and evaluate the capacity planning program to verify its ability to support future growth. • Verify any discrepancies between the system design and development documentation and the DHHS technology plan.
Adequacy of Disaster Recovery Planning	• Confirm that roles and responsibilities, timeframes and communication procedures and escalation procedures are clearly defined for all project stakeholders, including specific contacts. Both the routine and unexpected process requirements that are likely to impact the Eligibility Systems reliability should be addressed. • Review the available Business Continuity Plan accessing for identification of all critical systems alternate processes are documented, when a business disruption of a system requires moving to a disaster recovery plan and appropriate alternative sites and contracts are in place to support Business Continuity Plan and Disaster Recovery Plan. Assess the plans, processes and procedures for business continuity and recovery are in place in the event of a disaster or business emergency. • Verify that training and tests will be conducted periodically.

Table 3.4 – Modular Development Approach

3.1.1 Project Management

Describe the bidder's proven methodology, approach, and process for Project Management of Medicaid IV&V activities. (RFP Section IV, B.1.c.i)

First Data has worked with multiple states verifying and validating that their systems are built according to defined specifications. With decades of experience and a thorough understanding of industry standards, we bring professionals that can access work products and provide recommendations aimed at enhancing the overall quality and robustness of deliverables.

With our understanding of the ongoing EES Project and the future vision, First Data aligns our IV&V management methodology to the standard project phases as defined by the PMBOK and as reflected in the illustration below. We understand DHHS's strategic goals and the roadmap to achieve them. We tailor the IV&V program management methodology to work with the agreed upon development methodology to include waterfall, prototyping, interactive/incremental, spiral, rapid application development (RAD), and agile methodology.

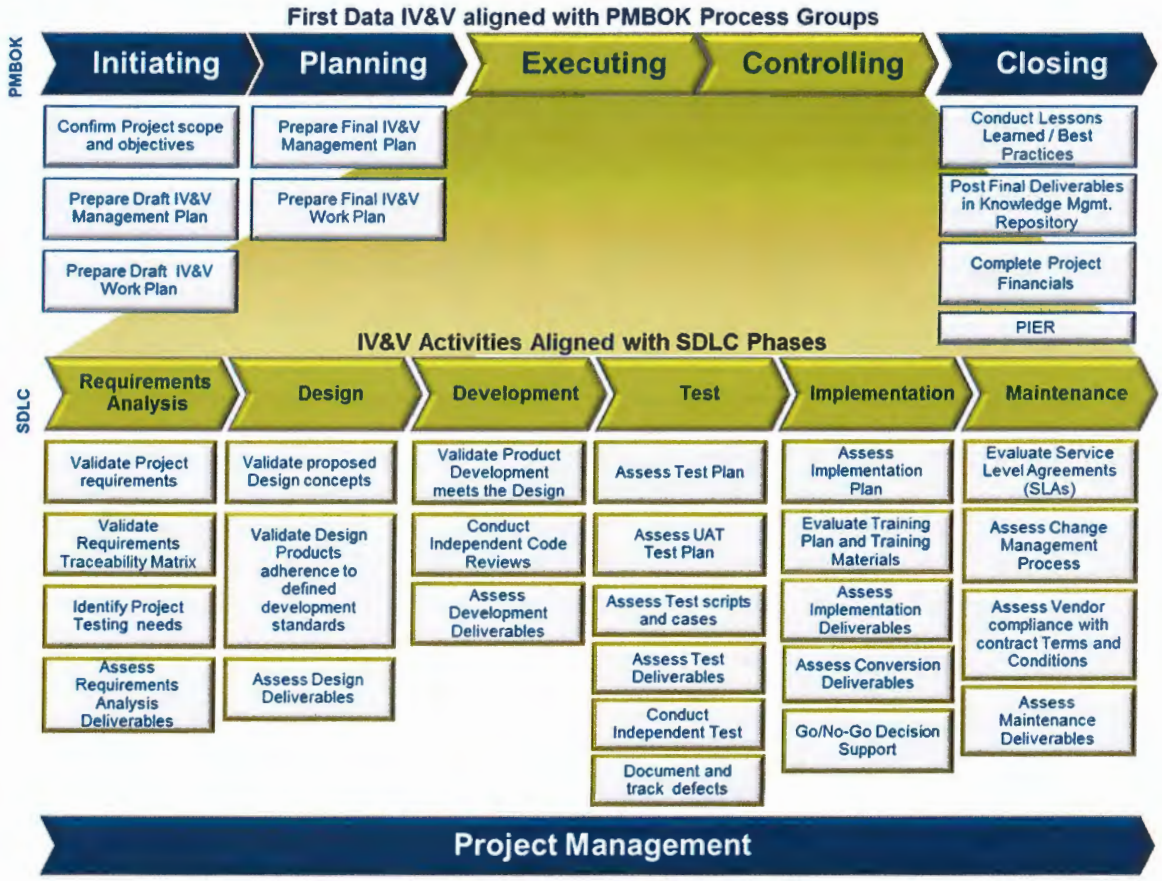


Figure 3.2 – First Data's IV&V Methodology Aligned with PMBOK Processes and SDLC Phases

First Data follows a structured IV&V project management approach as follows:

- **Initiate** - we confirm key project and IV&V objectives, secure staff and prepare a draft IV&V Management Plan and IV&V Work Plan.
- **Plan** - we create and maintain a structure to accomplish the objectives and prepare the team to begin the phase or task. This includes finalization of both the IV&V Management Plan and the IV&V Work Plan.

- **Execute** - we coordinate the people to carry out the IV&V Management Plan and build the IV&V products/tools. In this phase, we:
  - ✓ Complete all IV&V tasks, including deliverable, progress and process reviews
  - ✓ Provide and use our IV&V tools, such as checklists and metrics
  - ✓ Prepare required IV&V deliverables, including deliverable review reports and IV&V Status Reports
  - ✓ Share our findings through defined communication processes and channels
- **Control** - we confirm that project objectives are met by monitoring and measuring progress and recommending corrective action as necessary. We apply consistent assessment and monitoring processes throughout design, development and implementation. We track and monitor progress of our IV&V tasks and deliverables, assess the progress and performance of the EES implementation contractors and adherence to the overall schedule and budget.
- **Close** - we assist the project in verifying that all deliverables meet requirements, the products have been tested, that there are no findings that would preclude final implementation and provide a recommendation for final approval/acceptance.

Our proposed project management methodology is directed to the accomplishment of four fundamental objectives:

- **Effective Communications** - Timely and accurate communication of issues and progress to all project participants throughout the duration of the project.
- **Dynamic IV&V Project Management** - Estimating, planning, organizing, and managing the work to verify that quality work products are delivered on schedule and within budget.
- **Proactive IV&V Quality Management** – Building the processes for evaluating progress, work products, and work processes to deliver quality end products that meet business objectives, client expectations and project requirements into our internal standards for deliverable and work product development.
- **Comprehensive IV&V Risk Management** – Well-defined processes for anticipating, assessing and mitigating project risk areas. The proven practices developed by our staff over years of successfully conducting similar projects enable us to anticipate various types of risks and incorporate procedures to avoid or minimize areas of risk.

The overall project management methodology is structured to meet these four objectives, as illustrated below:

Objectives	Techniques	Tools
1. Effective Communication	• Communication and management reporting	• Standardized report formats • Communication plan with appropriate contact points and escalation procedures • Weekly and Monthly Status Reports • Document tracking system for procedures and reports
2. Dynamic IV&V Project Management	• Planning and organizing work • Documentation standards • Estimating and administering the work effort for the project • Managing project resources • Establishing project controls • Formalizing Change Control	• IV&V Management Plan is completed to establish standards and procedures • MS Project to manage tasks, activities, dependencies, and schedule • MS Office software to support email and the development of deliverables and presentations • Resource allocation and scheduling plan and procedures • Change Control procedures and approval process
3. Proactive IV&V Quality Management	• Establishing standards and approved conventions • Issue Identification • Scope/Change Control Management	• Quality Checklist and Templates • Scheduled Quality Assurance checkpoint reviews • Quality Control work product evaluations • Issue Tracking System • Established change control, change approval and communication procedures
4. Comprehensive IV&V Risk Management	• Identifying and anticipating all components of risk – managerial, political, technical and financial • Developing risk evaluation and mitigation strategies from project outset • Conducting ongoing risk assessments	• Standardized risk assessment templates • Standardized assessment categories • Best Risk Management practices from prior projects • Ongoing risk monitoring (risk triggers) included in the project status reports

Table 3.5 – Techniques and Tools of the Project Management Objectives

First Data applies a structured deliverable review and assessment methodology that our team has used on many prior IV&V engagements. This includes:

Phase 1 – Information Gathering

- Validate Scope – confirm why the assessment is being conducted, what areas, the timelines, schedules, types of communication, roles responsibilities, etc.
- Collect Documents – request for applicable historical documents, set up of repository and identify types of categories for your assessment type

- Conduct Interviews – schedule and conduct interviews with key staff/groups/divisions in applicable areas identified for the assessment(s), collect information

Phase 2 – Analysis of Information

- Review documents to identify the good, the bad, and the ugly – put into categories specific to assessment type

- Analyze information by category – identify common themes (i.e. how often they occur, performance measurements, policy or procedure gaps, age of equipment, skills gaps, defects, etc.)

- Conduct Analysis on Alternatives – Identify alternatives by research on other states, other departments, and national standards or there may also be an alternative to consider that research will not identify. Conduct the analysis including pros and cons, consideration of timelines and cost, Federal and state mandates, enterprise goals, etc.

Phase 3 - Final Report

- Document findings in accordance with specifications from the client and CMS.

- Summarize findings and summarize the alternatives (what the possibilities are). Additionally, depending on the statement of work and type of assessment the final report may include the future vision, objectives, gaps between the future and current, recommendation report, a roadmap, implementation plan or change resistance plan.

CMS is looking to IV&V contractors to serve a greater role in confirming that their requirements are met when supporting Medicaid transformation projects. First Data remains independent from the vendors who are providing solutions for these transformations and we understand the outcomes that CMS is encouraging Nebraska to achieve. Our flexible IV&V service offering is focused on helping Nebraska achieve its transformation of the Medicaid Enterprise to managed care while meeting CMS expectations.

First Data also understands the system development lifecycle, and the interplays between stakeholders and reporting cycles. The figure below describes our understanding of the processes and the relationship to MITA and CMS touchpoints.

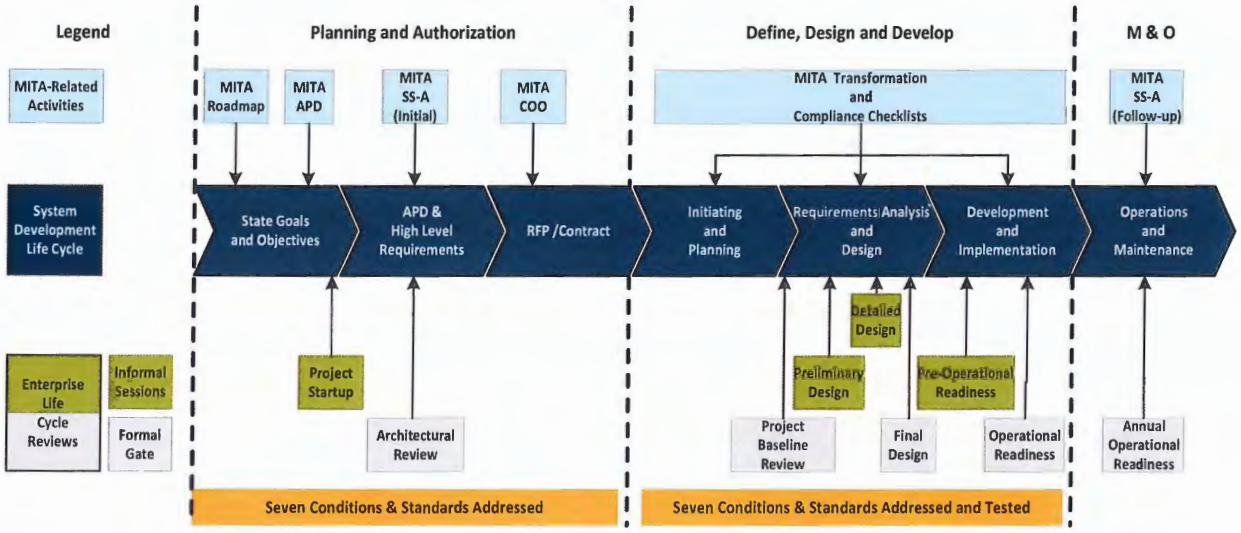


Figure 3.3: First Data's Assessment of the SDLC and CMS Touchpoints

First Data recognizes the importance of alignment to CMS standards and processes throughout the journey of system development. We will utilize the following methods to keep the project aligned with CMS:

- Work with the State to identify the most appropriate templates and artifacts to develop, based on the artifacts available in the CMS Collaborative Application Lifecycle Tool (CALT).
- Perform assessment of the implementation contractors' approaches and deliverables against MITA and the standards and conditions for Medicaid IT.
- Utilize the recently released Medicaid Enterprise Certification Toolkit (MECT) version 2.0, including applying the Medicaid Enterprise Certification Life Cycle (MELC) as defined by CMS

The First Data Team will create a culture of accountability by measuring the vendor's achievements against DHHS' explicit goals and objectives and, where necessary, will help clarify the desired outcomes to your contractors. While the CMS certification checklists are mandatory, we recognize that IV&V's duty to complete these on behalf of CMS must be balanced with the specific dynamics that pertain to Nebraska, and must ultimately be supportive of your defined strategy. Nebraska's vision for Medicaid transformation is clearly stated and will be an overarching consideration of First Data when providing IV&V oversight of your vendors. Our verification and validation practices are centered on protecting the interests of Nebraska citizens – clients you serve, your staff, and the economic interests of taxpayers.

Include an example of an IV&V project schedule utilized on similar projects. (RFP Section IV, B.1.c.ii)

We have included an example of a project schedule as Appendix 3. This example was taken from the Idaho Health Insurance Exchange IV&V Project. Your Health Idaho (YHI), Idaho's Health Insurance Exchange (HIX), initiated a project to migrate from the Federal Based Exchange to a State Based Marketplace in time for enrolling consumers into qualified health plans (QHPs) by October 2014. The state required IV&V services during the design, development and implementation (DDI) of the YHI Health Insurance Exchange system.

ID	WBS	Task Name	Start	Finish
1	1	YHI IV&V Project	Mon 4/21/14	Wed 12/31/14
2	1.1	Project Planning and Administration	Mon 4/21/14	Wed 12/31/14
3	1.1.1	Project Initiation	Mon 4/21/14	Thu 5/1/14
9	1.1.2	Project IVV Artifact Repository	Wed 4/30/14	Thu 5/1/14
12	1.1.3	Project Planning	Mon 4/28/14	Tue 5/27/14
13	1.1.3.1	IV&V Management Plan	Mon 4/28/14	Tue 5/27/14
19	1.1.3.2	IV&V Work Plan	Mon 4/28/14	Tue 5/27/14
24	1.1.3.3	IV&V Review Checklists	Mon 4/28/14	Tue 5/27/14
30	1.1.4	Project Execution, Monitoring and Controlling	Mon 4/28/14	Tue 12/30/14
31	1.1.4.1	Initial IV&V Review	Fri 5/2/14	Mon 6/2/14
41	1.1.4.2	Weekly IV&V Review Reports	Fri 5/2/14	Tue 12/30/14
76	1.1.4.3	Monthly IV&V Review Reports	Fri 5/16/14	Mon 12/29/14
85	1.1.4.4	Monthly IV&V Status Reports	Fri 5/16/14	Mon 12/29/14
94	1.1.4.5	Monthly Management Briefings (Per YHI Request)	Tue 5/27/14	Mon 12/29/14
103	1.1.4.6	Project Management Assessment	Mon 4/28/14	Mon 12/29/14
148	1.1.4.7	Requirements Validation Phase	Mon 4/28/14	Mon 6/2/14
176	1.1.4.8	System Design Phase	Tue 6/3/14	Tue 8/26/14
210	1.1.4.9	Technical Environment Assessment	Mon 5/26/14	Mon 9/8/14
242	1.1.4.10	Operations Environment Assessment	Thu 9/11/14	Wed 11/5/14
280	1.1.4.11	System Development	Mon 5/5/14	Tue 7/29/14
291	1.1.4.12	Testing	Mon 5/5/14	Thu 11/20/14
309	1.1.4.13	Pre-Operational Readiness Review (PORR)	Mon 5/5/14	Thu 7/24/14
316	1.1.4.14	Operational Readiness Review (ORR)	Mon 8/4/14	Wed 10/22/14

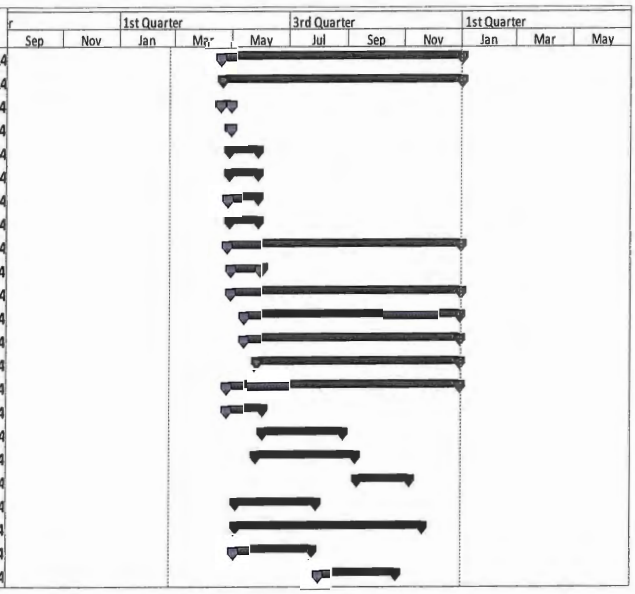


Figure 3.4First Data provided IV&V services during the design, development and implementation of the YHI HIX project and continues to support Blue Print Testing.

Describe how the IV&V bidder's project management approach adapts to varying State governance models. (RFP Section IV, B.1.c.iii)

First Data's IV&V project management approach can be calibrated to suit the needs of any organization or governance model as needed by DHHS. We bring the tools, templates and talent and apply the right amount of rigor to the processes as directed by our clients. As a leading provider for IV&V services in the healthcare industry we have seen vastly disparate service requests for IV&V. Some of our clients have taken the "kitchen sink" approach and included any augmentation services they needed and applied the title of IV&V, while other clients have taken an approach where they are only doing IV&V because they are required to, with minimalistic vendor involvement.

First Data will build on the processes already established for the ongoing EES Project incorporating and adapting as the governance needs and structure evolve in the project lifecycle. The complexity and dynamic nature of this and any large-scale project makes effective project management a mandatory ingredient for success. From our numerous and

wide-range of IV&V projects, we have found that the keys to project management success include the following:

- **Providing the right team** – skilled in project management and specific program areas with sound subject matter expertise.
- **Providing an understanding of the business problem** – given the timeframes and mission critical nature of the overall project, it is imperative to provide leadership assistance in prioritizing the work and maximizing productivity.
- **Providing best practice solutions** – based on individual customer requirements, provide a proven set of methods, tools and procedures that can be customized to each project's needs.
- **Creating a partnership** – with the client to create shared project success criteria, provide the professionals and experience to validate the project success criteria, and stand with the client throughout the project to reach this goal.
- **Mitigating Risk** – through our experience and commitment, we are able to add value and assist DHHS management in making informed decisions regarding risk mitigation, risk control, and project planning.
- **Credentials** – of having a national government practice with highly skilled professionals who have worked on engagements in nearly every State. This depth of experience has led to the development of a comprehensive methodology for managing and executing successful large-scale projects.

The project teams will follow a similar core approach to address the individual project needs, nature, and scope of the IV&V responsibilities. The project teams will be staffed with skills necessary to address the business needs, the technology used, and development methodology employed.

Address the bidder's approach to meeting each requirement in a table that contains the requirement and the contractor's approach to meeting the requirement. (RFP Section IV, B.1.c.iv)

The table below details our approach to meeting the following requirements.

	Project Management Requirements	First Data's Approach
1	Must develop and submit comprehensive IV&V Project Management Plan(s) work product for Department approach a maximum of 30 days after each project start, and must manage and perform the IV&V services in accordance with the IV&V	• The First Data Team will work collaboratively with the Department and key stakeholders to develop and customize an IV&V Project Management Plan (PMP) that integrates with, and meets the needs of, each project. We understand the value of this Plan comes from the execution of said plan's content. This is not a deliverable that

	Project Management Requirements	First Data's Approach
	Project Management Plan(s).	"sits on the shelf"; it is the guide for the entire First Data Team with some key components that the Department can also apply to enable programmatic oversight over the projects. First Data is committed to delivering an IV&V PMP that is practical and useful, applied consistently in the management of the IV&V effort, and coordinated with other project plans.
2	Must develop IV&V project schedule(s) work products a maximum of 30 days after the projects' start and update weekly IV&V schedules that coordinates IV&V activities with project schedules.	• First Data will work with DHHS and its partners to develop the baseline IV&V project schedule, outlining the project tasks, roles, responsibilities and deliverable for each project • IV&V schedules will align to implementation contractor project schedules when available and will provide the flexibility to modify workload as schedule changes occur. • Validate tasks and modify them as requested, to include: ✓ Validate tasks and deliverables from the RFP were included in the initial project Work Breakdown Structure (WBS) ✓ Identify any additional tasks and deliverables to add to WBS based on initial feedback from Department ✓ Identify predecessors and successors ✓ Incorporate tasks and due dates for all deliverables that require drafts and final submissions and review and approval periods • Assign resources to tasks and confirm that resources are not over allocated • Baseline approved work plan to track actual against baseline start and finish dates • Using Microsoft Project, review and update the work plan on a weekly basis to support currency, accuracy, and completeness as well as to facilitate timely progress and measurement tracking and reporting • Complete weekly updates to determine activities or tasks that may be at risk of budget or schedule variances and to allocate resources to address project risks, including: ✓ Summary of key impacts and changes made since prior month and risks and issues

	Project Management Requirements	First Data's Approach
		associated with changes ✓ Percent complete for each task and subtask ✓ Actual hours by task and subtask ✓ Resource adjustments as necessary ✓ Gantt charts and various views showing planned start and end dates and durations of all tasks, subtasks, and major milestones and deliverables, including timeframes for review and approval of all deliverables and work products and exceed contract commitments
3	Must develop clear lines of communication and collaborative working relationships with project teams, project leadership, and CMS.	• Assess the comprehensiveness of the Communication Plan and that is appropriately addresses all required contractors, partners, stakeholders and sponsors. • Encourage participation from stakeholders early and often through planning and development to encourage "buy-in". • Collaborate with CMS through the gate review process. • Devise a well-coordinated review process with stakeholders that includes result reporting. • Evaluate if additional communications are required or additional communication protocols need to be established and enacted. • Verify that there is timely and accurate communication of issues and progress to all project participants throughout the duration of the project. • First Data will leverage relationships currently in place with the State team, EES vendor and CMS to minimize any transition impact.

Table 3.6 –Project Management Requirements and First Data's Approach

3.1.2 Independent Assessment and Quality Assurance

Independent verification and validation (IV&V) is defined as processes that determine whether development products of a given activity conform to the requirements of that activity, and whether the product satisfies its intended use and user needs. This may include active analysis, evaluation, review, inspection, assessment, and testing of software products and processes.

Simply stated, IV&V is independent assessment of an IT project's products and processes to verify the quality of the final product.

First Data views IV&V as an independent assessment of a project's products and processes to confirm the quality of the final product. "Independence" refers to the fact that the IV&V organization is both technically and managerially separate from the organization responsible for developing the product.

There are two key principles that typify IV&V:

- **Are we building the thing right?** Independently verifying the development processes to confirm they adhere to best practices.
- **Are we building the right thing?** Independently validating the products to confirm quality.

The core of IV&V activity is deliverable assessment. The primary purpose of deliverable assessment is not only to verify each deliverable satisfies all applicable business and technical requirements and conforms to project quality and industry standards, but also to confirm that each deliverable moves the project one step closer to implementation. The results of IV&V deliverable reviews will help DHHS understand and measure progress in each area and correspondingly make informed decisions. The First Data deliverable review approach is an important tool in that it sets expectations for the State and vendor along the way.

Address the bidder's approach to meeting each requirement in a table that contains the requirement and the bidder's approach to meeting that requirement. (RFP Section IV, B.2.c.i)

The table below details our approach to meeting the following requirements.

	Independent Assessment and Quality Assurance Requirements	First Data's Approach
1	Must actively participate in the projects and provide ongoing assessment of the projects to proactively identify risks, issues, and opportunities along with associated recommendations for the project team.	First Data will actively participate in both the EES and DMA project. We will provide verbal feedback during meetings and ongoing assessments of the project work products and deliverables to identify and document issues and risks. We will provide recommendations for mitigation and remediation as needed.
2	Must assess the progress of the projects against the planned schedules, budgets, and resource allocations.	First Data will use a work breakdown structure (WBS) provided by the project team to identify the tasks, work products and milestones for the project. These should be associated with levels of effort and resources required. We pair them with assumptions and constraints, work plans, critical paths, phases, metrics, and trends, and summarize both internal and external schedule/project work plan dependencies.

	Independent Assessment and Quality Assurance Requirements	First Data's Approach
		Schedule management is the process of verifying that the project schedule is base lined, maintained, and managed accordingly. Schedule is the agreed-upon set of tasks, start dates, and finish dates used to guide and monitor the project to completion. It also describes the milestones of the project – significant accomplishments that typically are the culmination of a series of tasks. First Data will compare all of the details of the WBS against both preceding governance documentation and resulting work products. We will validate the WBS internally for correctly tabulated volumes of effort and metrics/trending. We will evaluate and make recommendations on the estimating and scheduling process of the project to confirm that the project budget and resources are adequate for the work breakdown structure and schedule. We will review schedules to verify that adequate time and resources are assigned for planning, development, review, testing, and rework.
3	Must assess the projects' resources, managerial responsibilities, and governance structure to identify gaps and provide recommendations.	We will verify that a project management plan (PMP) is created and being followed. The PMP is the main planning document for a project, and describes how major aspects of the project will be managed. This would include management responsibilities and governance structures. We will evaluate the project management plans and procedures to verify that they are developed, communicated, implemented, monitored, and complete.
4	Must participate in all project meetings unless otherwise directed by DHHS.	First Data understands and agrees to participate in all project meetings as directed by DHHS.
5	Must perform an independent assessment of issues where the implementation contractors and DHHS' project management organization disagree and provide the results of the assessment and recommendation to DHHS leadership.	First Data will use an issue management plan to describe how issues associated with the project will be independently identified and managed. We will outline what issue management activities will be conducted and how they will be performed, recorded, and monitored throughout the life of the project. We can conduct independent assessment of issues between the vendor and State as an outside 3rd party. Through the use of this plan, we will verify the existence and active adopted use of an appropriate

	Independent Assessment and Quality Assurance Requirements	First Data's Approach
		project issue tracking mechanism that documents issues as they arise, enables communication of issues to proper stakeholders and a process for addressing, documents a mitigation strategy as appropriate, and tracks the issue to closure. This should include but is not limited to technical and development efforts.
6	Must perform one or more reviews of project deliverables and work products including but not limited to infrastructure, system documentation, design, working code, test scenarios, test cases, test results, plans, etc. and provide a detailed assessment of the quality of the deliverables and work products along with recommended changes. Assessment must include a recommendation on whether DHHS should approve the work product or deliverable. Review must address at minimum the following attributes: • Traceability and adherence to requirements • Clarity • Completeness • Consistency • Quality • Adherence to applicable laws, rules and guidelines	With our previous experience in working with DHHS the First Data Team brings a knowledge base that enables us to verify that all deliverables reflect quality and adhere to applicable rules, regulations, laws and guidelines. This knowledge helps us to understand DHHS' project-specific needs and how to review and assess the work products and deliverables thus verifying completeness and that all requirements are met. First Data applies a structured deliverable review and assessment methodology that our team has used on many prior IV&V engagements. We will apply this methodology to the review of EES and DMA Project deliverables. Our methodology is based on the following tenets: • **Participate in the full deliverable lifecycle –** First Data works with project teams throughout the entire deliverable development, review, and comment and approval process, through submission of a recommendation for deliverable acceptance. • **Provide input and feedback on a flow basis –** This allows recommendations to be incorporated into subsequent versions of deliverables, which improves the quality of the final product and minimizes the time associated with final reviews. • **Use a structured tool to document findings –** This provides a consistent and consolidated format where cosmetic and material deficiencies are documented. • **Produce thorough Deliverable Review and Assessment Reports –** First Data reviews and assesses the readability, comprehensiveness, accuracy, level of detail, and quality of all required deliverables.

	Independent Assessment and Quality Assurance Requirements	First Data's Approach
7	Must assess project plans, processes, and procedures to identify improvements and whether they are being followed.	We will review project work plans, project management plans, and implementation contractor processes to verify they are being followed and identify potential improvements.
8	Must assess project change orders for the following: • The change order is following the approved change management plan and processes. • The change order is within the scope of the existing contract. • Cost and resources estimates for the change order are reasonable. • Recommendations for alternate approaches to achieving the outcome of the change order.	When changes are proposed by the implementation contractor or DHHS, the proposed change orders must be analyzed: • Review draft change orders with respect to scope, level of effort, resources, schedule, cost, and impact to the existing Work Plan. • Confer with the Vendor team during the change order analysis process and determine whether the vendor provided sufficient alternatives • Meet with the appropriate implementation contractor representatives to request additional information or clarification. First Data will use the following steps to conduct change order reviews: • Verify required information on the change order ✓ Can the completion date be achieved? Are the start and end dates realistic and achievable? • Validate the schedule to complete the change order ✓ Can the overall completion date be achieved? Are the start and end dates realistic and achievable? • Validate costs ✓ Conduct an independent estimate to provide the total cost ✓ Compare effort to other similar efforts in the original work plan ✓ Determine the appropriateness of the hourly rate structure used for resources and tasks ✓ Are resources assigned to the appropriate role? • Validate assumptions and constraints ✓ Confirm that the assumptions and constraints that affect the overall estimate have been identified and explained ✓ Make recommendations for more details as appropriate

	Independent Assessment and Quality Assurance Requirements	First Data's Approach
		✓ Document findings that are not valid or otherwise introduce risk • Analyze the impact on existing work plan ✓ Does the change order negatively impact work already scheduled? ✓ Do resources have to be relocated to change order tasks? • Document change order benefits and/or risks ✓ Evaluate the cost of not implementing a change order ✓ Do the costs outweigh the quantifiable benefits? ✓ Does implementing the change order introduce any risk to the project?
9	Must comply with IV&V regulatory requirements detailed in 45 CFR 95.626.	First Data understands and agrees to be an independent IV&V vendor for DHHS.
10	Must identify areas of unnecessary duplication and overlap between roles on the projects.	As part of the IV&V review of roles and responsibilities of the project staffing, First Data will assess whether there is any duplication and overlap between project roles and make recommendations on making changes for increasing efficacy and reducing costs. First Data will apply this assessment at a programmatic level to identify potential duplication between projects.
11	Must assess and verify requirement traceability throughout the project and system development lifecycle of the projects.	First Data will validate that all requirements are correctly identified in order to verify the system meets the needs of the project and its stakeholders. It is critical that these requirements are "traceable" through the SDLC phases: Requirements Analysis, Design, Development, Test, and Implementation phases. To accomplish this, the following steps are undertaken: • We validate the requirements in the RTM incorporate traceability of the requirement at requirement validation checkpoints and throughout the entire project. • To satisfy the criteria of traceability; every requirement is uniquely identified. We validate that each major section of requirements is numbered hierarchically and then individual requirements are uniquely identified within each section. This approach provides organization while keeping labels short, meaningful, and

	Independent Assessment and Quality Assurance Requirements	First Data's Approach
		independent. • Any issues or risks identified during the course of creating RTM are updated in the Issue and Risk Tracking Log Invariably, new requirements are identified once the initial gathering sessions complete, often the result of participants returning to their positions and looking at their business processes in a slightly different perspective. Inserting the occasional new requirement will not require a complete renumbering of the remaining section.
12	Must develop and monitor project performance metrics which allow tracking project completion against milestones.	First Data will develop and monitor project performance metrics which allow tracking to project completion milestones. Our team will work closely with DHHS to: • Identify Metrics • Obtain benchmark data • Identify metrics owners • Set clearly defined goals for improvement ranges and tolerances. • Provide periodic meetings and progress reports as agreed upon • Complete formal project milestones review • Compare actual vs. planned start date for project tasks
13	Must submit criteria for approval for defining a Critical Incident which could adversely affect the outcome of the projects.	First Data will work closely with the project teams to develop criteria to define Critical Incidents which would have an adverse effect on project outcomes.
14	Must notify the Department immediately when the IV&V Contractor discovers any Critical Incident. Provide a Contractor Critical Incident Report for each Critical Incident that summarizes the incident, how it may affect the project, notes any discrepancies found by the IV&V Contractor and provides a proposed action plan to resolve the incident and mitigate its impact.	The IV&V Manager will work directly with the State, EES and DMA Project Managers during Project Initiation to determine the proper cadence and communication channels for both actual and potential critical incidents. We will develop a critical incident report and process with steps from discovery through resolution, providing proposed action plans to aid a quick efficient resolution to mitigate impact.
15	Must interview and observe project	Through the use of meeting participation, interviews

	Independent Assessment and Quality Assurance Requirements	First Data's Approach
	management staff and developer staff and observe project meetings and activities to understand the process, procedures, and tools used.	and documentation, First Data will observe management and developer staff to better understand the processes, daily procedures and use of tools.
16	Must review and analyze all applicable and available documentation for adherence to accepted, contractually-defined industry standards.	First Data institutes our quality assurance methodologies from our Center of Excellence to perform verification of software development tasks and processes to confirm they are well-defined, repeatable, and consistent with contract requirements and industry standards. This includes validating quality standards and practices and performing assessments of items such as the following: • Technical Deliverables and Documentation • ACA, Medicaid System designs • Equipment Installation • ACA, Medicaid Testing Plans • Project management processes and reporting standards

Table 3.7 – Approach to Independent Assessment and Quality Assurance Requirements

Describe the bidder's approach in detail to IV&V including: (RFP Section IV, B.2.c.ii)

(a) Project participation at the level of detail necessary to assess the project's health

The figure below depicts the First Data Team's approach to IV&V relationships followed by each system feature during its development lifecycle. It focuses IV&V rigor on what is critically important throughout the lifecycle, and ties together static testing activities (reviews, inspections) with the dynamic test effort. It also requires that virtually every aspect of planning occurs much earlier in the lifecycle than would otherwise be the case.

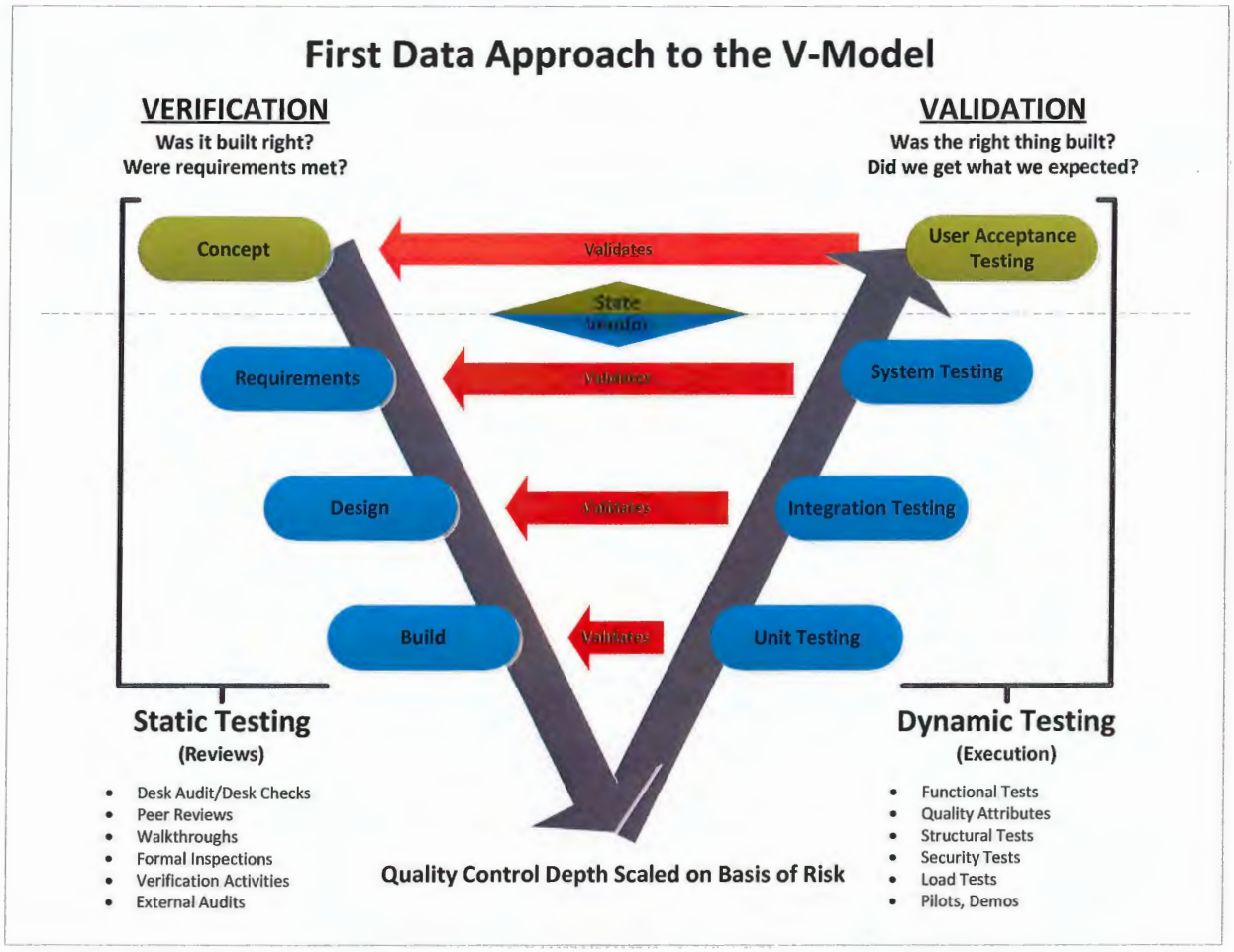


Figure 3.5 – First Data's Approach to the V Model

(b) Risk, issue, and opportunity management

Risk is the possibility of the occurrence of any event that can affect the success of a project. All large, complex technology integration projects are subject to risks because there is an inherent combination of uncertainty and constraints. Not all project risks can be completely eliminated. However, project risks can and must be managed and/or mitigated. To go beyond this initial identification of risks, however, the agencies must view risk management as a facet of quality, using basic techniques of analysis and measurement to verify that risks are properly identified, classified, and managed.

The First Data approach to risk management includes these key components.

- **Identify** - Before risks can be managed, they must be identified. Identification discovers risks before they become problems and adversely affect a project. First Data has developed techniques for surfacing risks by the application of a disciplined and systematic process that encourages project personnel to raise concerns and issues for subsequent analysis.

- **Analyze** - Analysis is the conversion of risk data into risk decision-making information. Analysis provides the basis for the EES and DMA Project Managers to work on the "right" risks. This step includes determining probability of occurrence to determine which risks warrant the highest level of attention.

- **Plan** - Planning turns risk information into decisions and actions (both present and future). Planning involves developing actions to address individual risks, prioritizing risk actions, establishing an owner to address each risk, and creating an integrated risk management plan. The plan for a specific risk could take many forms. Examples might include:

  - ✓ Mitigate the impact of the risk by developing a contingency plan (along with an identified triggering event) should the risk occur.

  - ✓ Avoid a risk by changing the design or the development process.

  - ✓ Accept the risk and take no further action, thus accepting the consequences if the risk occurs.

  - ✓ Study the risk further to acquire more information and better determine the characteristics of the risk to enable decision-making.

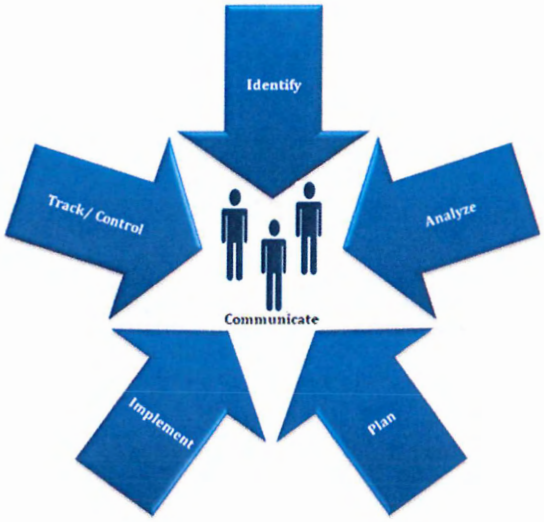


Figure 3.6 - Risk Management Process

- **Track** - Tracking consists of monitoring the status of risks and taking action to ameliorate risks. Appropriate risk metrics are identified and monitored to enable the evaluation of the status of risks themselves and of risk mitigation plans.

- **Control** - Risk control or abatement corrects for deviations from planned risk actions. Once risk metrics and triggering events have been chosen, there is nothing unique about risk control. Rather, risk control melds into project management and relies on project management processes to control risk action plans, correct for variations from plans, respond to triggering events, and improve risk management processes.

- **Communicate** - Risk communication lies at the center of the model to emphasize both its pervasiveness and its criticality. Without effective communication, the risk management approach cannot be viable. While communication facilitates interaction among the elements of the model, there are higher-level communications to consider as well. To be analyzed and managed correctly, risks must be communicated to and between the appropriate organizational levels and entities. Because communication is pervasive, our approach is to address it as

integral to every risk management activity and not as something performed outside of, and as a supplement to, other activities.

Issue Management

PMI defines an issue as "a point or matter in question or in dispute, or a point or matter that is not settled and is under discussion or over which there are opposing views or disagreements." As project issues are identified, they are managed, controlled and resolved through the Issue Management Process. The purpose of issue management is to help confirm the proper oversight and management of issues that arise throughout the project.

Upon inception of the IV&V services the First Data Team will work with DHHS to implement a comprehensive Issue Management Process using First Data's established Issue Management methodology. Issue management procedures to be followed by the First Data Team can be broadly classified as:

- Issue Identification and Documentation
- Issue Validation, Assignment and Prioritization
- Issue Analysis
- Issue Tracking and Reporting
- Issue Escalation (if needed)
- Issue Resolution and Closure

Tools utilized for Issue Management are similar to those used for Risk Management and in some cases a single tool is used for tracking both. After project inception, First Data will work with DHHS to determine the most appropriate Issue Management Tool for use in the IV&V assessment. As issues are identified during the project lifecycle and documented in the Issue Management Tool, an owner should be designated who can provide the following pieces of information to assist in issue resolution:

- Issue Category – high level operational area impacted by the issue
- Issue Type – sub-category that further defines the impacted area
- Priority – based on the severity of the issue
- Target Date – projected date of issue resolution
- Target Reason - justification for target date

Throughout the course of the project, the First Data Team will generate reports from the Issue Management Tool based on the requirements of the IV&V services. Reports may be generated based on Issue Category, Issue Type, or by Target Date. Data from these reports

may be included in status reports or reviewed in status meetings, particularly those issues which require escalation or input from project leadership.

The designated issue owner, with support from the First Data team, should perform issue analysis to determine the actions necessary to resolve the issue. The issue owner communicates the issue resolution recommendation to the First Data Team. For issues requiring further analysis, the issue owner determines the following:

- Impacts to Cost and/or Schedule
- Impacts to Project Staffing
- Impacts to User and/or Stakeholder Relationships
- Impacts to Existing Risks
- Suggested Resolution

The First Data Team will record the issue resolution recommendation in the Action Plan field of the Issues Management Tool.

Opportunity Management

First Data's experience not only proves our ability to help government agencies succeed, but it also gives us a wealth of insight and knowledge that can benefit the EES and DMA Projects. Our well-rounded experience with many different systems in complex, multi-agency projects enables us to bring best practices, lessons learned, and proven methodologies and tools to help verify the EES and DMA Projects learn from and take advantage of the experiences of other states.

Findings can be positive or negative. Positive findings can be further designated as opportunities or "best practices." First Data understands that in a successful project opportunities can be realized in various ways. Our teams, through detailed analysis, observations, and deliverables review were able to present recommendations and alternatives which have been able to help our clients realize various opportunities such as:

- Increased cost savings
- Increased project efficiency
- Improved product quality
- Improved delivery

First Data has been able to help our clients realize better project efficiency, on-time delivery and cost savings. An example is recommendations to improve JAD session collaboration, decreasing the need to rework any requirements and verifying requirements are gathered up front providing better resource and cost analysis up front.

(c) Deliverable review and reporting of deliverable findings

The First Data deliverable review and assessment methodology is a formal, structured process. This methodology should be applied to the review of all Vendor deliverables. First Data will provide an independent, unbiased, and comprehensive evaluation of the deliverables and services. Our methodology is based on the following tenets:

- **Participate in the full deliverable lifecycle** – Work with the Vendor and Client Agency project staff throughout the entire deliverable development, review, and comment and approval process, beginning with development of the Deliverable Expectation Document (DED) and continuing through submission of a recommendation for deliverable acceptance.

- **Provide input and feedback on a flow basis** – This allows recommendations to be incorporated into subsequent versions of deliverables, which improves the quality of the final product and minimizes the time associated with final reviews. Our ability to do this depends on whether deliverable reviews only occur during scheduled review periods.

- **Use a structured tool to document findings** – This provides a consistent and consolidated format for both First Data and State reviewers and includes a place for the Vendor to respond with justification if they do not agree with the disposition of a deficiency or corresponding recommendations.

- **Produce thorough Deliverable Review and Assessment Reports** – First Data reviews and assesses the readability, comprehensiveness, accuracy, level of detail, and quality of all required deliverables. These reviews are measured against the standards and requirements delineated in the approved DED.

- **Produce final Deliverable Review and Assessment** – This will allow the Project time to review and incorporate IV&V findings and recommendations into the deliverable approval process.

Figure 3.7 – Deliverable Review Process

Explain past challenges and common issues along with the recommendations provided to address the issues. (RFP Section IV, B.2.c.iii)

First Data is an industry leader and is a long time provider of IV&V and Quality Assurance services for the state and local governments. In California, for example, we have been a vital resource for our clients providing services in all phases of eligibility and data management projects. Issues arise on every project and during any phase of the lifecycle. Large, complex IT projects are inherently susceptible to full or partial failure due to them being late, over budget, having poor quality, lacking needed worker functionally, and/or not having implementation backing at the highest decision making levels.

Issues can be concerns such as schedule delays, changes in project scope, depth of deliverables, or newly identified requirements. Issues can also exist with designs, documentation, test scripts, environment configuration, data set-up, or business processes.

Many such issues have the potential to adversely impact the project if they are not resolved properly and in a timely fashion. The First Data Team brings a strong issue tracking and resolution process that effectively addresses issues before they impact the project.

Issue	First Data's Recommended Approach
Team assembled working together for the first time and has varying levels of development methodology understanding.	• Once team is established, use retrospect and storming early with team to make needs known.
Overall system performance	• Implement formal performance tracking procedures • Invest in additional data gathering • Conduct system load testing earlier • Apply capacity planning/analysis techniques • Create Service Level Objectives
Conversion Issues may occur.	• Involve team with test focus within the implementation/conversion plan • Conduct conversion testing with legacy data not "dummy" data • Provide early requirements for system migration, • Include lessons learned involving conversions from legacy systems
Quality of the delivered product	• Involve the team in defining standards in advance • Confirm that standards are formally documented, easily accessible, and easily understandable • Provide early feedback on adherence to standards • Include adherence to standards as an item in walk-throughs • Conduct code reviews • Review results of unit and system testing • Review results of UAT
Ability of developers to complete	• Identify changes in schedule

Issue	First Data's Recommended Approach
system development within specified timeframes	• Assess backlog and determine Project is falling behind schedule • Discuss plan/approach to working through • backlog
System documentation requirements need to meet CMS Gate review requirements.	• Assess the system documentation provided against the Stage Gate checklists • Use the CMS Collaborative Application Lifecycle Management Tool (CALT) to assess how other states have met the requirements using Agile development

Table 3.8 – Potential Issues and Recommended Approach to Mitigation

The First Data Team will continue to follow the progress of the risk or issue and its probability, as well as the status of any mitigation/contingency strategies that have been executed or the issue has been resolved. We provide recommendations to improve the effectiveness of the mitigation plans and discuss these at the Weekly and Monthly Status Meetings. Our risk management approach centers around identifying and dealing with potential threats to the overall project. On a proactive basis, the First Data Team helps the Agency formulate mitigation strategies to alleviate the impact of those threats.

Provide examples of opportunities or positive risks reported in past projects where the customer was able to capitalize. (RFP Section IV, B.2.c.iv)

We have worked closely with our clients to confirm risks are identified and managed in all phases of the project. We have also helped recommend alternatives to help the client realize cost savings and opportunities in other areas. Two examples of risk reports and assessments have been included in Appendix 4:

- **CalHEERS Release Performance Report** - This report provided the client with release performance metrics and recommendation & improvement tracking. This report provided an overview of improvements and changes achieved during a through various phases of the project lifecycle within a specific release. The table of recommendation and improvement tracking provides a detail of issues, recommendations and what was achieved with recommendations applied and the report provides metrics to measure the impact of decisions made.

- **CalHEERS Final eHIT Assessment** - The purpose of the First Data CalHEERS eHIT Assessment Report is to examine opportunities for improvements to the eHIT and supporting CalHEERS Project processes. The report incorporated methodologies used, findings from the observations and analysis. It reports the alternatives and options to the client on changes, providing the client an in-depth view including pros and cons of decision along with a scorecard.

Provide examples of the bidder's deliverable review findings and issue assessments utilized on previous projects. (RFP Section IV, B.2.c.v)

As part of First Data's methodology we complete comprehensive reviews and assessments for our clients. Some examples of past project reviews have been included in Appendix 5:

- **CalWIN Risk Assessment -** The CalWIN Risk Assessment report incorporates purpose scope and approach to the review and analysis of current project risks and provides finding and recommendations to eliminate/minimize project risks. The report also provides some project background and introduction which captures a quick overview of the report contents. The following areas are incorporated as part of the report:

  - ✓ Assessment Findings
  - ✓ Recommendations
  - ✓ Purpose, Scope and Approach

- **Final Assessment of Conversion Plan Tasks Complete Wave 1 -** This report provides and in-depth deliverable review. The report includes requirements analysis and documentation of all deficiencies. Included are recommendations provided on how to change the deliverables to correct all deficiencies and documents.

  - ✓ Deliverable Assessment Methodology
  - ✓ Deliverable Assessment Findings
  - ✓ Acceptance Recommendations
  - ✓ Deliverable Roles and Responsibilities
  - ✓ Deliverable Schedule
  - ✓ Deliverable Requirements
  - ✓ Deliverable Assumptions

- **IV&V Monthly Report** - Indiana Eligibility Determination Services System (IEDSS) - The IEDSS IV&V Monthly Report provides the project summary and overall health. The report has observations, activities, issues risk and decisions. It provides project metrics various areas of the project and includes review of project deliverables It is point in time snapshot providing the client with an in-depth view and includes the following:

  - ✓ Purpose
  - ✓ Summary
  - ✓ Observations
  - ✓ Activities Performed
  - ✓ Planned Activities
  - ✓ Performance metrics
  - ✓ Pending Action Items
  - ✓ Pending Issues

- ✓ Pending Decisions

- **QA Team Observation Regarding Deliverable 33h** – CalHEERS - The deliverable report provides and in-depth review of the deliverable in the following areas:
  - ✓ Deliverables expectation
  - ✓ Missing content
  - ✓ Incomplete or fragmented content
  - ✓ Document quality

3.1.3 IV&V Status Meetings and Reporting

Address the bidder's approach to meeting each requirement in a table that contains the requirement and the bidder's approach to meeting the requirement. (RFP Section IV, B.3.c.i)

The table below details our approach to meeting the following requirements.

	IV&V Status Meetings and Reports Requirements	First Data's Approach
1	Must prepare and submit a weekly status report including activities for the previous week and upcoming activities for the next two weeks that includes the following information: • Summation of project meeting participation including a summary of completed meetings and any recommendations for improvement • Planned project meetings for IV&V participation • Project deliverable review activities • Risks, issues, and opportunities which are new or have been updated since the previous submission • Updated IV&V schedule • Critical incidents summarizing the incident, impact to the project, and a proposed action plan to address the incident	First Data believes in keeping its customers well-informed of project activities, and will work with DHHS to customize the structure and format requirements for weekly project status reports. First Data recommends that, at a minimum, a weekly status report include the following: • Project meeting participation will include minutes from completed meetings that address action plans, issues and any recommendations for improvement • Planned project meetings for IV&V participation • Project deliverable review activities • Risks, issues, and opportunities which are new or have been updated since the previous submission • Updated IV&V schedule • Critical incidents summarizing the incident, impact to the project, and a proposed action plan to address the incident • Other IV&V activities as defined by DHHS

	IV&V Status Meetings and Reports Requirements	First Data's Approach
	• Other IV&V activities as defined by DHHS	
2	Must submit each weekly status report by the DHHS established day and time. DHHS will allow a minimum of one business day from the end of the weekly reporting period for submission.	First Data understands and agrees to submit each weekly status report by the agreed upon day and time.
3	Must facilitate a weekly IV&V status meeting with DHHS identified project leadership.	Weekly status meetings provide a forum for discussing the progress of the project. The First Data Team will validate that project status meetings are scheduled on a weekly basis with project sponsors, stakeholders and any other state or federal partners as required. We will verify that status meetings cover the following items: • Overall and phase-specific project status • High priority risks and issues identified • Tasks in the Project Work Plan that are behind schedule • Status of project deliverables
4	Must prepare and submit a maximum of five business days after month end a monthly IV&V report that includes the following: • Summary of IV&V activities for the past month • Summary of IV&V activities planned for the next month • IV&V assessment of the overall project, schedule, budget, scope, and quality status in comparison to the project teams' reported status clearly identifying any differences along with the reasoning • Additions or updates to executive level risks, issues, and opportunities along with further recommended actions • Summary assessment of project deliverables and work products reviewed in the last reporting period	The First Data Team will produce an IV&V Project Status Report monthly, which includes a summary of work activities and major accomplishments achieved during the reporting period in addition to any problems or issues that require management attention. The First Data Team will work with DHHS to develop the expectations, format, and communication channels for the status report. The status report will include an ongoing project scorecard or dashboard with key metrics to be jointly determined with DHHS. This indicator will advise if there are potential problems with scope, resources, budget or schedule or in the feasibility of achieving a project milestone or deliverable across all of the project components. It will also provide recommendations for solutions and required follow-up actions. In addition, each IV&V Project Status Report will include a current status of all project issues. The Issues Log is the method by which project issues will be documented, communicated, and monitored through resolution at the summary level. This log provides a synopsis and history of issues that the project will use

	IV&V Status Meetings and Reports Requirements	First Data's Approach
	• Other IV&V activities as defined by DHHS	for decision making purposes in status meetings, status reporting and executive meetings, briefings and/or reports.
5	Must facilitate a monthly IV&V report meeting with DHHS identified leadership.	First Data will meet with DHHS Management, identified stakeholders, and leadership to review content of the IV&V report related to both management and technical aspects of the project.
6	Must create the agenda and take the minutes for any IV&V meetings.	First Data understands and agrees to create the agenda and take the minutes for any scheduled IV&V meeting.

Table 3.9 – Approach to IV&V Status Meetings and Reports Requirements

Describe the bidder's process for capturing detailed status on project activities (i.e., scheduled tasks, risks, issues, staffing, communications, etc.) at a detailed level and reporting the information as needed based on the reporting audience. (RFP Section IV, B.3.c.ii)

The scope of the EES and DMA projects dictates the need for formal periodic status reporting to confirm that all project team members are kept informed of overall progress and direction of the project efforts.

Each status report will include a current status of all project issues. The issues log is the method by which project issues will be documented, communicated, and monitored through resolution at the summary level. This log provides a synopsis and history of issues that the project will use for decision making purposes in status meetings, status reporting and executive meetings, briefings and/or reports.

First Data understands that schedule management encompasses the monitoring of project accomplishments against the project schedule, the scheduling of future and current tasks, and the evaluation of the type and level of resources assigned to project tasks. The primary tool for schedule management is the Master Project Work Plan. This may be one file for a project, or a Master Schedule capable of relating many subordinate schedules. The status report may also reflect the following elements which may impact the project schedule:

- Number of tasks on the critical path that have started on time
- Number of tasks on the critical path that did not start on time
- Number of tasks on the critical path that have completed on time
- Number of tasks on the critical path that were not completed on time
- For tasks on the critical path that did not start or complete on time, number of days past the scheduled start or completion date

- Actual level of effort (work hours) compared to planned level of effort for tasks
- Actual resources/positions assigned to tasks compared to planned resources
- Any new tasks or changes in tasks that could affect the critical path
- Changes in task start dates or finish dates

Describe the bidder's methods for determining and reporting overall project, schedule, budget, scope, and quality status (i.e., determining whether a project is red, yellow, or green, and providing defined criteria as to what constitute each type of status). (RFP Section IV, B.3.c.iii)

As part of monitoring and measuring progress of the project, the First Data Team will produce a regular status report, which includes a summary of work activities and major accomplishments achieved during the reporting period in addition to any problems or issues that require management attention. The First Data Team will work with DHHS to modify the currently produced status report to confirm that it provides the content expected in the correct format and will clarify communication channels for the status reports. The status report will include an ongoing project scorecard or dashboard with Key Performance Indicators (KPIs) to be jointly determined. However, standard examples include:

- Process or Completion Timeliness for a piece of work
- Output Volume
- Defect Rate
- Cost Efficiency / Budget Usage

The KPI metrics are flexible to any data DHHS wants to gather. These indicators typically utilize a 'Red, Yellow, Green' scheme to indicate 'Fatal, Problematic, and Adequate', respectively; will advise if there are potential problems with scope, resources, budget or schedule or in the feasibility of achieving a project milestone or deliverable. It will also provide recommendations for solutions and required follow-up actions.

The Status report will encompass a broad view of activities and will also include specific summary data relative to the tasks performed. The status report will include the following information:

- Executive Summary Dashboard
- Schedule and Costs
- Deliverables and Milestones
- Activities Completed or in Process

- Activities Scheduled for the Upcoming Period
- Activities Scheduled for Completion this Period that were not Completed
- Risks/Issues/Concerns
- New or Escalated (triggered) Risks
- Open Action Items
- Recommendations

Provide the bidder's status report templates, including instructions and procedures for completing the templates. (RFP Section IV, B.3.c.iv)

First Data believes in keeping the project leadership and stakeholders well-informed of project activities. Project status reporting will occur weekly and monthly to confirm that accurate information is provided on a timely basis. Status reports will provide updates on project progress.

Weekly Status Reporting

A Weekly Status Report shall include the following:

- **Summary of Work** – details of the work completed during the previous reporting period and any results
- **Deliverable Milestones** – list of the milestones that were met during the reporting period
- **Project Schedule** – including updates as needed
- **Summary of Project Budget** – reviews of actuals to projected, costs, hours and estimates
- **Summary of Proposed Tasks and Deliverables** – details of tasks and deliverables to be performed during the upcoming reporting period
- **Issue Analysis** – list of critical issues
- **Risk Analysis** – tracking information, assessment and mitigation strategies
- **Management Documentation** – issue management and change management, including recommended CAP
- **Dashboard Summary** – tabulation of performance data, as well as work remaining on the project

A sample Weekly Status Report is provided below:

Sample Weekly Project Status Report

A. General Information

Project Name: _____ *Date:* _____
Controlling Agency: _____ *Modification Date:* _____
Prepared by: _____ *Authorized by:* _____

Reporting Period: From: To:

B. Summary of Work

C. CMS Deliverable Milestones

D. Project Schedule

E. Project Budget

Actuals to Projected:
- Costs
- Hours
- Estimates

F. Upcoming Tasks and Deliverables

G. Issue and Risk Analysis

H. Management Documentation

I. Dashboard Summary

Figure 3.8 – Sample Weekly Project Status Report

Monthly Status Reporting

As part of monitoring and measuring progress of the HIX Project, the First Data Team will produce a Monthly Status Report, which includes a summary of the current state of project effort.

The Monthly Status Report will encompass a broad view of the HIX Project and will also include specific summary data relative to the tasks performed. The Monthly Status Report will include the following information:

- Project Name and Information
- Executive Summary
- Task Summary

- IV&V project work product and deliverable assessments completed within the month
- Critical incident reports
- Requirements traceability matrix updates
- CMS and MITA compliance activities
- IV&V work plan updates
- IV&V work products Dashboard Management
- Process and Technical Gap Management
- Risk Management

As the starting point for defining the Monthly IV&V Report, in order to outline the information above, First Data uses the following structure:

1.0 Introduction and Purpose

2.0 Summary

3.0 Observations

- 3.1 Current Observations
- 3.2 Prior Observations
- 3.3 Testing Observations

4.0 Activities Performed

5.0 Planned Activities

6.0 Performance Metrics

- 6.1 Action Items Metrics
- 6.2 Change Requests
- 6.3 Issue Metrics
- 6.4 Decision Metrics
- 6.5 Schedule Review

Each Monthly Status Report will include a current status of all project issues. The Issues Log is the method by which project issues will be documented, communicated, and monitored through resolution at the summary level. This log provides a synopsis and history of issues that the project will use for decision making purposes in status meetings, status reporting and executive meetings, briefings and/or reports.

An example of a status report that could be used as a template for the Monthly Status Report is included below:

Status Report
For (insert reporting period)

AGENCY NAME
PROJECT NAME Project

[This template describes the required contents of the TYPE OF VENDOR vendor monthly reports.]

Executive Summary
[Provide a brief overview of the contractor's support during the reporting period.]

Activity Summary
[This section must contain the information listed below. Contractor format is acceptable, but the requested information must be readily identifiable, by using headings or other means. Work plans that support the activity summary can be attached, and may be referenced to support the activity summary.]

- Planned activities *[Activities that were planned during the reporting period.]*
- Activities completed *[Activities that were completed during the reporting period.]*
- Work in progress *[Ongoing activities that were not completed during the reporting period.]*
- Unplanned activities *[Activities either completed or ongoing that were not planned. Unplanned activities are rare but should be reported if they occur.]*
- Activities scheduled for the next reporting period. *[These are the new activities that are planned to begin in the next month. Work in progress does not need to be repeated in this section.]*

Deliverables this Month

[Show any deliverables that were provided, or should have been provided, during the month. For example, the monthly report for June would probably list the report for May that was delivered in June. Overdue or late deliverables require an explanation.]

Table 1: Deliverables this Month

Deliverable Table	SOW Reference	Date Due	Date Delivered
[Deliverable title, from SOW requirement]	*[Reference, as used in SOW, i.e., task number or unique reference]*	*[SOW due date]*	*[Actual delivery date]*

Deliverables Status

[List all deliverables from the SOW with current status. Each deliverable, whether delivered or due, should be shown. Periodic deliverables do not need to be listed more than once – see example. Other, ad-hoc deliverables should also be listed. These items should also be tied to the SOW requirement that the task fell under. Any concerns or issues relating to deliverables require an explanation.]

Table 2: Deliverable Status

Deliverable Table	SOW Reference	Date Due	Date Delivered
[Deliverable title, from SOW requirement]	*[Reference, as used in SOW, i.e., task number or unique reference]*	*[SOW due date]*	*[Actual delivery date]*
[Example] Monthly Report	*[Example]* Task 1.2 – Status Report	*[Example]* June 1, 2013	*[Example]* June 1, 2012

Schedule Management
[List concerns or issues that are pertinent to the schedule for completion of SOW tasks. Provide tables from the master Project Schedule showing tasks completed during the reporting period and those planned for the next 90 days.]

Resource Management
[At a minimum this section should reflect the baseline vs. actual full-time equivalents for contractor and its primary subcontractors.]

Risk Management
[This section includes an entry for each joint risk that required execution of its Risk Mitigation Plan during the reporting period. It should also include entries for risks with a high probability of future execution.]

Change/Issue Management
[This section lists trend information on Change Request activity on a cumulative basis. The latest month represents total Changes to date, the number "approved", "disapproved" or "in progress". This section also provides trend information on issue activity on a cumulative basis indicating the number "resolved", "unresolved" and "critical issues".]

Financial Management

[The contractor will provide cost performance spreadsheets in this section. Information provided will include baseline estimates versus actual expenditures by task. Any significant variance (greater than 10 percent) from the baseline proposed requires an explanation.]

Figure 3.9 – Monthly Status Report Template

Provide examples of similar weekly status reports used in previous projects. (RFP Section IV, B.3.c.v)

A Weekly Status Report provides an opportunity for to get support and decisions and address any concerns with the project sponsor. We work closely with our clients to tailor our monthly status reports to meet the specific needs of our clients and their projects. Below is a brief description of weekly reports, from past projects, which are included in Appendix 6:

- **Workstream Status Report - Your Health Idaho Health Insurance Exchange(YHI HIX)** - This report was tailored for the project to provide a snapshot of weekly activities completed, planned activities for the upcoming week and new issues and risks for the current period to be discussed and included to the risk register. The report is presented in customer required format for presentation at the project weekly status meetings for stakeholders and sponsors.

- **Weekly PMR Meeting Minutes - Short-Doyle Data Analytics** - The report provides activities with status and comment and also includes project risks and issues.

Provide examples of the IV&V vendor's previous monthly status reports from other projects. (RFP Section IV, B.3.c.vi)

First Data understands that a comprehensive monthly status report serves an important role in keeping project stakeholders, sponsors and staff updated and providing an overview of project progression from month to month. Below is a brief description of past project IV&V Monthly Status reports with examples of the actual report included in Appendix 7:

- **IV&V Bi-Monthly Report – State of Colorado Health Insurance Exchange (COHBE)** - The Bi-Monthly Report tailored for Colorado is detailed report providing, background status and overall health of the project with recommendation to keeps the project on track and on schedule. The report includes detailed information of deliverables reviewed by workstream, status and alternatives.

- **IV&V Status Report – Connecticut Health Benefits Exchange (CT IV&V)** - This report includes overall project health and provides status, findings and recommendation for the project work streams. The report categories are presented in format tailored to meet the needs of the client.

- **IEDSS IV&V Monthly Management Briefing** - This monthly briefing, was tailored for a specific audience, it provides review of project status by providing results from project observations. It discusses current and recommended future activities and performance measures to give a view of project progression. The briefing also presents currents risk and issues trends.

- **IEDSS IV&V Monthly Report** - This report provides a monthly view that is point in time of overall project health. It provides details for current and upcoming activities, observations and testing updates. The report is detailed and tailored to meet the State's IV&V Service Opportunity requirements. The report also includes breakdown of information by release and overall risk and issues. It has a view of deliverables produced and reviewed, defects management, and includes metrics for various project areas including risk and issues.

3.1.4 CMS and MITA Compliance

First Data has a demonstrated history of providing IV&V services to public and private sector entities for more than two decades in support of project certifications and securing enhanced funding. Our successful portfolio of engagements include efforts in support of state agencies that are in the process of or have replaced and upgraded their Medicaid Management Information System (MMIS) and Eligibility and Enrollment Systems (EES) environments, developed various forms of health insurance marketplaces and expanded healthcare service offerings. During this same time, First Data has amassed a wealth of experience related to the development of Enterprise Data warehouses that support state

healthcare initiatives. Our previous engagements have relied heavily upon CMS supplied documents, webinars and guidance which include the previous and current versions of Medicaid Information Technology Architecture (MITA) initiative, previously published Enterprise Life Cycle (ELC) documentation, Enhanced Funding Requirements: Seven Conditions and Standards (2011) as well as the Medicaid Enterprise Certification Toolkit (2007).

Why Choose First Data?

- ✓ *We are experienced in building the necessary relationships between CMS, States, and IV&V*
- ✓ *Our successful projects have occurred since the inception of MITA in 2005.*

With the release of the new Medicaid Enterprise Certification Toolkit (MECT) in March 2016, First Data is presently modifying our processes to facilitate alignment with the MECT. First Data will meet with CMS to come to a common understanding regarding the expected outcomes of the state's current effort to upgrade its eligibility and enrollment environment in light of the recent standards. This common understanding is necessary given the reality that the effort began several years prior to the most recent MECT release. At this time, the EES is expected to be operational in 2017. The current MECT provides much needed refined and targeted critical success factors (CSFs). The First Data Team will incorporate the CSFs into our efforts. The Medicaid Enterprise Certification Life Cycle (MECL) documentation, which was also released in March 2016, addresses the outsourcing of Medicaid functions to third parties. This documentation and suggested approaches will prove invaluable as DHHS moves forward with the Heritage Health initiative.

First Data understands there are primary objectives to your system automation projects, implement them to work properly, and implement them in accordance to CMS standards to secure funding. We can do both of these through our IV&V practice.

The table below details our approach to meeting the following requirements.

	CMS and MITA Compliance Requirements	First Data's Approach
1	Must provide IV&V services for CMS in support of the MECL in accordance with guidance to be released in the new MECT.	CMS sets forth three key activity sets in the MECT: conduct technical design reviews, perform project management reviews and prepare and submit certification progress reports to CMS. With regards to the technical design reviews, these artifacts will include Detail System Designs, Security & Privacy (MARS-E 2.0), Requirements Tractability, and User Acceptance (which must include Performance Testing). In previous IV&V engagements, First Data has performed these technical design reviews and prepared the necessary artifacts which contained our findings and recommendations that were presented to CMS.

	CMS and MITA Compliance Requirements	First Data's Approach
		In completing these tasks, First Data recognizes the importance of maintaining its independence. Independence is best characterized as being both technical independence (reliance upon subject matter expertise on the team and within First Data) and managerial independence (the team is internally directed in consultation with CMS but not directed by the client, vendor or stakeholders). First Data recognizes with the release of the updated MECT, CMS expectations and guidance have changed. The First Data Team will engage CMS and put together a plan to get the EES through the Operational and Certification Milestone reviews. The most important artifacts that need to be addressed are the Certification Progress Reports and the underlying checklists that are key components of the reports.
2	Must periodically, as needed, produce exception based Certification Progress Reports in the format required by CMS. The report must utilize the MECT checklists and MMIS Critical Success Factors (CSFs) and must objectively illustrate the strengths and weaknesses of the project and provide recommendations for correcting any identified weakness.	The Medicaid Enterprise Life Cycle instructs the First Data Team that at a minimum 4 Certification Progress Reports (CPRs) will be required over the life of a project. Given the fact that the engagement may evolve into distinct phases, the number of reports may increase dramatically. If all phases are executed as anticipated and each with its own SDLC, the First Data Team may end up producing multiple report sets. The First Data Team will utilize the MECT Certification Progress Report template supplied by CMS. The First Data Team will make use of the appropriate checklists, appropriateness based on the solution being addressed in the phase. The key checklist effort is the confirmation that the critical success factors are being address/satisfied with the solution. The expected sequence of events will be for the state to populate those parts of the checklist and then turn the checklist to the First Data IV&V Team. The team will complete the checklist and then send it directly to CMS. In addition to the checklist, the CPR will contain sections pertaining to overall engagement progress, remedial activities completed since the last CPR and an updated risk/issue registry.

	CMS and MITA Compliance Requirements	First Data's Approach
3	Must submit the monthly IV&V report to CMS.	In order for the relationship between CMS and First Data to be of value, our First Data IV&V Team's reports to CMS must be independent and objective. First Data expects to provide on-going reports directly to CMS throughout the engagement; which should align with information familiar to the state. Once submitted, the report is only then shared with the state agency. These reports fall into two groups, *Monthly Status Reports* and *Certification Progress Reports*. The First Data Team will be submitting monthly status reports electronically to CMS. The monthly report will provide an executive summary of the previous months events, important milestones achieved or missed (based on published project schedule), risk registry summary and a summary of deliverables. Lastly, the report will apprise CMS of upcoming events such as gate and milestone reviews and efforts underway to provide the necessary documentation to CMS sufficiently in advance of the event. In the case of milestone reviews, a complete listing of expected artifacts and their development status will be provided. If the engagement expands beyond the EES and DNA efforts, the monthly status report will be reorganized accordingly. This is essential because it is reasonable to anticipate some efforts will be further along the life cycle continuum. It is also possible that different engagements will employ different SDLC (Waterfall vs. Agile) which will impact what, how and when information will be reported to CMS. First Data IV&V Team's experience in both Waterfall and Agile in invaluable when establishing the CMS reporting matrix. In today's IT development environments, First Data is seeing organizations taking the best of breed approach, in terms of bringing projects to a successful conclusion rather than committing to one approach for all phases of an engagement. Bringing successful functionality to an environment as soon as possible is an important considering by all parties and the First Data Team is ready to modify its reporting approach.

	CMS and MITA Compliance Requirements	First Data's Approach
4	Must participate in meetings with CMS as directed by CMS or DHHS.	Collaboration is the cornerstone of our IVV efforts. The First Data Team recognizes the importance of Working within a collaborative environment and this extends to participation in any meeting in which CMS is present. The First Data Team will present updates during standing meetings and will also prepare additional information and present this to CMS and all meeting attendees as necessary. It is our experience as an experienced IV&V vendor that it is not only important to attend and present at CMS meetings but to view the other attendees as co-collaborators. It is our opinion that we succeed not as individual entities but as a group. The First Data Team will maintain our current positive professional cooperative relationships with the state, Project Management Office (PMO), implementation contractors and subcontractors.
5	As directed by DHHS, must coordinate and participate in the planning, preparation, and performance of CMS project reviews (Gate Reviews, readiness reviews, certification reviews, etc.).	First Data will work with DHHS to develop and execute the necessary certification activities for each of the named and proposed projects. The publication of the most recent Medicaid Enterprise Certification Toolkit introduces Milestone Reviews to the certification effort. The First Data Team will work with DHHS, the PMO and the appropriate implementation contractor to incorporate Milestone Reviews into the master project plan. The First Data Team will validate that the appropriate milestone and gate reviews are contained within the master project plan with subordinate activities identified and properly resourced. Each project plan will align with the system development life cycle for the related project. We will also work with DHHS and the Project PMO to identify specific roles and responsibilities for each task in the plan.
6	In preparation for certification milestone reviews, must evaluate documents and evidence along with any working modules/code applicable to that particular review, and complete the reviewer comments portion of the relevant Medicaid	The Medicaid Enterprise Certification Toolkit provides 20 checklists to support the certification process, each aligned to a specific Medicaid business area. Taken together, these checklists describe the business objectives for a Medicaid Enterprise System. As an early IV&V activity, the First Data Team will work with DHHS, the PMO and the vendor(s) to review the

	CMS and MITA Compliance Requirements	First Data's Approach
	Enterprise Certification Checklists. The completed checklists are appended to the Certification Progress Report. Progress report must be delivered with the necessary lead time as required by CMS prior to the scheduled MMIS certification milestone review. The certification progress reports must be provided to CMS at the same time they are presented to the state.	certification checklists and tailor them, as necessary, to reflect the specific business objectives of the projects. For example, some objectives may not apply to the project, while DHHS may also add additional business objectives unique to Nebraska. We will also work with DHHS and the implementation contractor to establish the system review criteria for each business objective. To develop the system review criteria, we will draw on the 2015 State self-assessment, IAPD, RFP, system design documents, and our experience in systems certification. Once we have tailored each relevant checklist to meet the unique requirements of the project, we will review these modifications with CMS to gain its agreement. It is critically important to certification that DHHS, its implementation contractor and CMS have a clear, consistent and shared view of the business objectives for each element of the project. Once the checklists are in place, we will monitor the implementation contractors' compliance with the checklists through deliverable reviews and periodic checklist reviews. Our approach is to integrate checklist compliance as *part* of our overall IV&V process.
7	Must periodically submit project progress data to the CMS dashboard on a schedule required by CMS.	Dashboards provide leadership and key stakeholders with a succinct picture of project status and health. They educate the reader as to a project's progress in achieving specific, measureable project objectives. First Data has developed and maintains dashboards both for internal use and for our external engagements. First Data teams have regularly supplied information for presentation on dashboards. Once CMS provides the First Data Team with the necessary reporting metrics, submission format, frequency and location, the First Data Team will begin providing/uploading the information.
8	Must assess impacts of projects to MITA business, informational, and technical architecture maturity.	As part of the initiation and planning phase of the project, the First Data Team reviews five MITA-related documents, including the State Self-Assessment. The

	CMS and MITA Compliance Requirements	First Data's Approach
		team's findings and recommendations will be contained in the initial CPR. Based on the indicated maturity as shown in the As-Is state, the First Data Team expects to see published requirements that, when satisfied, will advance the maturity of the various architectures. If the requirement traceability matrix indicates that requirements are not being satisfied, the First Data Team will update the risk/issue register accordingly.
9	Must track traceability of project activities and requirements through the entire project to CMS critical success factors and certification checklist criteria as applicable to the project to secure ongoing enhanced funding.	An early First Data Team activity would validate requirements. For the EES Project, this has mostly been done. This does not imply that requirements traceability stops, in fact it will be a part of all of our reviews and input in to the processes. There a number of alternative SLDC approaches that are more flexible than Waterfall but well suited for many development efforts. The First Data Team has experience working in collaboration with teams using more flexible approaches. Regardless, of the approach employed, it is still important to have as many requirements identified and confirmed as soon as possible as well as a confirming that the necessary development components (project backlogs, sprint backlogs, user stories, daily stand-up meeting and sprint reviews) are established, well documented and understood by all relevant stakeholders. Once the requirements are reviewed and clarification received (as necessary) the First Data Team will monitor the progress of addressing the requirements via a traceability matrix. An important aspect of the on-going monitoring effort by the team is to validate that the solution being developed and the decisions being made during implementation, planning and development are promoting the seven conditions and standards for enhanced funding. Given the eleven distinct phases outlined in this RFP, there appears to be a number of opportunities for the solutions put forth to embrace all seven conditions and standards. First Data will be monitoring the project schedule,

	CMS and MITA Compliance Requirements	First Data's Approach
		participating as a regular attendee, reviewing state and vendor deliverables throughout the month and then assembling its findings finding in the Monthly IV&V Stats Report which is provided to CMS. Once the monthly report is provided to CMS, an electronic copy is available to the State, vendors and appropriate stakeholders. How these reports (monthly status and CPR) are distributed is up to the discretion of the State. Often a document distribution matrix is developed and maintained by the PMO and the First Data Team will follow the matrix's instructions. The First Data Team will utilize the MECT Certification Progress Report template supplied by CMS. The First Data Team will make use of the appropriate checklists, appropriateness based on the nature of the engagement. The most important aspect of the checklist work effort is the First Data IV&V Team's completion of checklist's critical success factors. The team will indicate how the state and vendor(s) are doing in meeting the critical success factors. The First Data Team will complete the checklist(s) and then send the CPR directly to CMS. Once submitted to CMS, the First Data Team will provide copies of the report to the State, appropriate vendors and relevant stakeholders. In addition to the checklist, the CPR will contain sections pertaining to overall engagement progress and remediation activities completed since the last CPR. Remediation activities may be necessary when at the time of the last checklist submission, expect success factors had not been realized. The report will also contain updated summary and detailed risk/issue registry information.
10	Must perform all functions required by CMS for all CMS reviews.	First Data will utilize the IV&V Monthly Status Report and the MECT Certification Progress Report as the primary artifacts for reporting all IV&V functions are being completed as expected by CMS. The First Data Team will make use of the appropriate checklists, appropriateness based on the nature of the engagement. The most important aspect of the checklist work effort

	CMS and MITA Compliance Requirements	First Data's Approach
		is the First Data IV&V Team's completion of checklist's critical success factors. The team will indicate how the state and vendor(s) are doing in meeting the critical success factors. The First Data Team will complete the checklist(s) and then send CPR directly to CMS. In addition to the checklist, the CPR will contain sections pertaining to overall engagement progress and remediation activities completed since the last CPR. The report will also contain updated summary and detailed risk/issue registry information.
11	Must coordinate certification activities for the project including review of certification packet materials from the DMA implementation contractor. Must evaluate and make recommendations about the state artifacts that are required for MMIS certification milestone reviews. A list of required artifacts is included in the CMS Medicaid Enterprise Certification Toolkit.	The First Data First Data Team will develop its own IV&V Project Plan for the Nebraska engagement. The project plan will be modified (expanded) as necessary to accommodate the expected multiple engagement phases for the projects. It is our experience that a master project plan under the control of the PMO is the best way to facilitate coordination among distinct vendor project plans. The First Data Team will review the individual state and vendor's project plans (or master project plan if that be the case) to validate that the expected deliverables are accounted for, scheduled/sequenced and properly resourced. All individual project plans should align with MECL phases, unless otherwise directed by DHHS. Each phase (Initiation and Planning, Requirements, Design and Development, Implementation and Operations) has one or more associated CPRs. In all cases, a CPR is required to be submitted to CMS prior to one of the Milestone Reviews. As stated in other parts of our proposal, the First Data Team will utilize the CMS-supplied CPR template. The template either natively contains or call be modified to contain all of the necessary reporting topics necessary for the upcoming Milestone Review. The State and vendor deliverables are reviewed and reported on in the IV&V Monthly Status Report. In addition to reporting on reviewed deliverables, the monthly report contains a section that provides information and updates regarding expected

	CMS and MITA Compliance Requirements	First Data's Approach
		deliverables that were not presented during the reporting period. The IV&V's findings and recommendations presented in the monthly status report are also included as part of the CPR. The inclusion is predicated on the relevance of the deliverable to the impending milestone review.
12	Must review all new or updated documentation, guidance, and rules promulgated by CMS applicable to the project and provide summary impacts to the project along with any recommendations.	Members of the First Data Team as well as the larger First Data's *Center of Excellence's Assessment Practice* have access to CALT. The *Assessment Practice* group meets on a bi-weekly basis, providing a forum for commutating changes in policies and information captured in discussions with CMS on other First Data engagements. The composition of the Assessment Practice also includes senior First Data Security and Privacy resources. These are invaluable resources to the First Data Team given the nature of the data being captured, stored and used in Nebraska. First Data normally handles these types of updates by adding a section to the IV&V Monthly Status Report. Once submitted to CMS, this report is available to state leadership, the PMO, vendors and appropriate stakeholders. In instances where there is a time sensitive component to the update(s), the IV&V PM may request a meeting to apprise leadership and impacted parties.
13	Must perform any IV&V services and roles required by CMS or DHHS necessary to secure the enhanced funding.	Beginning with the *Enhanced Funding Requirements: Seven Conditions and Standards* document in 2011 and continuing in subsequent publications, CMS has been abundantly clear as to its expectations of states seeking enhanced funding for projects. Given the eleven distinct phases outlined in this RFP, there appears to be numerous opportunities for the solutions put forth to embrace all seven conditions and standards. The origins of current checklists provided in the MECT are based in MITA, one of the 7 conditions/standards. As stated earlier in our proposal, there are twenty checklists included in the MECT. CMS made the decision to duplicate ten checklists and simply change the order within a given checklist based on the checklist's usage, hence the increase to twenty. One of

	CMS and MITA Compliance Requirements	First Data's Approach
		the two sets is expressly organized the usage on an MMIS engagement, the other for non-MMIS engagements. Depending on the engagement's nature, the First Data Team will use the appropriate checklist set. The sets include the critical success factors that must be satisfied. At least four times during the MECL, CMS expects Certification Progress Reports. The First Data First Data Team is responsible for presenting its review of project artifacts, evidence and completes the reviewer portion of the checklist. This effort is done after the State has entered its contribution to the report. Once both parties have completed their sections, the First Data Team will submit the Certification Progress Report directly to CMS. CMS reserves the right to demand non-scheduled Certification Progress Reports based on findings provided to CMS by the First Data Team or at its own discretion.

Table 3.10 – Approach to CMS and MITA Compliance Requirements

Describe the bidder's understanding of CMS' expectations for an IV&V contractor and approach to compliance with CMS expectations. (RFP Section IV, B.4.c.ii)

First Data has a demonstrated history of successful IV&V efforts, as outlined in Section 2.8 describing our Corporate Experience. The First Data Team takes the position that when functioning in the capacity of the IV&V contractor; they are functioning as a conduit of timely, accurate and objective information to CMS. First Data works tirelessly to make certain that the relationship and information shared between First Data and CMS is devoid of outside influence. As stated earlier in our response, we strive to develop and maintain a collaborative relationship with all key parties but First Data clearly understands that the development and maintenance of the First Data/CMS relationship is paramount.

First Data has a clear understanding of CMS's expectations of an IV&V contractor.

- As contractor, First Data must build and maintain the necessary relationships in order to have access to all meetings necessary to provide feedback to CMS.
- In addition, an important aspect of our efforts will be the review of all key documents (requirements, traceability matrices, risk registry, project plan, and test results).

- Given that this engagement may well end up being a series of distinct, yet related engagements, the First Data Team will need to prepare distinct deliverables for each engagement to satisfy CMS's expectations.

With the introduction of the updated Medicaid Enterprise Certification Toolkit, First Data will build upon its previous certification knowledge and experiences in providing information prior to the appropriate milestone review.

Experience tells us that the better informed CMS and its designees are about the project as it enters a milestone review, it better the opportunity for a successful outcome.

Describe in detail the bidder's approach to supporting the CMS gate review process for the EES project. (RFP Section IV, B.4.c.iii)

First Data's experience working with MMIS and other large systems that must be certified by CMS has taught us that the most effective way to gain certification quickly and easily upon system completion is to begin planning for certification early in the system development lifecycle. Rather than view the MMIS Certification Final Review as discrete period within the project schedule, we view the Final Review as an ongoing task, with a period of intense focus and effort and the end of the project.

CMS certifies systems to confirm they meet federal programmatic requirements, as well as the technology and functional requirements to receive enhanced Federal Financial Participation (FFP). In general, the First Data Team will support DHHS by conducting preliminary certification reviews to confirm the system:

- Meets minimum requirements, functions, and objectives of Part 11 of the State Medicaid Manual (SMM), Part 11, Chapter 2, Sections 11210 – 11260 – Approval of MMIS Systems and Chapter 3, Sections 11375 – Minimum Required Data Elements (see Appendix A and B)
- Satisfies the terms of the State's APD and subsequent updates
- Meets functional area descriptions in the RFP including Contract Amendments
- Operates in compliance with regulations and policy for 75 percent FFP

During the certification process, DHHS, with support from First Data, will present documentation demonstrating each EES system is operational, processing all data and reports, as of the requested date of certification.

First Data will support the following major activities as part of the certification process:

First Data has provided the following attestations to CMS as a part of legacy system testing results:

- ✓ Data Sharing Hub (DSH) H15 Account Transfer Enhancement (2.3.2)
- ✓ Data Sharing Hub (DSH) Verify Lawful Presence (VLP) testing
- ✓ Payment Error Rate Measurement testing for multiple Rounds

- **MMIS Pre-Certification Training** – First Data will facilitate training that will establish a firm background of the needs and reasons for MMIS certification. The Pre-Certification Training program will take DHHS through the Certification process, highlighting in detail, important areas, i.e., responsibilities, teamwork, system readiness, needed documentation, and Certification checklists folders.

- **Submission of a Letter Requesting System Certification to CMS** - First Data will assist DHHS in initiating the Federal Certification review process by submitting a letter requesting Certification of the MMIS for continued enhanced FFP. The letter requesting certification must indicate to CMS that the MMIS operationally meets the requirements of Part 11 of the SMM.

- **Submission of Documentation to CMS** – First Data will assist DHHS in compiling and submitting all necessary documentation to CMS.

- **CMS Pre-Certification Visit or Conference Call** - CMS may conduct a one and one-half day on-site Pre-Certification visit. At this time, First Data will assist DHHS in presenting the Nebraska MMIS to CMS.

- **CMS On-site Certification Review** – First Data will support the on-site review of DHHS's MMIS to confirm that the system meets the requirements documented in Part 11 of the State Medicaid Manual including the CMS Certification Review Checklist. DHHS should provide documentation that reflects production dates to support the requested certification date, demonstrating that the entire system, including all claim types, has been operational as of the requested date of certification.

- **Exit Conference** - At the conclusion of the on-site Certification Review, CMS will hold an exit conference with DHHS. First Data will attend if requested by DHHS.

- **Certification Decision** - Following the on-site Certification Review, the CMS team will review any additional documentation requested and subsequently provided by DHHS, and any items that needed clarification. CMS will prepare their Certification report and recommendations; they generally make their decision within 60 days. A letter, with their report, will be sent to the Agency, through the Regional Office.

We will also work with DHHS and CMS to understand the impact of CMS' "Seven Standards and Conditions", as we expect additional guidance from CMS as to how it will evaluate compliance among state systems.

Describe in detail the bidder's approach to coordination of the CMS certification of the DMA project. (RFP Section IV, B.4.c.iv)

The Data Management and Analytics (DMA) project will be a dramatic paradigm shift in the way the in which the state executes the Medicaid and CHIP programs. This project will have a profound impact on every business process currently executed by DHHS. The most dramatic change will be the outsourcing of FFS claims adjudication and payment. In

addition, a significant number of other business processes will be outsourced. As but one example, predicated upon the information supplied within the RFP, MLTC intends to migrate fee-for-service claims adjudication from the Nebraska MMIS to the contract of one of the HMOs already providing healthcare services to a portion of the Nebraska Medicaid population. The paradigm shift will necessitate the shift of large amounts of legacy claims and reference data. CMS will expect that all MMIS checklists be utilized during this effort.

One of the first things that needs to be understood by the First Data Team is the system development life cycle approach (Waterfall vs. Agile) for the DMA Project. This approach will dictate how the First Data Team will structure its oversight and review. Verification and Validation will be complex for infrastructure that resides outside of the DHHS footprint. The outsourcing aspect of this effort adds a high degree of complexity to subjects such as claims, service authorization, third party liability, security, legacy data and interfaces. These topics are typically resource intensive and may be more so due to the fact that several IT environments will be outside the control of the state.

The First Data Team will utilize the Certification Progress Report (CPR) template, MECT, Appendix D, Certification Progress Report Template. The MECL indicates a minimum of four Certification Progress Reports (CPRs) are expected by CMS to be submitted by the First Data IV&V Team. The initial CPR will be submitted by the First Data Team to CMS prior to the Project Initiation Milestone Review. With this Report, First Data Team will provide CMS a review of artifacts and work efforts listed in MECT, Appendix B, Required Artifacts List, 2016.

Depending upon the SDLC approach, there are between twelve and fourteen artifacts reviewed and commented on by the First Data Team. Several critical documents are reviewed in the initial CPR, including the MITA Self-Assessment, state goals/objectives, and security.

At least two CPRs will be prepared by the First Data Team and submitted to CMS prior to each Operation Milestone Review. These CPRs will build upon previous CPRs and will make greater use of the MECT checklists. The checklist provide CMS with a clear understanding of how the effort is meeting the critical success factors associated with the business processes referenced in the checklist. If critical success factors are not being met creating a possible issue, the CPR will provide CMS with the mitigation plan to address the issue. An updated risk registry is also supplied as part of the CPR.

A final CPR is provided prior to Final Certification Review. Depending upon the SDLC deployed, there may be a series of Operational Milestone Reviews and MMIS Certification Milestone Reviews. The First Data Team expects that based on the information supplied in the RFP there could be as many as eleven Operational Milestone Reviews and eleven Certification Milestone Reviews. The total number may decrease based on when various phases are completed and ready to become operational.

Describe the bidder's approach to assessing the impacts of a project on MITA maturity levels. (RFP Section IV, B.4.c.v)

The First Data Team will begin with its review of the State self-assessment, submitted March 19, 2015. The assessment will indicate the present state and the desired state. The Team will then look at the particular phase of the engagement (eleven are anticipated over time) and align the phase to the appropriate MITA business area(s). As described earlier the First Data Team will be reviewing the functional and non-functional requirements associated to the phase's solution. Our Team can then make an educated decision as to the solution's ability to advance from the present state to the desired state. This decision will be based on comparing the actual scores from one or more of the matrices (Business, Informational and Technical) to the anticipated functional improvements achieved by a specific phase's solution. We recognize that given the fact that engagement will occur in multiple phases, it may be necessary for the State to revisit the initial self-assessment and update its reported maturity levels. The First Data Team will advise the State how to accomplish this task.

There are aspects of maturity that First Data is mindful of as part of IV&V, related to MITA and the Seven Conditions and Standards. Obviously, MITA is one of the Seven but as the engagement phases are successfully completed, CMS needs to be apprised and the State deserves recognition for advancing along the maturity continuum.

Describe the bidder's approach to monitoring for documentation, guidance, and regulations from CMS. (RFP Section IV, B.4.c.vi)

As stated earlier in our proposal, members of the First Data First Data Team as well as the larger First Data's *Center of Excellence's Assessment Practice* have access to CALT. The Assessment Practice group meets on a bi-weekly basis. These meetings provide a structured forum for communicating changes in policies and information captured while conducting research and/or in discussions with CMS at other First Data engagements. The composition of the Assessment Practice also includes senior Security and Privacy resources. These are invaluable resources to the First Data Team given the nature of the data being captured, stored and used in Nebraska.

In addition, First Data is a member of the Private Sector Technology Group (PSTG). PSTG partners with CMS to organize webinars throughout the year to educate attendees on proposed changes in policy and publications. Most recently, PSTG hosted a webinar specifically on the recently released MMIS Certification Toolkit. The First Data IV&V Team's participation with PSTG and the assessment group keeps the team current on changes in CMS policy expectations that may impact the DHHS engagement.

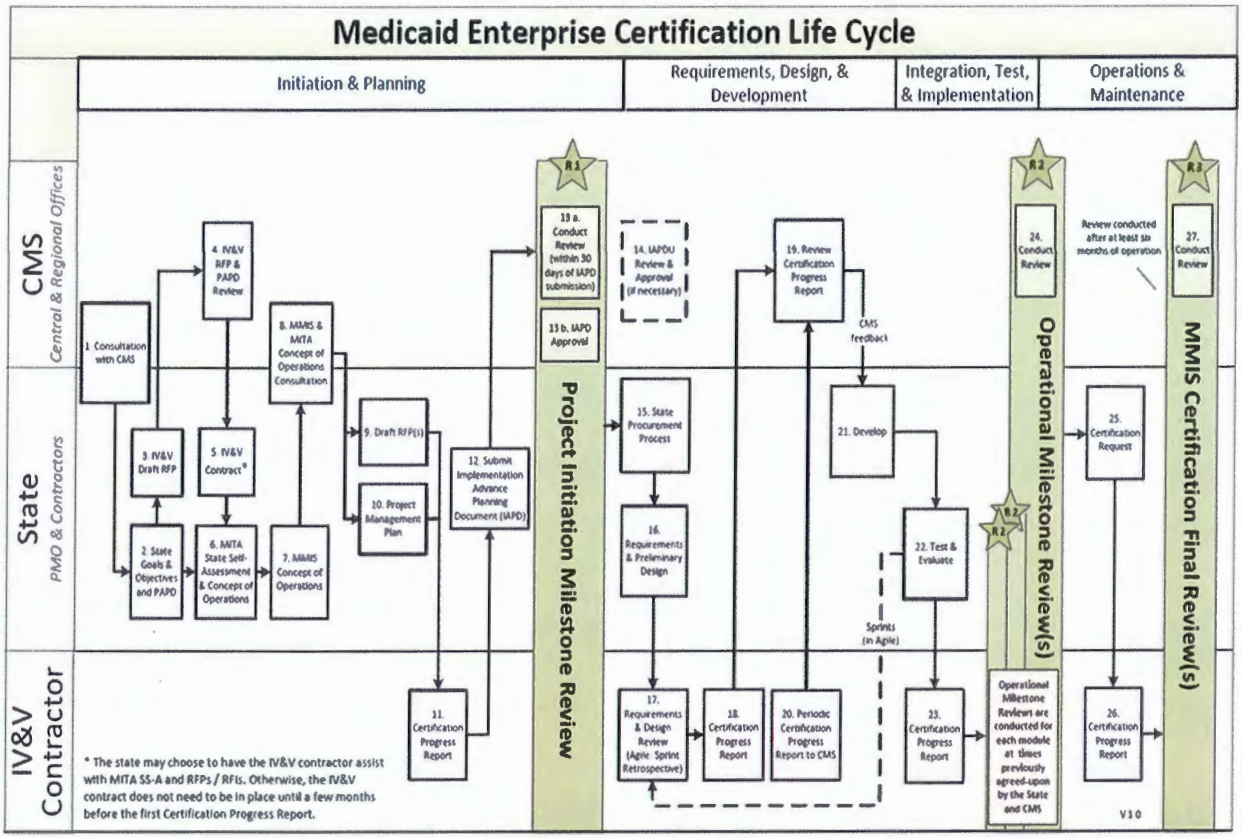


Figure 3.10 – Medicaid Enterprise Certification Life Cycle

3.1.5 Operational and System Readiness

Address the bidder's approach to meeting each requirement in a table that contains the requirement and the bidder's approach to meeting the requirement. (RFP Section IV, B.5.c.i)

Operational and System Readiness defines the point at which a developed system, organization, and affected stakeholders are sufficiently prepared to implement a change. Too often, insufficient preparation stems from an insular vision resulting in unsatisfied project goals and objectives. It is important to recognize that successful operational readiness goes far beyond the system and is the culmination of a process of preparation, review and scrutiny that span the project life cycle.

The First Data Team has experience from both sides of the readiness picture – system readiness preparation and IV&V. This experience gives us strong perspectives to be effective and proactive in our approach to IV&V. Not only does First Data have a proven methodology, but a depth of expertise we can call upon to facilitate project success. We bring:

- **Experience** – We both understand the IV&V process and have considerable demonstrated success

- **Skill** – Qualified, experienced staff are the core of our success
- **Depth of Resources** – We have acquired a library of refined tools and assets to facilitate IV&V project work to every project and are committed to DHHS success.

The table below details our approach to meeting the RFP requirements.

	Operational and System Readiness Requirements	First Data's Approach
1	Must assess project testing activities including test scenarios, cases, and results including traceability of testing to project requirements. Assessment must include whether additional test scenarios or cases are needed to sufficiently test the project requirements.	First Data is well versed in both the performance and review of testing activities and deliverables. We recognize that testing effectiveness and scope of work are governed by time and budget constraints. We also understand the balance between full test coverage and that which is sufficient to adequately test the project requirements. First Data employs the following approach for assessment of vendor testing to confirm completeness, accuracy, and efficacy. **Vendor Testing** • Evaluate the vendor's Test Plan to verify inclusion and completeness of all required components to include goals and objectives, methods, approaches, test requirements (including data set and environment), detailed test descriptions, defect reporting and resolution process. • Assess vendor testing approach to confirm: ✓ Test planning is based on requirements and design specifications to meet intended purpose ✓ Test scheduling and resource allocation are adequate, appropriate and reasonable ✓ The configuration management plan is complete, maintained, and adhered to ✓ Validate the requirements traceability matrix to confirm that test cases adequately test system requirements and that all requirements are tested. ✓ The detailed testing process is complete, accurate, and proper including ✓ Defects are accurately captured, tracked, and resolved • Review test preparation to validate that test environments replicate production, proper tools are employed, appropriate supporting processes are in place, and adequate resources (e.g. staff) are allocated to support testing. • Monitor test efforts to verify adherence to test

	Operational and System Readiness Requirements	First Data's Approach
		procedures and witness record of test results. • Review and assess executed tests to determine the completeness of testing, accuracy, and efficacy of vendor testing efforts. • Report overall testing findings so they may be shared with DHHS and the vendor. First Data uses IEEE Standard 829-2008 as a guideline to assess test methodology with the approach for planning, preparing for, executing, and reporting on all test phases as documented in the vendor master test plan. First Data will closely collaborate with DHHS in the specific configuration of our assessment to confirm that all processes are thoroughly reviewed. **UAT Testing** • Evaluate the DHHS UAT Plan for completeness, reasonableness of approach, effectiveness and adherence to standards* • Assess the UAT schedule for structure and reasonableness of timing and resources • Verify presence of UAT Training Plan and validate adequate staff training • Verify the completeness, relevance, effectiveness and accuracy of testing environment, scenarios, scripts, and test cases. • Validate that testing incorporates all appropriate stakeholders to verify proper perspective **Independent Testing** This step may be performed at the request of DHHS to independently validate the quality of implementation contractor testing. Results from this independent testing would be compared to those obtained by the DDI. • This process duplicates the testing process of the implementation contractor and includes: ✓ Test planning ✓ Test environment preparation ✓ Test execution ✓ Defect Management ✓ Test Maintenance ✓ Test Reporting *The standards employed in First Data IV&V project work

	Operational and System Readiness Requirements	First Data's Approach
		are drawn from the following recognized standards bodies: ✓ The Project Management Institute's (PMI®) ✓ The Institute of Electrical and Electronics Engineers, Inc. (IEEE) ✓ The International Organization for Standardization (ISO) ✓ The International Electro technical Commission (IEC)
2	Must assess defect resolution and retesting activities to validate defect was appropriately resolved.	The First Data Team is committed to confirming that the appropriate systems and controls are in place prior to system deployment. Determining the severity and appropriate level of resolution to system defects is a key element in operational readiness. Drawing on past experience and industry standards, First Data will: • Validate that System and User Acceptance Test Plans contains valid processes and tools for defect classification and reporting. • Verify the defect reporting tool: ✓ Uniquely identifies the defect ✓ Defines fields required for each defect ✓ Identifies metrics and trends related to the defect ✓ Classifies and categorizes the defect level of severity ✓ Defines the resolution/mitigation strategy ✓ Captures the regression testing process and results • Verify that defect resolution processes are aligned with the Master Test Plan. • Review test configuration to validate that appropriate stakeholders are involved in test execution and tracking to account for all perspectives. • Monitor vendor testing and UAT efforts to validate that identified defects are logged and classified according to established protocols. • Periodically review the defect tracking tool to verify that the appropriate action has been taken to resolve or mitigate any recorded defects.
3	Must develop and submit a comprehensive System and Business Operations Readiness Review Plan work product for each project for Department approval a minimum of 90 days prior to the acceptance testing	The purpose of Operational Readiness Review (ORR) is to satisfy federal partner oversight groups that the developed system is operationally ready and prepared to support the project requirements. By working with DHHS and vendor partners, First Data will develop a System and Business Operations Readiness Review Plan that defines the what, how, and timing of validating operational readiness.

	Operational and System Readiness Requirements	First Data's Approach
	schedule date in the project work plan.	The core of the First Data's approach to the ORR Plan is a checklist process used for the development of a go-live recommendation and support of a go-live decision. The checklist process defines the necessary functionality and scenarios to determine readiness in the areas of: • System readiness • Staff training and support • The number and nature of known defects • Adequacy of security processes First Data includes the following content as part a standard ORR Plan: • Introduction and Purpose – defines the project details, purpose, and the scope of intended use • Roles and Responsibilities – defines the teams, plans, and responsibilities • Readiness Assessments – defines the operational areas, activities to be conducted, and measurement processes and metrics; this entails sections for: ✓ Organization Readiness ✓ User Readiness ✓ Data Readiness ✓ Technical Readiness ✓ Implementation Readiness • Criteria Assessment - The criteria and thresholds for the determination of a Go/No-Go decision First Data will submit Readiness Review Plans no later than 90 days prior to the scheduled date of acceptance testing.
4	Must conduct a system and business operational readiness review and assessment and provide the results to DHHS.	The First Data Team will conduct the Operational Readiness Review and Assessment according to the prescribed and approved Plan. First Data includes the following components in the ORR assessment: • Introduction and Purpose – provides a summary of the project, including the business need, purpose, and defines the project stakeholders • Roles and Responsibilities – defines the individuals by name, their role in conducting the activities contained in the plan, and the responsibilities assigned to the named party

	Operational and System Readiness Requirements	First Data's Approach
		• Operational Readiness Review (ORR) – defines the components and process conducted during the ORR. The ORR consists primarily of checklists used in conducting oversight of the implementation. The checklists include functionality, scenarios, factors for consideration, and observations for each business area. The First Data team employs the use CMS checklists from the MECT, where applicable • Project Artifacts and Comments – defines any additional source documentation beyond the physical review process • Assumptions/Constraints/Risks – identifies any assumption used in conducting the review process, identifies defined risks as a result of the operational readiness demonstration, and articulates the shortcomings of the system demonstration. The First Data Team will report the results of this review to DHHS and CMS in accordance with 45 CFR 95.626.

Table 3.11 – Approach to Operational and System Readiness Requirements

Describe the bidder's approach to operational and systems readiness. (RFP Section IV, B.5.c.ii)

First Data will work with the implementation contractor, the DHHS PMO, key State personnel and interface partners to verify systems are stable and ready to implement; staff are prepared to conduct the business of serving Nebraska's most vulnerable using the new systems; and required tools are in place to facilitate the transition. A Go/No-Go process facilitates the evaluation of implementation readiness, identifies any incomplete tasks, outstanding items or concerns, and the implications of not completing those tasks or resolving those items or concerns prior to Go-Live.

A final Go/No-Go meeting will be conducted to assess the overall readiness for the EES and DMA implementations. The respective implementation contractor and the First Data Team will present their Go/No-Go recommendations and, as appropriate, certification letter(s) that the systems are ready for implementation. Key State personnel will make the final Go/No-Go decision based upon the evidence provided during this meeting. There are several inputs that contribute to the Go/No-Go decision process, including:

- Implementation contractor and IV&V vendor status reports
- Open risks and issues
- Implementation contractor project plan and work plan

- Implementation readiness checklist

Implementation Readiness Checklist

The fundamental purpose of the readiness checklist is to help key stakeholders determine if they are ready for system implementation. The checklist serves as a mechanism to clearly understand the status of each readiness task, outstanding items and evaluate the risk of proceeding.

The readiness checklist includes metrics that can impact the overall success of the implementation, and the status of these items is tracked using "stoplight" indicators (shown in the example below). Open items on the readiness checklist may not be 100% complete, have a red or yellow status, or fall outside a defined threshold at the time of the final Go/No-Go meeting. The items on the list can be utilized to assess if any item or combination of items exceeds the acceptable risk threshold and thus jeopardize the implementation of the system.

The readiness checklist covers specific areas of readiness with defined criteria, targets or thresholds, the process by which the measurement is taken, when data associated with the measurement is collected, and whether or not a specific measurement is associated with a specific project requirement. These metrics are reviewed at defined intervals, and during each review, they are assigned a status of Red, Yellow or Green ("stoplight reporting") depending on the progress or status of the metric. Determining the stoplight status of a metric is not an exact science, as there are both qualitative and quantitative aspects that can impact the status. The status can also change from a "Green" to a "Red" depending on progress or lack thereof, or if a new issue has surfaced.

Metrics

IN FSSA IEDSS IV&V Monthly Dashboard						
Metrics	Description	Red	Yellow	Green	Jan-2013	Feb-13
Deliverable Quality Index	Measures the quality of DDI Vendor's deliverables based on number of critical and high priority defects found in the first review of the					
Project Schedule		>=10	10>x>3	<=3	31	0
Project Management Plan		>=10	10>x>3	<=3	17	0
Monthly Status Report		>=10	10>x>3	<=3	2	0
Initial Risk Assessment		>=10	10>x>3	<=3	1	0
Communication Plan		>=10	10>x>3	<=3	0	0
Deliverable Defect Resolution Quality Index	Measures the quality of Deliverable fixes based on the total number of defects remaining in resubmitted Deliverable					
Project Schedule	# defects remaining in resubmitted Deliverable				4	0
	# defects found in prior reviews				39	39
	Index	>=25%	25%>x>10%	<=10%	10%	0%
Project Management Plan	# defects remaining in resubmitted Deliverable				5	0

Figure 3.11 – Example of Stoplight Reporting

The readiness checklist is an Excel spreadsheet that addresses various criteria including but not limited to:

- Change readiness
- Training
- Interfaces
- Conversion
- Application development through UAT
- Application infrastructure
- Client correspondence
- Reporting
- Service delivery

The readiness checklist provides both qualitative and quantitative measures of readiness we will track in the months and weeks leading up to implementation. First Data can assist in defining parameters and criteria for acceptability and help determine the appropriate status. Some examples of acceptability criteria include:

- Percentage of staff that still need to complete a training course to be certified (Number of staff certified to date in relation to the total number of staff)
- Percentage of data converted successfully - did the data convert within the acceptable fallout threshold?
- Percentage of site preps completed

Provide an example of a readiness review plan utilized for other projects. (RFP Section IV, B.5.c.iii)

An example of a readiness review plan is found as Appendix 8. This example was taken from the Louisiana DCFS project.

- **The Louisiana DCFS Go/No-Go Process** – describes how to manage and track project milestones in preparation for implementation. The process describes the requisite checkpoints needed prior to Go Live to verify the project is on track, elevates any known risks, and helps to eliminate surprises that can cause delays.
- **DCFS CAFE Release 1 Readiness Checklist** – is a sample checklist from Louisiana that shows stoplight reporting related to project areas and tasks and the intervals in which the state chose to assess each item.

Provide examples of operation and system readiness review reports used on previous projects. (RFP Section IV, B.5.c.iv)

Examples of operation and system readiness review reports are found in Appendix 9.

- **ID IVV Operational Readiness Review Report** – First Data provided an Operational Readiness review to Idaho in preparation for the implementation of their Health Benefit Exchange. The document includes our observations in specific areas and highlights specific risks to the overall success of the implementation.

- **Riverside CCC Readiness Assessment –** First Data provided detailed analysis and recommendations to our client in the areas of Business Model, Operations, Business Process Management and Change Management.

3.1.6 IV&V Deliverables and Work Products

Address the bidder's approach to meeting each requirement in a table that contains the requirement and the contractor's approach to meeting the requirement. (RFP Section IV, B.6.c.i)

First Data has broad experience and a methodology which has been proven highly effective in a portfolio management environment and has been applied to some of the largest system integrators in the country. Through our experience we have developed templates, checklists, and best practices that are drawn upon to standardize processes and provide clear, integrated, uniform client reporting. These tools allow First Data to effectively identify and consolidate findings across projects, identify key issues and deliver comprehensive yet concise client reports.

The table below details our approach to meeting the IV&V Deliverables and Work Products requirements.

	IV&V Deliverables and Work Products Requirements	First Data's Approach
1	For each project, must fulfill all IV&V contractor responsibilities and submit a monthly deliverable including activities and work products completed within the month: • The Monthly IV&V Report • Weekly Status Report materials for the month • IV&V project work product and deliverable assessments completed within the month • Critical incident reports • Requirements traceability matrix updates • CMS and MITA compliance activities • IV&V work plan updates • IV&V work products	First Data has a proven ability to deliver IV&V reporting in a clear and timely fashion. Our methodology has proven effective on singular IV&V engagements and within a portfolio management environment. We accomplish this with skilled and knowledgeable staff and the use of standard processes and templates, where possible. As discussed in earlier sections of this proposal, First Data has established a close relationship with EES project vendors and our client to foster project success. By establishing a spirit of collaboration, we integrate with existing work processes to make our efforts as transparent as possible facilitating the overall execution and delivery of all work efforts. By being part of the process and providing interim feedback according to the integrated project schedule, the First Data approach promotes timeliness in the delivery of work products. We will leverage these relationships to push the EES project toward successful implementation and to support the DMA and complementary projects envisioned to achieve DHHS's

	IV&V Deliverables and Work Products Requirements	First Data's Approach
		goals. First Data also uses standard reporting and work product formats. Using this standardized approach allows First Data to quickly and cleanly consolidate findings and information from multiple projects to a singular report. This style of reporting also provides a familiar view for the client which improves readability, eases navigation to find critical information, and employs standard metrics, where applicable. First Data verifies the completion and timely delivery of all the reports within the scope of our work. The following approaches will be used in support of contracted activities: **Monthly IV&V Report** To facilitate timely integration and approval of monthly reporting, First Data employs: • Standard, integrated reporting of inputs • Integration of IV&V activities to facilitate timely delivery As the starting point for defining the Monthly IV&V Report, First Data uses the following structure: 1.0 Introduction and Purpose 2.0 Summary 3.0 Observations 3.1 Current Observations 3.2 Prior Observations 3.3 Testing Observations 4.0 Activities Performed 5.0 Planned Activities 6.0 Performance Metrics 6.1 Action Items Metrics 6.2 Change Requests 6.3 Issue Metrics 6.4 Decision Metrics 6.5 Schedule Review In addition to providing a summary of any of the activities listed immediately hereafter, First Data will include, as an appendix, any work products completed

	IV&V Deliverables and Work Products Requirements	First Data's Approach
		not limited to: • Weekly Status Report materials for the month • IV&V project work product and deliverable assessments completed within the month • Critical Incident Reports • Requirements Traceability Matrix updates • CMS and MITA compliance activities • IV&V work plan updates • IV&V work products Drawing on past experience and our experience with DHHS, First Data will refine the existing report formats to satisfy DHHS needs. **Weekly Status Report materials for the month** First Data employs a standard approach to each project which facilitates the ease of integration when employed within a portfolio reporting environment. We will work with DHHS and the implementation vendor(s) to integrate IV&V progress reporting within the scope of ongoing project meetings. As the basis of weekly reporting, First Data includes: • A summary of the activities completed • A summary of the planned activities • A summary of the current issues, risks, and opportunities • Updated IV&V schedule • Critical incidents Clarity and brevity are the key concepts behind our approach to weekly reporting as we believe it should not inhibit project progress. **IV&V project work product and deliverable assessments** First Data utilizes a Deliverable Expectation Document (DED) process in the delivery of its own work products. When working with implementation vendors, we integrate our review efforts within the existing review processes and provide formal feedback. If a DED exists as part of the process, First Data reviews vendor work in relation to conformance to the DED. For work products where no DED is present, First Data will work

	IV&V Deliverables and Work Products Requirements	First Data's Approach
		with vendors early in the review cycle to provide feedback to reduce the possibility of an unsatisfactory deliverable. We also will work with vendors to establish a DED into their work deliverables for future work products. To facilitate a thorough review of vendor deliverables, particularly for more complex deliverables, the First Data Team will utilize checklists tailored to DHS needs and the specific deliverable requirements and content. **Critical Incident Reports** First Data draws from lessons learned on past projects to bring a selection of best practices for defining critical incidents, developing metrics, and appropriate mitigation/resolution responses. We will work with DHHS to establish identification and measurement criteria and to define effective tools for reporting of critical incidents. **Requirements Traceability Matrix updates** First Data employs a host of ISO standards to verify the quality, completeness, and traceability of project requirements. First Data further verifies that that a comprehensive process for managing system requirements is in place during the entire System Development Life Cycle (SDLC) from design through testing and implementation. We evaluate the requirements management tool, the Requirements Traceability Matrix (RTM) and verify that the requirements are under configuration control to validate that the system is being built correctly and will meet DHHS needs. As requirements are introduced or changed, First Data will verify that the requirement is well written, properly tracked, and the history of the requirement maintained Based on findings, First Data will work collaboratively with DHHS and the implementation vendor(s) to conduct changes to the RTM conforming with the project change control process. As part of our approach, First Data: • Validates that requirements are managed

	IV&V Deliverables and Work Products Requirements	First Data's Approach
		properly throughout all phases the project life cycle. • Verifies that existing and newly written requirements conform to SMART (specific, measurable, achievable, traceable, and testable) principle. • Verifies requirements are uniquely identified. • Reviews RTM tracking mechanism to confirm requested changes and updates have been completed and completed properly. **CMS and MITA compliance activities** First Data is conversant with IV&V requirements set forth in 45 CFR 95.610. We are also well experienced with conformance to MITA Standards. First Data will verify that all reporting and the timing thereof complies with the MECT, CMS Expedited Life Cycle processes, or other agency standards. We will also help in the preparation for and participate in any meetings with federal partners. **IV&V work plan updates** First Data will work closely with the PMO to integrate IV&V Project work plans at project onset and report progress and changes. First Data work plan development conforms to applicable PMI, HHS Enterprise Performance Life Cycle, and ISO standards. We practice iterative work plan development confirming project plan currency and actively communicate and report work plan updates in weekly, monthly and ad hoc reporting. **IV&V work products** First Data utilizes a Deliverable Expectation Document (DED) process to eliminate ambiguity and set expectations for final work products. As the basis for our verification work, we employ appropriate industry standards and develop work product specific checklists. First Data also incorporates internal quality assurance as part of our work product development process.
2	Must perform work and submit work products and deliverables for State review and approval in accordance	First Data understands and agrees to adhere to the approved IV&V work plan and its scheduled dates. We will submit work products and deliverables for State

	IV&V Deliverables and Work Products Requirements	First Data's Approach
	with the approved IV&V work plan scheduled dates.	review and approval in accordance with scheduled dates. In the initiation and planning phases of the project, First Data will work closely with the PMO to integrate the IV&V work plan with the overall project work plan.
3	Must provide a tracking capability for tracking of work product and deliverable submission and review status.	First Data uses a Deliverable Schedule and Tracking Tool to track all work products within the assigned project(s). to: • maintain a singular record of all project deliverables • monitor vendor deliverable dates to plan assessments • record all changes to the deliverable schedules • allows for adjustments to be made to all corresponding deliverables
4	Must submit any changes to previously approved deliverables for approval through the review process.	First Data will comply with DHHS process for review and approval related to any recommended changes to previously approved deliverables. To minimize the number of instances where this occurs, First Data will work with the PMO, client, and project vendors to integrate its review activities and provide proactive feedback within the existing review cycle.

Table 3.12 – Approach to IV&V Deliverables and Work Products Requirements

3.2 Organizational Staffing

Beyond the tools, methodologies, and approaches, it is clearly the quality of the team members that will help determine success on the project. First Data prides itself on being able to offer a unique combination of business processing acumen and government programmatic subject matter expertise in order to confirm our solutions fit with the appropriate context of State business needs, financial constraints, and client services.

For a particular agency initiative, First Data will assemble a team that represents the real, hands-on, practical knowledge, experience and expertise required by the specific project. Our team brings methodologies, best practices, and tools from some of the latest projects in the country. Most important to the realization of Nebraska's goals is that we propose staff to the EES and

First Data's Team for Nebraska:

- ✓ *100% of proposed EES team has practical and relevant Cúram experience*
- ✓ *Executive Oversight, Kelly Tinsley, has experience with multiple Cúram implementations as an implementation vendor*
- ✓ *Team structure allows for cost-effective just-in-time staffing with the addition of as-needed SMEs*

DMA projects that have clear and first hand understanding of the challenges, issues and needs presented by the planned initiatives. As a result, we understand what it takes to deliver IV&V services in a cost effective manner and how to help DHHS implement these projects successfully.

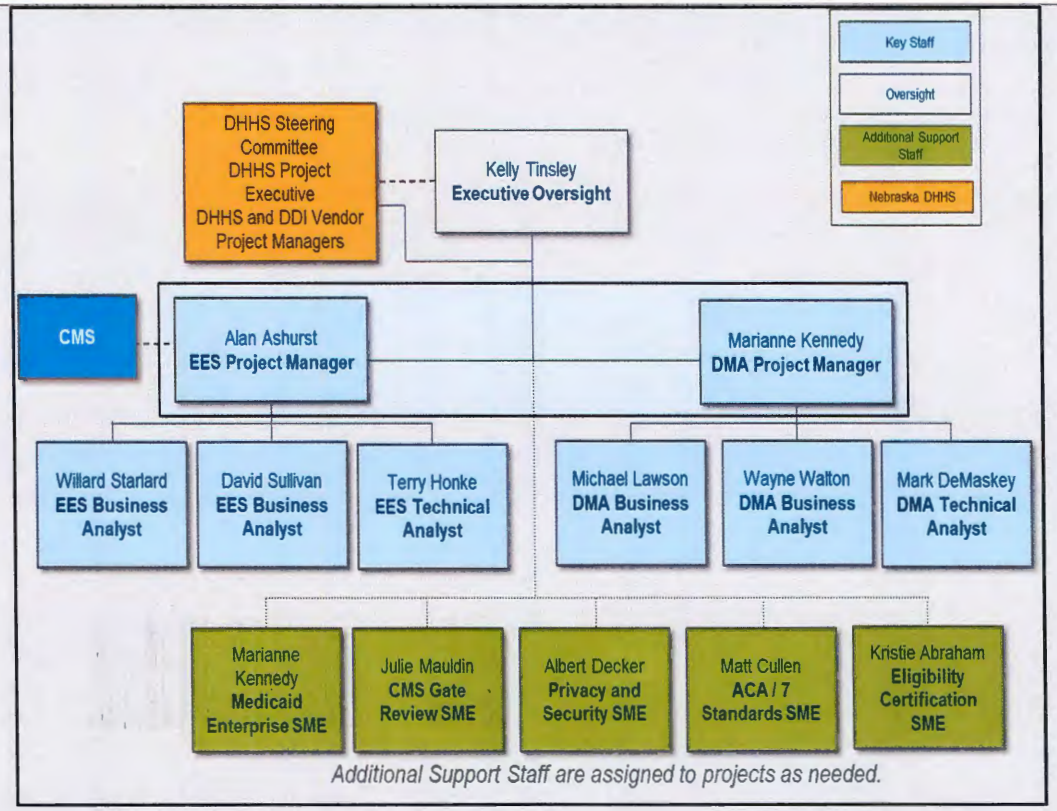
The relevant qualifications, expertise, and experience of the staff at First Data are truly unique, particularly in the areas of project management, change management, and organizational change not only in state government agencies, but in Nebraska specifically.

Address the bidder's approach to meeting each requirement in a table that contains the requirement and the contractor's approach to meeting the requirement. (RFP Section IV, C.3.i)

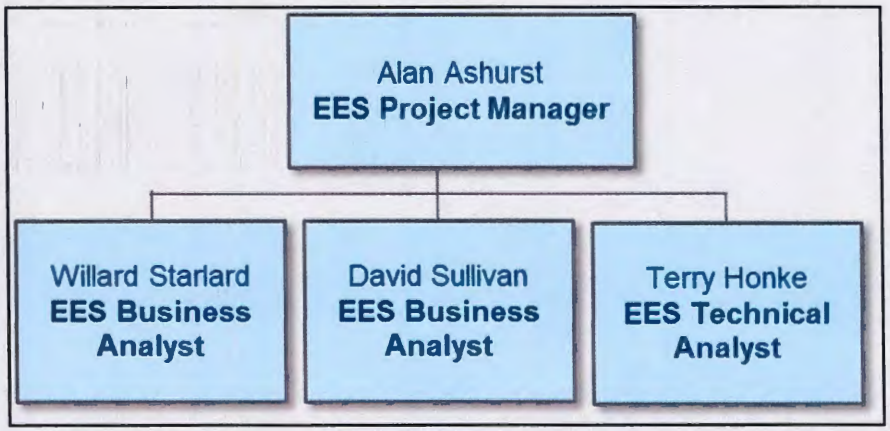
The following table documents our approach to the requirements for organizational staffing.

	Organizational Staffing Requirements	First Data's Approach
1	Must provide an organizational structure which reflects coordinated activities among DHHS, IV&V, EES, DMA and other contractors.	As illustrated in the graphic below, the First Data Team is steeped with relevant experience to support the efforts of EES, DMA and multiple projects as required by DHHS. Pursuant to the requirements outlined in this RFP, we have included an experienced project manager, two business analysts and a technical analyst for each of the named projects: EES and DMA. In addition, understanding the depth and breadth of in-flight projects and the optional projects on the horizon, we have included an additional complement of subject matter experts covering Medicaid, CMS Certifications, Privacy and Security and ACA/7 Conditions Standards. These four resources will be utilized on an as needed basis to support the portfolio of projects DHHS may pursue.

	Organizational Staffing Requirements	First Data's Approach

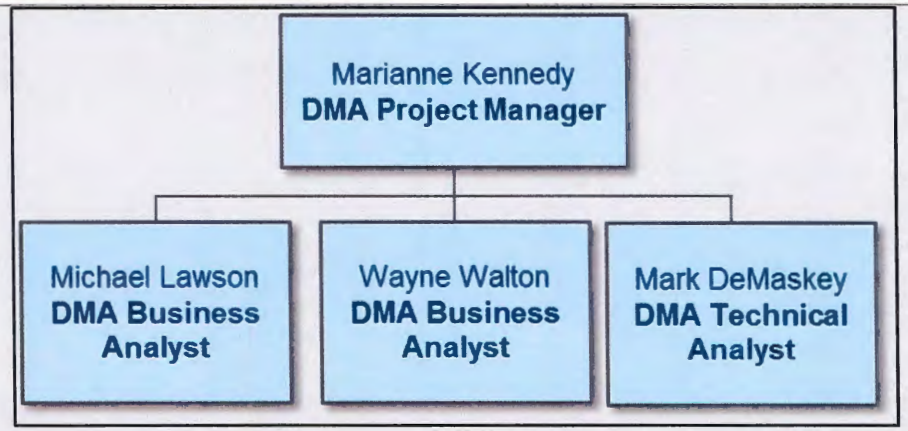


First Data understands the important roles the Key Personnel will have on this project. In addition, First Data recognizes the importance of having a governance structure in place that optimizes efficiency in the delivery of IV&V services. To this end, we have selected **Alan Ashurst** to serve as the Project Manager for EES and **Marianne Kennedy** as the Project Manager for DMA. Mr. Ashurst has over 30 years as an information technology professional with extensive management and leadership expertise in the health care, government, technology, transportation, and beverage industries. His major emphasis has been on managing teams to

	Organizational Staffing Requirements	First Data's Approach
		collaborate on solutions through clear identification of business needs and appropriate application of technology to meet those needs has allowed Mr. Ashurst succeeds in delivering results in IT organizations. He applies passion and high ethical values to bring team leadership, people and project management, process implementation, and strategic planning skills enabling organizational success. Ms. Kennedy, MS, CSM®, CSPO®, PMP®, PEAF® Professional, has over 30 years of Technology and Business Leadership in Consulting, Enterprise and IT Strategic Planning, Software Product Development, Agile Implementation, Portfolio Management, Program and Project Management and Technical Operations (Data Center, Network and Support in Multi-tenant SaaS). The following sections provide greater detail on the team composition, skills and experience the First Data Team will bring to DHHS. **EES Project Organization**  The EES Team is composed of three (3) additional staff, two (2) Business Analysts: **Willard Starlard and David Sullivan** and one (1) Technical Analyst, **Terry Honke**. Mr. Sullivan is a certified Project Management Professional and Certified Scrum Master with expertise in project management, quality assurance,

	Organizational Staffing Requirements	First Data's Approach
		independent verification and validation, development, and training services to government health and human services agencies. For the past 20 years, he has managed teams of IT professionals in the areas of analysis, design and development of new technology solutions, project management and oversight, cost-benefit analysis, and system design. Mr. Starlard brings over thirty years Information Technology experience in State Government, Military and Public Utilities with comprehensive involvement in the complete system development lifecycle at both project management and technical levels including analysis, design, development, conversion, testing, and implementation. He has extensive experience in Team Leadership, Independent Verification & Validation, Business Analysis, Joint Application Design planning, and Business requirements documentation. He has broad application experience in analysis, design, development and implementation in Accounting, Eligibility, Child Welfare, Inventory Management and other State services. Mr. Honke has more than 20 years of experience in technical support and management of large-scale projects. He has supported projects in Nebraska for 10 years, including serving as the Technical Lead on the current Nebraska DHHS eligibility and enrollment system project. Mr. Honke is a certified Scrum Master. He has directed teams in enterprise architecture, quality control, and application development. The EES Team will work under the direction of Mr. Ashurst and in collaboration with DHHS and Wipro's project management team to create required design, development, implementation and certification deliverables. **DMA Project Organization**

	Organizational Staffing Requirements	First Data's Approach



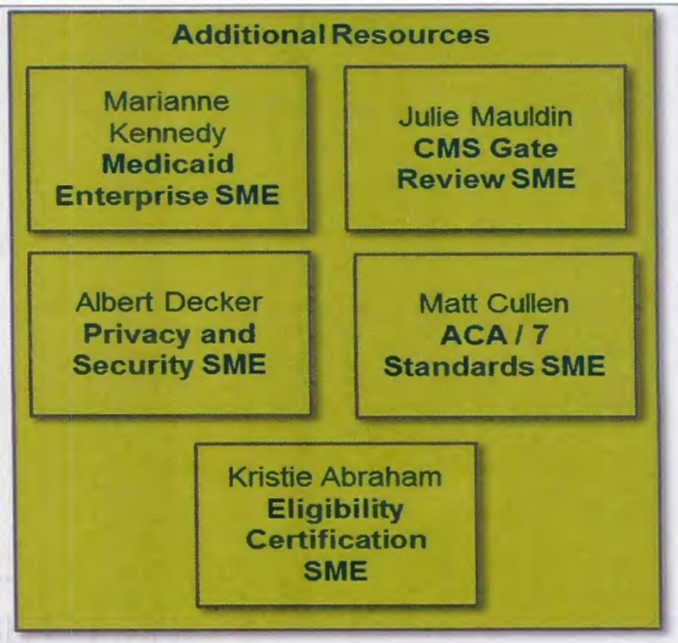
The DMA project is also composed of three (3) additional staff, two (2) Business Analysts: **Michael Lawson** and **Wayne Walton** and one (1) Technical Analyst, **Mark DeMaskey**. Mr. Lawson is an experienced consultant, analyst, and subject matter expert in the healthcare industry who brings over 10 years of Medicaid expertise including fiscal agent operations, Medicaid Management Information Systems (MMIS), Independent Verification & Validation (IV&V) and Project Management Office (PMO) experience. His background has included User Acceptance Testing management and coordination, training development, requirements gathering and analysis, schedule management, technical analysis, and development of Request for Proposal (RFP) requirements.

Mr. Walton is an information systems consultant with experience in project management and SDLC methodologies. He is experienced in requirements gathering and analysis and documentation. He brings subject matter expertise in CMS healthcare policy. Mr. Walton has supported several state government agencies in health and human services efforts.

Mr. DeMaskey has more than 15 years of experience in support of Medicaid and health and human service agency efforts. He has served as a team lead, analyst, and subject matter expert on several government projects. Mr. DeMaskey has contributed to MMIS DDI efforts across a dozen states serving in many varied

	Organizational Staffing Requirements	First Data's Approach
		roles outlined below and brings extensive experience in the implementation of MMIS systems, as well as solid Medicaid enterprise business and technical leadership. Mr. DeMaskey brings considerable analytical/business intelligence experience and expertise as well. The DMA Team will work under the direction of Ms. Kennedy and in collaboration with DHHS and the selected DMA implementation contractor's project management team to create required requirements, design, development, implementation and certification deliverables. Further, we have identified seasoned subject matter experts in the areas of Medicaid, CMS Certifications, Privacy and Security, ACA/7 Conditions Standards and Eligibility Certification to provide support and assistance to the First Data Team and DHHS and it vendors on an as needed basis. The staff below will report directly to Alan Ashurst when DHHS requests their services.

	Organizational Staffing Requirements	First Data's Approach



- **Marianne Kennedy** plays a dual role on the project. If deeper Medicaid expertise is needed to support DHHS efforts in advance of the DMA start Ms. Kennedy will provide consultative services for DA. This advance participation will allow Ms. Kennedy to "hit the ground running" when DMA begins.
- **Julie Mauldin, CMS Certification SME**, is a PMP-certified senior consultant and project manager with 15 years of proven experience leading projects for public and private clients and delivering results on very tight timeframes. She has planned, designed and deployed multi-million dollar projects from RFP composition and planning to project launch and delivery. She is an expert in the implementation of Health Insurance Exchanges and integrated Medicaid eligibility, and has demonstrated experienced in the development of APDs, APD Updates and Level 2 grant applications.
- **Albert Decker, Privacy and Security SME**, is a Certified Enterprise Architect (CEA), FEAC Institute and a Certified Information Systems Security Professional (CISSP). Mr. Decker brings over 30 years of experience as a business and IT consultant, with 10 years of management and business ownership. He

	Organizational Staffing Requirements	First Data's Approach
		has experience with a wide variety of frameworks, platforms, tools and methodologies. Mr. Decker has held positions in both management and technology. • **Matt Cullen, ACA & Standards SME**, is an expert consultant to healthcare industries that are continuously challenged with changing regulations and compliance requirements. He is able to identify, coordinate and implement state of the art information management systems tailored to public sector organization cultures. His experience includes both public and private sector healthcare program oversight and ranges from to development of agency-specific to creation of complex statewide systems. • **Kristie Abraham, Eligibility Certification SME**, has 15 years of overall experience in Health and Human Service information systems technology experience. She brings twelve years' experience in business and systems analysis and system testing with experience in HHS data modeling. She has demonstrated success streamlining, optimizing, and maintaining system functionality and performance in highly sensitive government environments and an excellent capacity to work with executives and IT managers (state and vendors) to effectively prioritize activities, achieve defined IT objectives, and translate business requirements into IT secure solutions. <u>Multiple Projects' Oversight</u> First Data proposes a governance structure above to address the two named projects. If DHHS determines support is required for the additional projects, First Data recognizes that the governance structure should be modified to address increased complexity and coordination. If there are more than two projects in flight, we propose a **Project Director** role to be held by **Mr. Ashurst** to facilitate IV&V governance. The Project Director acts as the manager of all IV&V activities. Mr. Ashurst will coordinate activities of IV&V projects in alignment with DHHS goals, serve as the primary operational customer liaison, consolidate IV&V status reports for presentation to the Steering Committee; coordinate the production of monthly status reports; and manage all IV&V project personnel. This optional role is included in our Optional Projects cost proposal and can be exercised at the discretion of DHHS. Finally, providing Executive Oversight over the services the Firsts Data IV&V Team will provide is **Kelly Tinsley**. The First Data Team functions as a cohesive unit, working collaboratively within each team and with external members of the larger project team. Mr. Ashurst and Ms. Kennedy are the lynchpins in effective

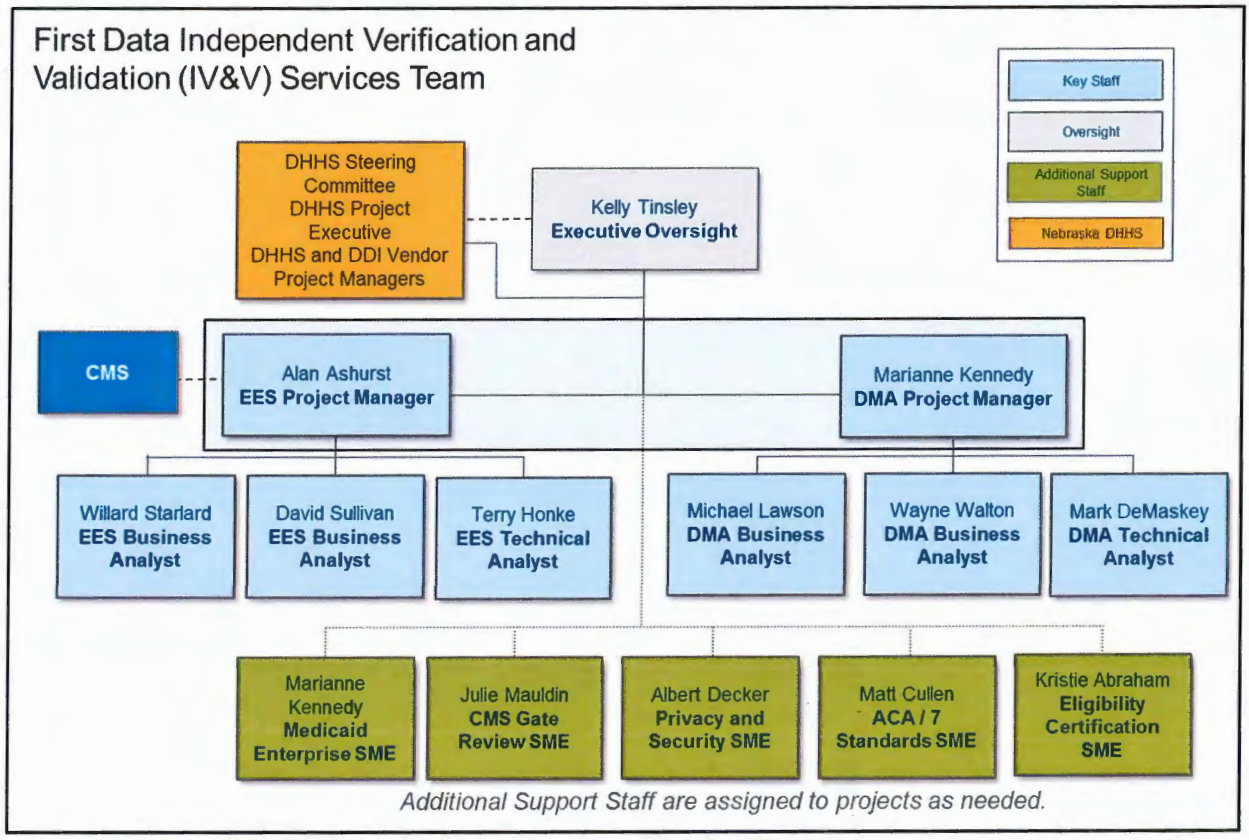
	Organizational Staffing Requirements	First Data's Approach
		governance of the First Data Team's activities and aligning those activities to DHHS overarching strategies, goals and objectives. As the "voice" of IV&V, the Project Managers will present to both the Steering Committee, its designees and to CMS. Open, frequent and honest communication is the cornerstone of our methodology to deliver IV&V services to our clients. The team we propose to work with DHHS through the EES, DMA and optional projects is steeped in programmatic and project management knowledge. This combination coupled with our extensive knowledge of Nebraska will allow DHHS to achieve its mission, on-time and on budget.
2	Must provide criminal background investigations on all personnel and follow-up investigations every five years. Must report any individuals who have criminal activity identified to DHHS.	Each new hire to First Data must pass a rigorous background check before they are allowed to start work or gain access to First Data systems, or begin work for our clients. First Data has also mandated that staff complete drug screening prior to beginning work. We take our responsibility to keep employees and affiliates informed of applicable laws guarding confidential information very seriously. Privacy training is provided by First Data Corporate Security and is mandatory for new hires (during the first 90 days of employment) and annually thereafter for existing staff. All First Data employees, contractors, and subcontractors must complete an on-line training each year. This training covers First Data's security policy and clarifies exactly what constitutes disclosure of confidential information. The training also details the civil and criminal sanctions that can be applied to either First Data or individuals responsible for a data breach, or both. As a matter of practice, First Data consultants do not distribute or collect Personally Identifiable Information (PII) through non-encrypted transfer mechanisms. First Data recognizes that in this age of technology it is our responsibility to confirm that government data is not compromised. We take this responsibility upon ourselves, and escalate breaches we encounter.
3	Must provide all key positions identified IV.C.1.	We agree to provide all key positions as identified. Names and resumes for each of the key staff can be found in the following section.
4	Must maintain an Organizational Chart and project contact list.	First Data understands and agrees to maintain an organizational chart and project contact list through the duration of the project.
5	Must acquire DHHS	We understand that key staff and any potential replacements must be approved by DHHS.

	Organizational Staffing Requirements	First Data's Approach
	approval for key staff and key staff replacements.	
6	Must not reassign or replace key personnel without the prior written approval of DHHS.	First Data understands and agrees that key personnel will not be reassigned or replaced without discussion and approval of DHHS. If a staff member needs to be reassigned or replaced for any reason, we will work cooperatively with DHHS to provide acceptable replacement candidates who bring the same or higher qualifications and experience.
7	Must provide monthly IV&V staff as proposed.	We understand and agree to provide monthly IV&V staff as proposed.

Table 3.13 – Approach to Organizational Staffing

Names and resumes of the bidder's key staff for the DMA and EES projects. (RFP Section IV, C.3.ii)

We have provided a qualification summary table below, to detail our proposed key staff for the DMA and EES projects. Resumes can be found in Appendix 2.



Name	Title	Qualifications Summary
Kelly Tinsley, PMP	Executive Oversight	• Ms. Tinsley has over 20 years' experience in complex human services implementations. • As a certified PMP, Ms. Tinsley delivered Project Executive oversight for multiple states, localities and not-for-profits for social services case management, child welfare, HIE, integrated eligibility and unemployment insurance. Ms. Tinsley was responsible for revenue, profit, sales, pipeline generation and client relationships for consulting services in strategic states. She developed client strategies and business cases. Kelly managed proposal development for SLE case management, health insurance exchange, Medicaid eligibility,

Name	Title	Qualifications Summary
		integrated eligibility and unemployment insurance
Alan Ashurst	Project Manager – EES Project	• Mr. Ashurst has over thirty (30) years' systems development, database management and IV&V, services for human services and private industry of which more than twelve (12) years has focused on MMIS and Health Care Eligibility in multiple states. • Mr. Ashurst has had progressive management and leadership responsibility to provide strategic planning, enterprise application development and support, computing infrastructure and network management, process improvement implementation via ITIL, and data warehouse creation. • Practical application in multiple states of the Seven Standards and Conditions for enhanced funding set forth by the CMS and required for enhanced Federal Financial Participation at 90 percent. • Proven project leadership of multi-year human services programs as both integrator and IV&V professional.
Willard Starlard	EES Business Analyst	• Mr. Starlard brings over thirty (30) years' Information Technology experience in State Government, Military and Public Utilities with comprehensive involvement in the complete system development lifecycle at both project management and technical • Mr. Starlard has extensive experience in Independent Verification & Validation, Business Analysis, Joint Application Design planning, and Business requirements documentation. • Mr. Starlard has broad application experience in analysis, design, development and implementation in Eligibility & Enrollment, SNAP, Child Welfare, Data Warehouse applications.
David Sullivan, PMP	EES Business Analyst	• Mr. Sullivan is Certified Project Management Professional and Certified Scrum Master with over 20 years' experience managing IT professionals in the areas of analysis, design and development of new technology solutions, project management and oversight, cost-benefit analysis, and system design for multiple human services agencies. • Mr., Sullivan has a deep understanding and application of project mangwm4nt methodologies to

Name	Title	Qualifications Summary
		multi program and multi-year projects as PMO Lead through the analysis of processes and mentoring of State project management staff. • Mr. Sullivan has proven experience conducting in-depth analysis of vendor deliverables to validate compliance with state requirements and CMS objectives.
Terry Honke	EES Technical Analyst	• Mr. Honke has over twenty (20) years" experience of technical support and management of large-scale projects, ten (10) of which has been focused on supporting State of Nebraska projects including the DHHS EES project. • Mr. Honke is a Certified Scrum Master who has extensive experience with multiple SDLC methodologies. • Mr., Honke serves as the CMS Payment Error Rate Measurement (PERM) IVV lead. • Mr. Honke had practical experience with Service Oriented Architecture (SOA) governance for web and mobile platforms.
Marianne Kennedy, PMP	DMA Project Manager / MMIS SME	• As a PMP®, PEAF (Pragmatic Enterprise Architecture Framework) Certified EA Professional, Certified SCRUM Master and Certified SCRUM Product Owner, Ms. Kennedy brings over thirty (30) years' experience as a technology leader for Healthcare: data analytics, HIE / HIT, MITA; CRM Software; Financial Services and DOD / Government. • Ms. Kennedy has expertise in Enterprise Transformation, Business modeling, Business plan development, Technical Roadmap development, and Financial / Accounting / Billing Systems. • Ms. Kennedy brings experience in Enterprise Architecture, the development of the HIE / HIT Roadmap for California Health and Human Services Medical Program including initiatives for: MDM, IdAM, SOA and ESB, Member and Provider Portals, Big Data Analytics for population analysis and fraud detection, Technical Services re-use strategy, Enterprise Roadmap and Portfolio Management Process development.
Michael Lawson	DMA Business Analyst	• Mr. Lawson brings over 10 years of Medicaid expertise including fiscal agent operations, Medicaid

Name	Title	Qualifications Summary
		Management Information Systems (MMIS), Independent Verification & Validation (IV&V) and Project Management Office (PMO) experience. • Mr. Lawson's experience has included User Acceptance Testing management and coordination, training development, requirements gathering and analysis, schedule management, technical analysis, and development of Request for Proposal (RFP) requirements. • Mr. Lawson possesses practical understanding and application of quality driven processes for Medicaid operations including Claims, Third Party Liability, and Provider Enrollment.
Wayne Walton	DMA Business Analyst	• Mr. Walton brings over ten (10) years' experience with progressive experience in business analysis and project management for Medicaid implementations. • Mr. Walton Mr. Walton has led and facilitated joint application development sessions with client's business users to clearly define and document business needs. He has developed Use Cases and Test Scenarios for the State client to introduce to the implementation contractor. • Mr. Walton provided IV&V of multiple enhancements for a $400 million state wide systems reengineering implementation. As a consulting subject matter expert, he provided input and direction on client deliverables, oversight for the implementation, assisting with use case creation, UAT, and validating and verifying contractor submitted deliverables.
Mark DeMaskey	DMA Technical Analyst	• Mr. DeMaskey has more than 15 years of experience in support of Medicaid and health and human service agency efforts. • Mr. DeMaskey has contributed to MMIS DDI efforts across a dozen states serving in many varied roles including MMIS SME, Technical and Systems Analyst. • Mr. DeMaskey brings considerable analytical/business intelligence experience and expertise including business intelligence development for the Medicare Services (MCS Part-B) Surveillance Utilization Review system (SURS), specifically provider peer analysis based on claim

Name	Title	Qualifications Summary
		sampling within defined statistical parameters.
Albert Decker	Privacy and Security SME	• Mr. Decker brings over 30 years of experience as a business and IT consultant, with 10 years of management and business ownership' • Mr. Decker has served as Technical Security Lead for multiple states where he was responsible for leading security and privacy documentation and implementation for distributed and outsourced multi-vendor environments. • Mr. Decker assisted with the data architecture vision, and was responsible for the development of security and architecture work products including the audit plan, documentation review, and site visit due diligence.
Julie Mauldin	CMS Gate Review SME	• Ms. Mauldin is a PMP-certified senior consultant and project manager with 15 years of proven experience leading projects for public and private clients and delivering results on very tight timeframes. • She is an expert in the implementation of Health Insurance Exchanges and integrated Medicaid eligibility, and has demonstrated experienced in the development of APDs, APD Updates and Level 2 grant applications. • Ms. Mauldin implemented health insurance exchanges and integrated Medicaid eligibility while serving as the CMS IT Project Manager for 14 states in the Great Lakes and Pacific Coast regions.
Matt Cullen	ACA/7 Standards SME	• Mr. Cullen has demonstrated senior level healthcare industry expertise and mastery of technical systems. As a senior consultant he has the critical ability to address both organizational vision and individual customer needs and outcomes. • Mr. Cullen was responsible for the monitoring the execution of the IV&V team's test plans and responsible for the reporting of test findings to CMS relating to Wave and Blueprint Scenario and End-to-End testing efforts. • Mr. Cullen reviewed project materials for conformance with ACA rules, including 7 Standards & Conditions
Kristie Abraham	Eligibility Certification	• Ms. Abraham has over fifteen (15) years' experience in Health and Human Services implementations as

Name	Title	Qualifications Summary
	SME	business analyst and project manager. • Ms. Abraham has proven understanding and application of business analysis methodologies for multi-year eligibility programs. • Ms. Abraham is skilled quality assurance tester for system, integration, performance and user acceptance testing phases of eligibility programs across multiple states. • As an Arkansas State employee, Ms. Abraham served as Program Manager for the citizen online portal for Medicaid, TANF and SNAP to streamline the client intake process.

Table 3.14 – Qualification Summaries for First Data's Proposed Staff

The bidder's staffing plan for each project. (RFP Section IV, C.3.iii)

Pursuant to the requirements outlined in this RFP, we have included and experienced project manager, two business analysts and a technical analyst for each of the named projects: EES and DMA. In addition, understanding the depth and breadth of in-flight projects and the optional projects on the horizon, we have included an additional complement of subject matter experts covering Medicaid, CMS Certifications, Privacy and Security, ACA/7 Conditions Standards, Eligibility Certification requirements and First Data Executive Oversight. These additional SME resources will be utilized on an as needed basis to support the portfolio of projects DHHS may pursue.

EES Project Staffing Plan

EES Project FTE	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Role												
Project Manager - EES	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
IV&V Business/Test Analysts 1 - EES	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
IV&V Business/Test Analysts 2 - EES	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
IV&V Technical Analyst/Architect - EES	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
ACA / 7 Standards SME	0.13	0.00	0.00	0.00	0.00	0.00	0.13	0.00	0.00	0.00	0.00	0.00
Medicaid Enterprise Services SME	0.00	0.25	0.00	0.00	0.25	0.00	0.25	0.00	0.00	0.00	0.00	0.00
CMS Certification SME	0.00	0.00	0.25	0.25	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Privacy and Security SME	0.50	0.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Eligibility Certification SME	0.00	0.25	0.00	0.00	0.25	0.00	0.25	0.00	0.00	0.00	0.00	0.00
Total Monthly FTE	**4.63**	**5.00**	**4.25**	**4.25**	**4.50**	**4.00**	**4.63**	**4.00**	**4.00**	**4.00**	**4.00**	**4.00**

Figure 3.12 – EES Project Staffing Plan

The EES Team is composed of four (4) staff: one (1) project manager, **Alan Ashurst**, two (2) Business Analysts: **David Sullivan** and **Willard Starlard** and one (1) Technical Analyst, **Terry Honke**.

Mr. Ashurst has over 30 years as an information technology professional with extensive management and leadership expertise in the health care, government, technology, transportation, and beverage industries. His major emphasis has been on managing teams to collaborate on solutions through clear identification of business needs and appropriate application of technology to meet those needs has allowed Mr. Ashurst succeeds in delivering results in IT organizations. He applies passion and high ethical values to bring team leadership, people and project management, process implementation, and strategic planning skills enabling organizational success.

Mr. Sullivan is a certified Project Management Professional and Certified Scrum Master with expertise in project management, quality assurance, independent verification and validation, development, and training services to government health and human services agencies. For the past 20 years, he has managed teams of IT professionals in the areas of analysis, design and development of new technology solutions, project management and oversight, cost-benefit analysis, and system design.

Mr. Starlard brings over thirty years Information Technology experience in State Government, Military and Public Utilities with comprehensive involvement in the complete system development lifecycle at both project management and technical levels including analysis, design, development, conversion, testing, and implementation. He has extensive experience in Team Leadership, Independent Verification & Validation, Business Analysis, Joint Application Design planning, and Business requirements documentation. He has broad application experience in analysis, design, development and implementation in Accounting, Eligibility, Child Welfare, Inventory Management and other State services.

Mr. Honke has more than 20 years of experience in technical support and management of large-scale projects. He has supported projects in Nebraska for 10 years, including serving as the Technical Lead on the current Nebraska DHHS eligibility and enrollment system project. Mr. Honke is a certified Scrum Master. He has directed teams in enterprise architecture, quality control, and application development. The EES Team will work under the direction of MR. Sullivan and in collaboration with DHHS and Wipro's project management team to create required design, development, implementation and certification deliverables.

DMA Project Staffing Plan

DMA Project FTE																														
Role	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30	M31	M32	M33	M34	M35	M36
Project Manager 1 - DMA	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
IV&V Business/Test Analysts 1-DMA	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
IV&V Business/Test Analysts 2-DMA	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
IV&V Technical Analyst/Architect-DMA	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Project Manager 2 - DMA	0.00	0.00	0.00	0.00	0.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
ACA / 7 Standards SME	0.00	0.00	0.00	0.00	0.00	0.13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.25	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.25	0.25	0.00	0.00
Medicaid Enterprise Services SME	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
CMS Certification SME	0.00	0.00	0.00	0.00	0.25	0.25	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.25	0.25
Privacy and Security SME	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Eligibility Certification SME	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Total Monthly FTE	**4.00**	**4.00**	**4.00**	**4.00**	**4.25**	**5.38**	**4.00**	**4.00**	**4.00**	**4.00**	**4.00**	**4.00**	**4.00**	**4.00**	**4.25**	**4.00**	**4.00**	**4.00**	**4.00**	**4.00**	**4.00**	**4.00**	**4.00**	**4.00**	**4.00**	**4.25**	**4.25**	**4.25**	**4.25**

Figure 3.13 – DMA Project Staffing Plan

Under the leadership of Marianne Kennedy, MS, CSM®, CSPO®, PMP®, PEAF® Professional, the DMA project is also composed of three (3) additional staff, two (2) Business Analysts: Michael Lawson and Wayne Walton and one (1) Technical Analyst, Mark DeMaskey.

Mr. Lawson is an experienced consultant, analyst, and subject matter expert in the healthcare industry who brings over 10 years of Medicaid expertise including fiscal agent operations, Medicaid Management Information Systems (MMIS), Independent Verification & Validation (IV&V) and Project Management Office (PMO) experience. His background has included User Acceptance Testing management and coordination, training development, requirements gathering and analysis, schedule management, technical analysis, and development of Request for Proposal (RFP) requirements.

Mr. Walton is an information systems consultant with experience in project management and SDLC methodologies. He is experienced in requirements gathering and analysis and documentation. He brings subject matter expertise in CMS healthcare policy. Mr. Walton has supported several state government agencies in health and human services efforts.

Mr. DeMaskey has more than 15 years of experience in support of Medicaid and health and human service agency efforts. He has served as a team lead, analyst, and subject matter expert on several government projects. Mr. DeMaskey has contributed to MMIS DDI efforts across a dozen states serving in many varied roles outlined below and brings extensive experience in the implementation of MMIS systems, as well as solid Medicaid enterprise business and technical leadership. Mr. DeMaskey brings considerable analytical/business intelligence experience and expertise as well.

The DMA Team will work under the direction of Ms. Kennedy and in collaboration with DHHS and the selected DMA implementation contractor's project management team to create required requirements, design, development, implementation and certification deliverables.

The bidder's organizational chart for each project team. (RFP Section IV, C.3.iv)

As illustrated in the graphic below, the First Data Team is replete with relevant experience to support the efforts of EES, DMA and multiple projects as required by DHHS. The structure facilitates collaboration ad focus on what needs to be accomplished within the purview of each project's directives. If requested by DHHS, as additional projects are added to the First Data Team's purview, DHHS may include a Project Director role (to be filled by Alan Ashurst) to fulfill increased complexity, coordination and governance requirements.

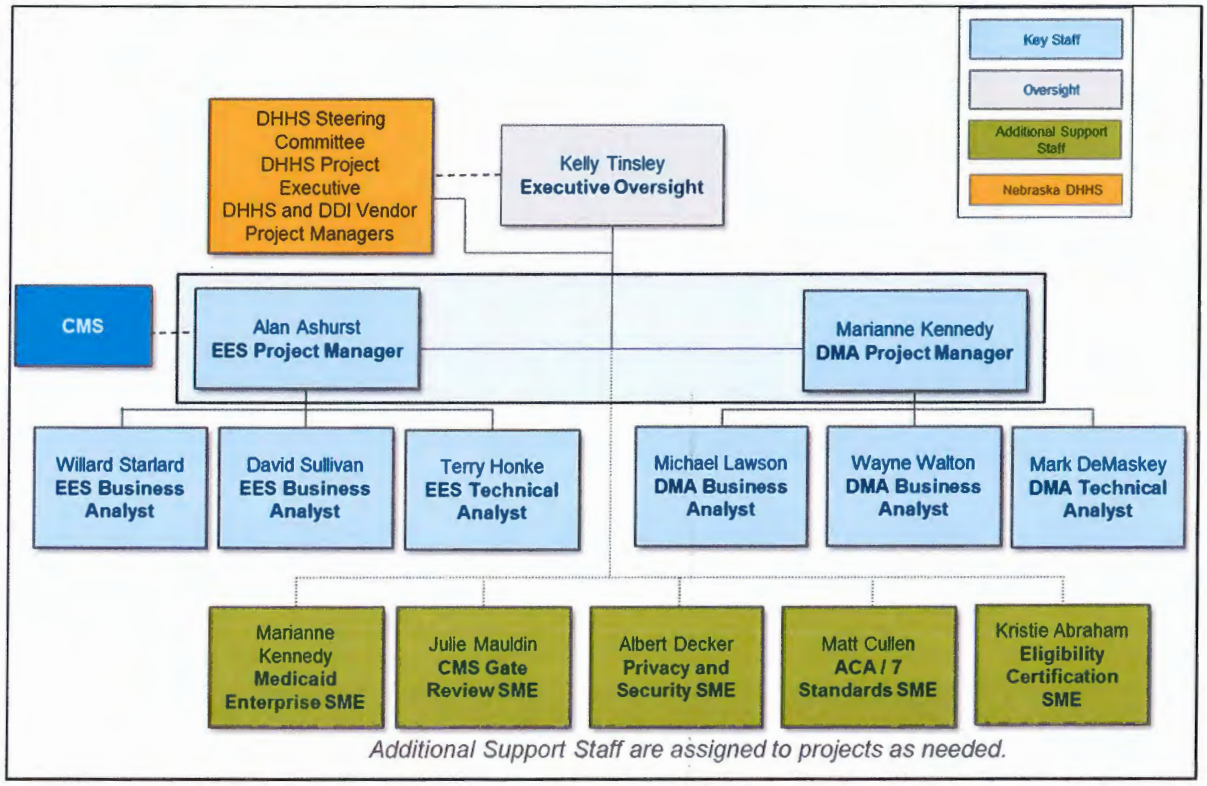


Figure 3.14 – Organizational Chart

DHHS has required a minimum of four key staff positions for each project. Describe the strategy and approach to maintain the appropriate number of staff for each project. (RFP Section IV, C.3.v)

For First Data project staff to be sustainable we must bring strategic focus that speaks to the mission, vision, goals and niche of DHHS. By naming staff with deep Nebraska, program knowledge and experience with multiple states' eligibility and Medicaid implementations, we are committed to sustaining our staff to the levels outlined above. We understand the requirements of each named project and have complemented core staff with requisite subject matter expertise throughout the life of DHHS' initiatives. Further, our Center of Excellence, provided at no cost to DHHS, will provide as needed support in the achievement of First Data requirements. First Data's national knowledge Center of Excellence (COE) is our intellectual capital hub and contains recommended practices, project management methods, tools and techniques, lessons learned, and sample deliverables from our previous projects. The First Data Teams across the country avail themselves of these non-

proprietary methodologies and tools to enhance productivity and provide a proactive and grounded footing in quality standards and measurements for our customers.

Finally, understanding the requirement for 90% on-site participation of named resources, approximately 50% of our named resources are local or near-local to Lincoln, Nebraska. This serves to support continuity of service and facilitates Monday thru Friday coverage for each project. In addition, we have included SME support for each of the named DHHS initiatives. The addition of these staff allows for critical on-site coverage by multiple resources during key project operations. The Frist Data IV&V Team is poised and ready to support DHHS, with the right skills, the right experience with a just-in-time resource staffing methodology.

3.3 Logistics

Address the bidder's approach to meeting each requirement in a table that contains the requirement and the contractor's approach to meeting the requirement. (RFP Section IV, D.3.i)

The following table documents our approach to the requirements for logistics.

	Logistics Requirements	First Data's Approach
1	Must store all work products in DHHS designated repository and using designated folder structure.	While we agree to store all work products in a DHHS designated repository, First Data recommends the use of Microsoft SharePoint for the management of work products and documents. First Data uses SharePoint to manage documents and collaborate on client engagements, as well as for internal purposes. We are thoroughly familiar with the features and capabilities of SharePoint
2	Must have controlled access to all contractor facilities where any contract related work is performed in compliance with privacy and security requirements.	First Data does not expect to secure facilities to support the work to be performed for DHHS. Out staff will work onsite at DHHS designated locations or will work remotely from an at-home location. First Data complies with state security and technology standards by leveraging state provided resources to perform remote work. In Nebraska, we will use Microsoft Remote Desktop Connection to access assigned workstation resources remotely. Outlook Web Access (OWA) will also be used to access state e-mail remotely.

Table 3.15 – Approach to Logistics Requirements

Provide an overview and describe the bidder's facilities where contractor staff may perform work when not on-site in Lincoln. (RFP Section IV, D.3.ii)

We understand the significance of confidentiality and comply with all applicable federal and state regulations pertaining to protection of customer data. First Data has a company-wide Information Security Policy in place that is aligned with ISO17799:00, the International Organization for Standardization's code that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. Our policy has been analyzed against the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and is compliant.

Staff may perform work offsite and their actions are governed not only by the First Data security and privacy policies, but also by the State's requirements regarding access to State systems.

3.4 Privacy and Security

First Data is keenly aware of the importance of data security. As the largest processor of credit card transactions in the world, data security is a fundamental business practice for First Data. We understand the significance of confidentiality and comply with all applicable federal and state regulations pertaining to protection of customer data. First Data has a company-wide Information Security Policy in place that is aligned with ISO17799:00, the International Organization for Standardization's code that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. Our policy has been analyzed against the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and is compliant.

In addition, First Data will comply with all applicable federal and Commonwealth policies regarding data security and compliance. We will work with DHHS and its chosen implementation contractor to assess and mitigate data security risks.

Address the bidder's approach to meeting each requirement in a table that contains the requirement and the contractor's approach to meeting the requirement. (RFP Section IV, E.3.i)

The following table documents our approach to the requirements for privacy and security.

	Privacy and Security Requirements	First Data's Approach
1	Must develop and submit a Privacy and Security Plan work product that includes a description of how contractor safeguards all state information that is transmitted within contractors systems (i.e., email). The	First Data agrees to develop and submit a Privacy and Security Plan for the approval of DHHS to verify our staff follows proper security protocols. Our work product will include the following components covering information security as it pertains to the activities of First Data staff in the execution of its required activities:

	Privacy and Security Requirements	First Data's Approach
	plan must be approved by DHHS prior to the contractor having access to project materials.	• Introduction and Overview of Security Plan • Roles and Responsibilities (Security Management) • Security Processes and Procedures • (Information/Data) Classification and Control • Personnel Security (Managing People and the use of Information) • Physical Asset Security (including electronic and physical security) • Communication Security (including email and telecommunications) • Access Control (protecting passwords, access and data) • Monitoring System Access and Use • Incident Management • Disaster Recovery and Business Continuity • External Dependencies • Third Party Security • Operations Management • Compliance • Appendices - Sample Logs, Matrices, Training Information, Diagrams, Sample Forms, Sample Threat Levels, • Glossary
2	Must comply with all security and privacy laws, regulations, and policies, including HIPAA, and related breach notification laws and directives.	First Data will comply with all applicable security and privacy laws, regulations, and policies, including HIPAA, and related breach notification laws and directives as required by First Data and DHHS.
3	Must provide initial and ongoing privacy and security and HIPAA compliance training to all employees and contract personnel assigned to the project prior to providing access to PHI.	Privacy training is provided by First Data Corporate Security and is mandatory for new hires (during the first 90 days of employment) and annually thereafter for existing staff. All First Data employees, contractors, and subcontractors must complete an on-line training each year. This training covers First Data's security policy and clarifies exactly what constitutes disclosure of confidential information. The training also details the civil and criminal sanctions that can be applied to either First Data or individuals responsible for a data breach, or both.
4	Must take all reasonable industry recognized methods to secure the system from unauthorized access.	First Data will maintain commercially reasonable security standards and protocols to inhibit unauthorized access to DHHS systems and data.
5	Must permanently destroy all confidential data and protected health	First Data plans to comply with this requirement by not allowing any confidential data or protected health

	Privacy and Security Requirements	First Data's Approach
	information entrusted to the contractor for the performance of the contract upon approval of DHHS.	information to be on its information technology systems. .

Table 3.16 – Approach to Privacy and Security Requirements

Description of the proposed strategy, methodology, and capabilities for systems, operations, and physical security. (RFP Section IV, E.3.ii)

First Data's policies have been reviewed and approved by these three broadly recognized assessors – SSAE16/SOC 1 (Ernst & Young), PCI DSS (Trustwave) and GLBA (FFIEC) – as well as a many state, local, and customer assessors. The Information Security Policy framework is based upon the following: ISO27001:2005, ISO27002:2005, PCI DSS, PCI ADSS. Corporate security policies also include practices in FTC 16 CFR Part 314, Standards for Safeguarding Customer Information; Final Rule.

We have chosen this broader approach rather than the strict adherence to one standard because it enables:

- A single, global First Data IT security policy
- That meets the full scope of legal and regulatory requirements
- Across a diverse spectrum of products and services

First Data has earned PCI compliance, as well as meeting the many requirements of state, federal and industry regulations through the controls of its defense-in-depth architecture. First Data requires access controls on all applications, operating systems, databases, and network devices to verify that persons only have the minimal privileges they require. Data from disparate clients is logically segregated and safeguarded through these access controls.

There are formal processes in place for managers and data owners to grant and approve and terminate access, communicate passwords, enforce password complexity and expiration and perform password resets. Access privileges are based on job responsibilities and are regularly reviewed to confirm that only those people with a current need-to-know have access. Each ID is unique and is associated with a specific individual. Systems require multi-factor authentication.

From a network perspective, secure, encrypted communications are used for remote administration of production systems and applications. System standards/procedures include disabling all unneeded or unused services.

Physical Security

First Data's Data Center facilities are designed to be continuously available. Each is a hardened enclosure, engineered to withstand a local natural disaster and maintain room-

to-room building integrity for building disasters, such as fire, flood, etc. All sites are constructed to withstand impact on all external walls. Electrical and mechanical systems are redundant end-to-end. All systems can be isolated for service and testing without compromising the ability to support the data center during this activity. All systems are monitored for performance; and engineers are available 24 hours per day, 7 days per week, to respond to utility or system alarms or outages. Maintenance is performed to verify all systems are operating as designed. Any work performed at First Data will be covered by these security standards.

While onsite, the First Data Team understands the importance of additional physical security standards, such as:

- The importance wearing an identification badge while on premises.
- The need to check in and out with security when entering or leaving.
- Ensuring anyone not wearing identification is not allowed to wander unaccompanied without being reported.

Our Team is trained and recertified annually on physical security standards and understands to report any potential breaches identified.

Sample of a Privacy and Security Plan from a previous project. (RFP Section IV, E.3.iii)

First Data is including a Security Plan in Appendix 10 that encompasses a multitude of other documents relating to physical security, logical security, general operations, technical architecture, disaster recovery and business continuity. References to separate documents exist throughout the Security Plan and such documents will be made available as requested. All documents are to be considered living documents that must be continually updated, correlated back to the Security Plan and controlled under configuration management.

We have included the Security Plan from the CA State Disbursement Unit (SDU) for Child Support. First Data managed all aspects of security for the SDU including data security and facility security.

Privacy and Security Plan template with instructions and procedures for completing the template. (RFP Section IV, E.3.iv)

First Data is including, in Appendix 11, a Privacy and Security Plan template we propose to use to govern our activities and support of DHHS objectives throughout the life of the program.

Description of how workforce privacy and security awareness is supported. (RFP Section IV, E.3.v)

All First Data employees and contractors with access to customer data are required to sign-off on the Information Security End User Policy and the Standard Operating Procedure:

Privacy & Protection of Personal and Business Confidential Information. These documents are based on relevant sections of the Information Security Policy, with additional detail. The Information Security Policy itself is posted on the corporate intranet, accessible to employees. By contract, third party vendors who have access to customer data must sign an amendment agreeing to meet or exceed First Data's security policies and standards, which includes employee training on those policies. In addition, Contractors must be trained on and agree to Third Party Employees Privacy/InfoSec Operating Procedures.

As stated above, workforce privacy and security awareness is supported through training provided by First Data Corporate Security and is mandatory for new hires (during the first 90 days of employment) and annually thereafter for existing staff. All First Data employees, contractors, and subcontractors must complete an on-line training each year. This training covers First Data's security policy and clarifies exactly what constitutes disclosure of confidential information. The training also details the civil and criminal sanctions that can be applied to either First Data or individuals responsible for a data breach, or both.

Description of the approach to monitoring attempted security violations and the actions that will be taken when security violation attempts are made as well as breaches. (RFP Section IV, E.3.vi)

When we identify an information security risk, we follow an aggressive and disciplined process to remedy or mitigate the risk. First Data has established a corporate-wide Governance, Risk, & Compliance group, reporting up to the Senior Vice President of Enterprise Security, Risk, & Compliance, to identify and mitigate any information security risks. We mention this because security is not something First Data takes lightly; it is a core tenet of our corporate structure. As one of the largest transaction processors in the country, you and your families take trust in First Data on a daily basis that our firm will entrust your purchases and safeguard your information. We train our staff annually and take specific measures to minimize security threats.

As our role as an IV&V vendor, our access to project sensitive information will be safeguarded. If we suspect any sort of violation we will follow the following protocols:

1. Report a security violation to the State Project Manager and First Data Project Manager
2. Report the security violation to First Data Security Team
3. Control any documentation and conduct an inventory of secured data
4. Provide a report of compromised data including the impacts

First Data takes extreme measures to verify our staff and our technologies are not impacted. For example, our staff has:

- Annual security training
- Bit locker protected laptops
- Laptops with USB ports deactivated
- Security monitoring over email to validate Personally Identifiable Information (PII) is not distributed
- Mandates to only use encrypted flash drives

The First Data Team will be knowledgeable and equipped to keep your data secure.

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-K

☒ ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the fiscal year ended December 31, 2015

OR

☐ TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the transition period from to

Commission file number 001-11073

First Data

FIRST DATA CORPORATION

DELAWARE	**47-0731996**
(State of incorporation)	(I.R.S. Employer Identification No.)

225 LIBERTY STREET, 29th FLOOR, NEW YORK, NEW YORK 10281
(Address of principal executive offices) (Zip Code)

Registrant's telephone number, including area code **(800) 735-3362**

Securities registered pursuant to Section 12(b) of the Act: **None**

Securities registered pursuant to Section 12(g) of the Act: **None**

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☐ No ☒

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§ 229.405 of this chapter) is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See definition of "large accelerated filer," "accelerated filer" and "smaller reporting company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer ☐	Accelerated filer ☐
Non-accelerated filer ☒	Smaller Reporting Company ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Act). Yes ☐ No ☒

Indicate the number of shares outstanding of each of the issuer's classes of common stock, as of the latest practicable date.

Class	**Outstanding at January 31, 2016**
Class A Common Stock, $0.01 par value per share	179,873,244 shares
Class B Common Stock, $0.01 par value per share	719,330,114 shares

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's Proxy Statement for the Annual Meeting of Shareholder to be held on May 11, 2016 are incorporated by reference in Part III.

INDEX

		PAGE NUMBER
PART I.		
Item 1.	Business	4
Item 1A.	Risk Factors	20
Item 1B.	Unresolved Staff Comments	30
Item 2.	Properties	30
Item 3.	Legal Proceedings	30
Item 4.	Mine Safety Disclosures	30
PART II.		
Item 5.	Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities	31
Item 6.	Selected Financial Data	32
Item 7.	Management's Discussion and Analysis of Financial Condition and Results of Operations	34
Item 7A.	Quantitative and Qualitative Disclosures About Market Risk	54
Item 8.	Financial Statements and Supplementary Data	56
Item 9.	Changes in and Disagreements with Accountants on Accounting and Financial Disclosure	109
Item 9A.	Controls and Procedures	109
Item 9B.	Other Information	111
PART III.		
Item 10.	Directors, Executive Officers and Corporate Governance	111
Item 11.	Executive Compensation	111
Item 12.	Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters	111
Item 13.	Certain Relationships and Related Transactions, and Director Independence	111
Item 14.	Principal Accountant Fees and Services	111
PART IV.		
Item 15.	Exhibits, Financial Statement Schedules	112
Signatures		133

Unless otherwise indicated or the context otherwise requires, financial data in this Form 10-K reflects the consolidated business and operations of First Data Corporation and its consolidated subsidiaries. Unless the context otherwise requires, all references herein to "First Data," "FDC," the "Company," "we," "our," or "us" refer to First Data Corporation and its consolidated subsidiaries.

Amounts in this Form 10-K and the consolidated financial statements included in this Form 10-K are presented in U.S. Dollars rounded to the nearest million, unless otherwise noted.

Forward-Looking Statements

Certain matters we discuss in this Form 10-K and in other public statements may constitute forward-looking statements. You can identify forward-looking statements because they contain words such as "believes," "expects," "may," "will," "should," "seeks," "intends," "plans," "estimates," or "anticipates" or similar expressions which concern our strategy, plans, projections or intentions. Examples of forward-looking statements include, but are not limited to, all statements we make relating to revenue, earnings before net interest expense, income taxes, depreciation, and amortization (EBITDA), earnings, margins, growth rates, and other financial results for future periods. By their nature, forward-looking statements speak only as of the date they are made; are not statements of historical fact or guarantees of future performance; and are subject to risks, uncertainties, assumptions or changes in circumstances that are difficult to predict or quantify. Actual results could differ materially and adversely from our forward-looking statements due to a variety of factors, including the following: (1) adverse impacts from global economic, political, and other conditions affecting trends in consumer, business, and government spending; (2) our ability to anticipate and respond to changing industry trends, including technological changes and increasing competition; (3) our ability to successfully renew existing client contracts on favorable terms and obtain new clients; (4) our ability to prevent a material breach of security of any of our systems; (5) our ability to implement and improve processing systems to provide new products, improve functionality, and increase efficiencies; (6) our merchant alliance program which involves several alliances not under our sole control and each of which acts independently of the others; (7) credit and fraud risks in our business units and merchant alliances, particularly in the context of eCommerce and mobile markets; (8) consolidation among financial institution clients or other client groups that impacts our client relationships; (9) our ability to improve our profitability and maintain flexibility in our capital resources through the implementation of cost savings initiatives; (10) our ability to successfully value and integrate acquired businesses, including those outside of the United States; (11) our high degree of leverage; (12) adverse impacts from currency exchange rates or currency controls imposed by any government or otherwise; (13) changes in the interest rate environment that increase interest on our borrowings or the interest rate at which we can refinance our borrowings; (14) the impact of new laws, regulations, credit card association rules, or other industry standards; and (15) new lawsuits, investigations, or proceedings, or changes to our potential exposure in connection with pending lawsuits, investigations or proceedings, or changes to our potential exposure in connection with pending lawsuits, investigations or proceedings, and various other factors discussed throughout this report, including but not limited to, Item 1 - Business, Item 1A - Risk Factors, and Item 7 - Management's Discussion and Analysis of Financial Condition and Results of Operations. Except as required by law, we do not intend to revise or update any forward-looking statement as a result of new information, future developments or otherwise.

PART I

ITEM 1. BUSINESS

General

First Data Corporation (we, our, Company or First Data) sits at the center of global electronic commerce. We believe we offer our clients the most complete array of integrated solutions in the industry, covering their needs across next-generation commerce technologies, merchant acquiring, issuing, and network solutions. We serve our clients in 118 countries, reaching approximately 6 million business locations and over 4,000 financial institutions. We believe we have the industry's largest distribution network, driven by our partnerships with many of the world's leading financial institutions, our direct sales force, and a network of distribution partners. We are the largest merchant acquirer, issuer processor, and independent network services provider in the world, enabling businesses to accept electronic payments, helping financial institutions issue credit, debit and prepaid cards, and routing secure transactions between them. In 2015, we processed 79 billion transactions globally, or over 2,500 per second, and processed 28% of the world's eCommerce volume. In our largest market, the United States, we acquired $1.7 trillion of payment volume, accounting for nearly 10% of U.S. GDP last year.

On October 15, 2015, we filed a Prospectus for our Initial Public Offering with the Securities and Exchange Commission pursuant to Rule 424(b). We issued 176,076,869 shares of Class A common stock and began trading on the New York Stock Exchange under the symbol "FDC". The net proceeds to us from the offering, after deducting underwriting discounts and commissions were $2.7 billion. We used the net proceeds from the offering to redeem all $510 million aggregate principal amount of our 11.25% senior unsecured notes due 2021 and $1.9 billion aggregate principal amount of our 12.625% senior unsecured notes due 2021, to pay applicable premiums and related fees and expenses, and for general corporate purposes.

On October 13, 2015, First Data Holdings Inc. (FDH), our direct parent company, merged with and into First Data Corporation, with First Data Corporation being the surviving entity (HoldCo Merger). All outstanding shares of FDH were converted into Class B common stock, which are entitled to ten votes per share. All of First Data's outstanding common stock was eliminated upon the merger. We accounted for the HoldCo Merger as a transfer of assets between entities under common control and reflected the transaction in our financial statements on a prospective basis.

On October 13, 2015, we amended our certificate of incorporation which affected a reverse stock split of our authorized, issued and outstanding Class B common stock, on the basis of 1 new share of Class B common stock for each 3.16091 old shares of common stock. Note 4 "Stock Compensation Plans" to our consolidated financial statements in Part II, Item 8 of this Form 10-K has been retrospectively adjusted to reflect the impact of the reverse stock split. The shares on our consolidated balance sheet were not retrospectively adjusted as of December 31, 2014, because the shares of our stock were not subject to the stock split.

We have operations and offices located within the United States (U.S.) (domestic) and outside of the U.S. (international) where sales, customer service and/or administrative personnel are based. Total revenues from processing domestic and international transactions as a percentage of total revenues and total long lived assets attributable to domestic and international operations as a percentage of total long lived assets, are displayed in the below table.

	Year ended December 31,		
	2015	2014	2013
Total generated from processing transactions:			
Domestic	86%	85%	85%
International	14%	15%	15%
Long-lived assets attributable to operations:			
Domestic	89%	88%	87%
International	11%	12%	13%

No single international country is greater than 10% of our total revenues or long-lived assets during any of the years presented in the above table. Further financial information relating to our international and domestic revenues and long-lived assets is set forth in note 7 "Segment Information" to our consolidated financial statements in Part II, Item 8 of this Form 10-K.

Our business is characterized by transaction related fees, multi-year contracts, and a diverse client base, which allows us to grow alongside our clients. Our multi-year contracts allow us to achieve a high level of recurring revenues with the same clients. While the contracts typically do not specify fixed revenues to be realized thereunder, they do provide a framework for revenues to be

generated based on volume of services provided during such contract's term. Our business also generally requires minimal incremental capital expenditures and working capital to support additional revenue within our existing business lines.

Products and Services Segments Information

We provide a range of solutions to businesses and financial institutions across the value chain of commerce-enabling services and technologies. We create our value-added solutions from a suite of proprietary technology products, software, cloud-based applications, processing services, security offerings, and customer support programs that we configure to meet our clients' individual needs.

We operate three reportable segments: Global Business Solutions (GBS), Global Financial Solutions (GFS), and Network & Security Solutions (NSS). Our segments are designed to establish global lines of businesses that support our global client base and allow us to further globalize our solutions while working seamlessly with our geographic teams across our regions: the United States and Canada (North America); Europe, Middle East, and Africa (EMEA); Latin America (LATAM); and Asia Pacific (APAC) and be supported by a corporate team focused on companywide issues.

- **Global Business Solutions (GBS)** - This segment provides retail point-of-sale merchant acquiring and eCommerce services as well as next-generation offerings such as mobile payment services, webstore-in-a-box solutions, and our cloud-based *Clover* point-of-sale operating system, which includes a marketplace for proprietary and third-party business applications.

- **Global Financial Solutions (GFS) -** This segment provides credit solutions for bank and non-bank issuers. These include credit and retail private-label card processing within the United States and international markets, as well as licensed financial software systems, such as our *VisionPLUS* bank processing application, and lending solutions. Global Financial Solutions also provides financial institutions with a suite of related services including card personalization and embossing, statement printing, client service, and remittance processing.

- **Network & Security Solutions (NSS) -** This segment provides a wide range of value-added solutions that we sell to clients in our Global Business Solutions and Global Financial Solutions segments, smaller financial institutions, and other enterprise clients. These solutions include our EFT network solutions, such as our *STAR Network*, our debit card processing solutions, our stored value network solutions, such as *Money Network*, *ValueLink*, *Gyft*, and *Transaction Wireless (TWI)*, and our security and fraud solutions, such as *TransArmor* and *TeleCheck*. This segment also supports our other digital strategies, including online and mobile banking, and our business supporting mobile wallets.

See "Item 7 - Management's Discussion and Analysis of Financial Condition and Results of Operations" for a detailed explanation of our operating results.

Segment products and services are illustrated below:

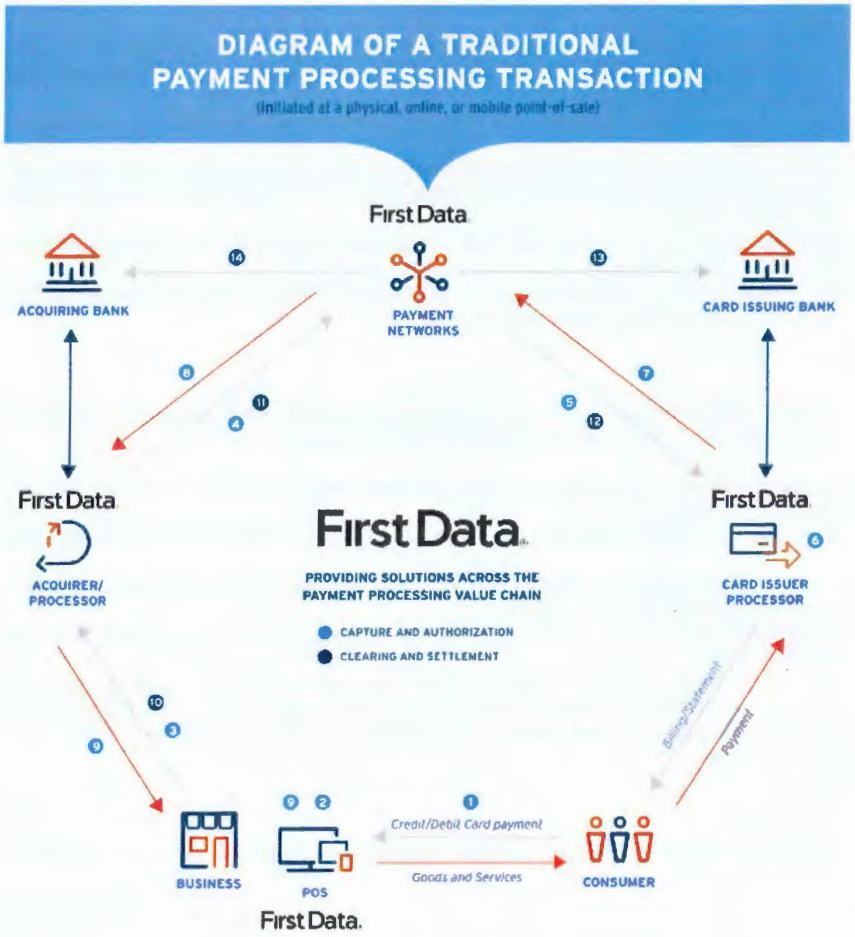
	Global Business Solutions (GBS)	Global Financial Solutions (GFS)	Network & Security Solutions (NSS)
Clients:	Businesses and business owners of all types and sizes	Financial Institutions and other issuers of all sizes	GBS and GFS clients, small banks, and other enterprises
Goals:	To help businesses grow commerce at the retail, online, and mobile POS	To help issuers empower their customers to transact	To help connect, manage, protect, and secure our clients' data
Key Solutions:	• Merchant Acquiring • eCommerce • *Clover* POS technology • Business Software • Marketing/Loyalty	• Credit/Retail Private Label Issuer Processing • Output Services • *VisionPLUS* Software • Marketing/Loyalty	• EFT Network solutions *(STAR, debit processing)* • Stored Value Network Solutions *(Valuelink, MoneyNetwork, Gyft, and TWI)* • Security/Risk Management
2015 Segment Revenue:	$4.1 billion, up 1% from 2014	$1.5 billion, flat over 2014	$1.5 billion, up 7% from 2014
Adjusted EBITDA:	$1.7 billion, flat over 2014	$550 million, up 4% from 2014	$639 million, up 5% from 2014

The segments' profit measure is a form of EBITDA (earnings before net interest expense, income taxes, depreciation, and amortization). A discussion of factors potentially affecting our operations is set forth in Item 7 "Management's Discussion and Analysis of Financial Condition and Results of Operations" of this Form 10-K.

We do not have any significant customers that account for 10% or more of total consolidated revenues.

Overview of Payment Processing

The processing of a traditional card transaction includes two sub-processes: (1) capture and authorization and (2) clearing and settlement. Below is an illustrative diagram of the flow of a typical card transaction and an explanation of each step in the process.



Capture and Authorization

In the capture and authorization process, the business obtains approval for payment from the card issuing bank. This process includes the following steps:

1. Once the consumer is ready to make a purchase, he or she presents their card for payment;
2. The card is swiped in the Point-of-Sale (POS) device at the business location, which captures the account information contained on the card's magnetic stripe or EMV-compliant chip;
    - In a mobile commerce transaction facilitated by a mobile wallet, such as Apple Pay, the appropriate card details are stored virtually on an application on the phone and transmitted to the POS device through a chip equipped with near-field communication (NFC) technology;
    - In an eCommerce transaction, the POS device is replaced by a virtual terminal application and the consumer types the card number into the check-out page of the online storefront. In some circumstances, an online wallet, such as PayPal, may be used to transmit the appropriate payment credentials;
3. The customer's card details are transmitted from the POS to the merchant acquirer, or the merchant acquirer's processor, via an internet connection or a phone line;

- In an eCommerce transaction, the information is encrypted and then transmitted to the merchant acquirer, or merchant acquirer's processor, via an online gateway;

4. The merchant acquirer, or the merchant acquirer's processor, identifies the appropriate payment network affiliated with the card, such as Visa, MasterCard, or *STAR*, and forwards the card details to the appropriate network;
5. The payment network receives the request for payment authorization, identifies the appropriate card issuing bank, and routes the transaction to the bank or its issuer processor;
6. The card issuing bank, or its issuer processor, receives the request and then executes a series of inquiries into its account systems to assess the potential risk of fraud for the transaction, establish that the account is in good standing, and verify that the cardholder has sufficient credit or adequate funds to cover the amount of the transaction;
7. The card issuing bank, or its issuer processor, approves or declines the transaction and sends back the response to the payment network. In this example the transaction is approved;
8. The payment network receives the approval and forwards the authorization to the merchant acquirer, or merchant acquirer's processor; and
9. The merchant acquirer, or merchant acquirer's processor, sends the authorization back to the POS device at the business location, which provides an approval confirmation and prints a receipt;
    - In a mobile commerce transaction, the approval confirmation and receipt may also be transmitted to the consumer's mobile wallet application or to the consumer via email;
    - In an eCommerce transaction, the authorization is sent to the online storefront, which communicates the approval to the consumer on the screen, and may provide the receipt for printing online or via email.

Clearing and Settlement

In the clearing and settlement process, a request for payment is initiated, funds are transferred and the transaction is posted to the business owner's and the consumer's account statements. The clearing and settlement process includes the following steps:

10. Typically at the end of the day, the business submits a batch of all of its approved authorizations to the merchant acquirer, or the merchant acquirer's processor, through a function on its POS device;
    - In the case of an eCommerce business, the online storefront's gateway sends the batch to the merchant acquirer, or to the merchant acquirer's processor;
11. The merchant acquirer, or the merchant acquirer's processor, receives the batch, notes the final amounts due for settlement, and routes the batch of approved authorizations to each applicable payment network;
12. Each payment network sends the batch of approved authorizations to the applicable card issuing bank, or its issuer processor, which posts the transaction to the consumer's statement;
13. Typically within 48 hours, the payment network calculates net settlement positions for the merchant acquirer and the card issuing bank, sends advisements to the merchant acquirer and card issuing bank, and submits a fund transfer order to a settlement bank; and
14. The settlement bank facilitates the exchange of funds between the merchant acquirer and the card issuing bank; and the merchant acquirer transfers the funds to the business owner's account.

Global Business Solutions Segment

The following table presents Global Business Solutions information as a percentage of total segment revenue and adjusted EBITDA:

	Year ended December 31,		
	2015	2014	2013
Segment revenue	58%	58%	59%
Adjusted EBITDA	62%	63%	67%

See note 7 "Segment Information" to our consolidated financial statements in Part II, Item 8 of this Form 10-K for a detail of segment revenue and adjusted EBITDA results.

Global Business Solutions Operations Our largest segment, Global Business Solutions, provides businesses of all sizes and types with a wide range of solutions at the point of sale, including merchant acquiring, eCommerce, mobile commerce, POS, and other business solutions. We served approximately 3.3 million business locations in the United States and 2.3 million outside the United States. Our largest service in this segment is merchant acquiring, which facilitates the acceptance of commercial transactions at the POS, whether a retail transaction at a physical business location, a mobile commerce transaction through a mobile or tablet device, or an eCommerce transaction over the Internet. In 2015, we acquired $1.7 trillion of payment volume in the United States and $178 billion of payment volume outside the United States.

We employ a variety of go-to-market strategies in our Global Business Solutions segment. We operate direct sales teams and also partner with indirect non-bank sales forces, such as independent sales agents, independent sales organizations (ISOs), independent software vendors (ISVs), value added retailers (VARs), and payment services providers (PSPs) to sell our commerce solutions to Small and Medium Sized Business (SMBs). In addition, we leverage the powerful sales capabilities of our bank partners to go to market through several structures, including joint venture equity alliances, revenue sharing alliances, and referral partnerships.

Our Global Business Solutions segment revenues are primarily derived from processing credit and debit card transactions for merchants and other business clients and includes fees for providing processing, loyalty and software services, and sales and leases of POS devices. Revenues are generated from a variety of sources, including:

- Discount fees charged to a merchant, net of credit and debit card interchange and assessment fees charged by the payment networks. The discount fee is typically either a percentage of the purchase amount or an interchange fee plus a fixed dollar amount;
- Processing fees charged to our alliances;
- Processing fees charged to merchant acquirers who have outsourced their transaction processing to us;
- Sales and leases of POS devices;
- Fees from providing reporting and other services; and
- Software fees such as security and *Clover* related fees.

We typically provide these services as part of a broader commerce-enabling solution to our business clients across multiple channels, including:

- Retail POS - Physical businesses or storefront locations, such as retailers, supermarkets, restaurants, and petroleum stations, with brick and mortar facilities, which we refer to as *Retail POS*;
- Mobile POS - Physical businesses with remote or wireless storefront locations, such as small retailers and service providers that use mobile devices to accept electronic payments, which we refer to as *Mobile POS*; and
- Online POS - Online businesses or website locations, such as retailers, digital content providers, and mobile app developers with Internet-based storefronts that can be accessed through a personal computer or a mobile device, which we refer to as *eCommerce*.

Clover Operating System We acquired *Clover*, an open architecture, integrated POS operating system, in December 2012 and invested in the technology to significantly enhance and expand its capabilities. Our goal with *Clover* is to create for business owners the largest open architecture platform of commerce-enabling solutions and applications in the world. We have expanded the family of *Clover* products to include the *Clover Station*, *Clover Mobile, Clover Mini*, and *Clover Go* and each device provides a broad range of next-generation features and software applications designed to help business clients conduct commerce. Within *Clover*, we also offer a cloud-based *Clover App Market* for business applications. Our software marketplace is designed specifically to provide business clients with integrated software applications that they can download and install quickly and easily on their *Clover* devices. Business applications can be developed internally by us, such as *Insightics* or by third party developers. As of December 31, 2015, the *Clover App Market* has 141 active business applications and 389 in development.

In addition to enhancing our ability to drive core acquiring sales, *Clover* allows us to earn incremental revenue from business clients. Currently, certain versions of *Clover* charge a recurring software-as-a-service fee, and we also earn economics from the *Clover App Market*, where we typically have a revenue share arrangement on paid applications with the application developer.

We also believe *Clover* can help enhance client retention because we believe it will become core to our clients' businesses, and position us as a value-added partner. For example, business owners may use applications in the *Clover App Market* to manage their employees' work schedules, operate customer loyalty programs, integrate transaction information directly into their accounting software, manage inventory, and provide analytics on their business.

Global Business Solutions Competition Our Global Business Solutions segment competes with merchant acquirers that include Vantiv, Worldpay, Global Payments, and Heartland Payment Systems, in addition to financial institutions that provide acquiring and processing services to businesses on their own, such as Chase Paymentech Solutions, Elavon (a subsidiary of U.S. Bancorp), and Barclaycard. In many cases our alliance and commercial partners compete against each other. Additionally, payment networks such as Visa and MasterCard are increasingly offering products and services that compete with our suite of solutions. Competitors of our next-generation services include PayPal, Braintree (a subsidiary of PayPal), CyberSource (a subsidiary of Visa Inc.), Adyen, and Stripe, along with integrated point of sale providers such as Micros, NCR, Square, ShopKeep, Revel, and others.

The primary competitive factors impacting this segment are brand, data security, breadth of features and functionality, ease of technological integration, strength of financial institution partnerships, price, and servicing capability. Other factors impacting

this segment include consolidation among large businesses and financial institutions, the pace of integrated point of sale solution development, and the creation of new payment methods and related technologies.

Global Business Solutions Seasonality Our Global Business Solutions segment experiences a modest level of seasonality, with the first quarter representing the lowest level of sales and the fourth quarter representing the highest level of sales. Over the past eight quarters, our quarterly revenue as a percentage of total yearly revenue has ranged between 23% and 26% each quarter.

Global Business Solutions Geographic Mix and Revenues Our Global Business Solutions segment generates approximately 78% of its revenues from clients in our North America region, 13% from clients in the EMEA region, 5% from clients in our APAC region, and 4% from clients in our LATAM region. The Global Business Solutions segment's revenues and earnings are impacted by the number of transactions and payment volume, the mix of consumer usage of credit cards, debit cards, and the size of the business.

Global Financial Solutions Segment

The following table presents Global Financial Solutions information as a percentage of total segment revenue and adjusted EBITDA:

	Year ended December 31,		
	2015	2014	2013
Segment revenue	21%	22%	21%
Adjusted EBITDA	20%	20%	16%

See note 7 "Segment Information" to our consolidated financial statements in Part II, Item 8 of this Form 10-K for a detail of segment revenue and adjusted EBITDA results.

Global Financial Solutions Operations Our Global Financial Solutions segment provides financial institutions, which include bank and non-bank issuers such as retailers with proprietary card portfolios, with a broad range of solutions that enable them to offer financial products and solutions to their customers. Our Global Financial Solutions segments serves approximately 1,400 financial institutions globally and deliver value to clients through a variety of channels, including end-to-end outsourced processing, managed services, and various software delivery models utilizing our proprietary *VisionPLUS* application. Our services include credit card and loan processing, commercial payments, and related supporting products. In 2015, we processed 7.4 billion transactions on our platforms. As of December 31, 2015, Global Financial Solutions managed 813 million card accounts on file in the United States, up 14% over 2014 and 146 million card accounts on file outside the United States, up 11% over 2014.

Our Global Financial Solutions clients include some of the world's largest financial institutions, which we serve across 90 countries. Our largest service in this segment is issuer processing, which helps banks and non-bank issuers provide credit, commercial, and retail card programs to their account holders. We also provide licensed and managed platforms for processing activities to financial institutions globally. Depending on the market, our solutions are often bundled with related offerings, such as statement printing and personalization of plastic cards, settlement and back office support, outsourced billing, remittance processing, and customer support call center services. As part of these solutions, we also provide custom programming and development to clients.

Global Financial Solutions' revenues and earnings are impacted by the number of consumer, commercial, and retail private label credit card accounts that are issued and actively in use. Revenue and profit growth is primarily driven by increased card usage, issuance of new cards from growth in existing clients and sales to new clients, and the related account conversions.

Our Global Financial Solutions' revenues are primarily derived from credit and retail card processing services, print, plastics, and remittance services, and loyalty and software services provided to financial institutions. Revenues for Global Financial Solutions are typically generated on the basis of number of accounts on file, statements/letters printed and mailed, and personalized plastics issued.

Processing Services and Licensing Processing services and licensing provide solutions to financial institutions and other issuers of credit, such as banks, group service providers, retailers, consumer finance companies, and credit unions that enable these issuers to process transactions on behalf of customers. Depending on our clients' needs, we deliver these solutions through our proprietary outsourced services platforms, software application licenses, or software-as-a-service hosted in the cloud. Services in our proprietary platform include transaction authorization and posting, account maintenance, and settlement. Our *VisionPLUS* software is used globally as both a processing solution and a licensed software solution that enables clients to process their own transactions, depending on the market. We also enable merchants and financial institutions to offer next generation payment solutions to their clients, such as Apple Pay, Android Pay, and Samsung Pay.

Revenues for card issuing processing services are derived from fees payable under contracts that depend primarily on the number of cardholder accounts on file. More revenue is derived from active accounts (those accounts on file that had a balance or any monetary posting or authorization activity during a specified period) than inactive accounts. Revenues are also derived from licensing fees for our *VisionPLUS* application, as well as cardholder and data transactions and professional services such as programming.

Account Support Services Along with our processing and licensing solutions, we provide a variety of supporting services throughout the life cycle of each account. Services include processing a card application, initiating service for the cardholder, accumulating the card's transactions into a monthly billing statement, and posting cardholder payments. Other services provided include customized communications to cardholders, plastics personalization and mailing, information verification associated with granting credit, debt collection, remittance processing, and client service on behalf of financial institutions. We also provide programming and customization to enhance and tailor our solutions to clients' needs through professional services.

Global Financial Solutions Competition Our Global Financial Solutions segment competes with card issuer processors, such as Total System Services, Vantiv, Fidelity National Information Services, Fiserv, Worldline, Equens, and SIX Payment Services, as well as the card issuer processing businesses of the global payment networks such as UnionPay Data. In addition, we compete with various software or custom-designed solutions that some financial institutions use to perform these services in-house.

The primary competitive factors impacting this segment are system performance and reliability, data security, breadth of features and functionality, disaster recovery capabilities and business continuity preparedness, platform scalability and flexibility, price, and servicing capability. Another factor impacting this segment is financial institution consolidation.

Global Financial Solutions Seasonality Our Global Financial Solutions segment experiences a modest level of seasonality, with the first quarter representing the lowest level of sales and the fourth quarter representing the highest level of sales. Over the past eight quarters, our quarterly revenue as a percentage of total yearly revenue has ranged between 24% and 26% each quarter.

Global Financial Solutions Geographic Mix and Revenues Our Global Financial Solutions segment generates approximately 59% of its revenues from clients in our North America region, 29% from clients in our EMEA region, 7% from clients in our LATAM region, and 5% from clients in our APAC region. Within the United States, revenues are diversified across financial institutions of all sizes and are spread across the country.

Network & Security Solutions Segment

The following table presents Network & Security Solutions information as a percentage of total segment revenue and adjusted EBITDA:

	Year ended December 31,		
	2015	2014	2013
Segment revenue	21%	20%	20%
Adjusted EBITDA	23%	23%	22%

See note 7 "Segment Information" to our consolidated financial statements in Part II, Item 8 of this Form 10-K for a detail of segment revenue and adjusted EBITDA results.

Network & Security Solutions Operations Our Network & Security Solutions segment provides a range of network solutions and security, risk and fraud management solutions to business and financial institution clients in our Global Business Solutions and Global Financial Solutions segments, and independently to financial institutions, businesses, governments, processors and other clients. Our EFT Network Solutions manage debit card and account processing solutions and facilitate EFT commerce, such as PIN debit, PIN-less debit, and ATM transactions. Our *STAR Network* enables clients to encrypt, route, and decrypt various types of financial data, process debit and ATM transactions, and provide access to demand deposit accounts. In 2015, our *STAR Network* routed approximately 4.3 billion transactions in the United States. Our *Stored Value Network Solutions* facilitate stored value commerce, such as (1) closed-loop prepaid transactions, which are initiated by various types of prepaid cards issued by enterprises, such as retailers, that issue enterprise-branded cards that can generally be used only at the enterprise issuing the card or account, and (2) open-loop prepaid transactions, which are initiated by various types of prepaid cards issued by a bank and carry a network association brand, such as Visa or MasterCard, enabling them to be used at multiple merchant locations. This segment also includes our Data and Analytics Solutions, Online and Mobile Banking Solutions, Healthcare Solutions, and Government Solutions, and serves clients in the United States and outside the United States.

EFT Network Solutions enables our business and financial institution clients to route secure, encrypted data between themselves on our *STAR Network* to facilitate PIN and PIN-less debit and ATM transactions. Our *STAR Network* is connected to approximately 3,600 financial institutions and community banks, over 1 million POS and ATM locations, and numerous third-party payment processors, ATM processors, and card processors that participate in the network. When a business, a merchant acquirer, or an ATM owner acquires a *STAR Network* transaction, it sends the transaction data to the network switch, which is operated by us, which in turn routes the encrypted information to the appropriate financial institution for authorization. To be routed through the *STAR Network*, a transaction must be initiated with a card participating in the *STAR Network* at an ATM or POS device also participating in the *STAR Network*.

Revenues related to the *STAR Network* are derived from fees payable under contracts and negotiated rate structures, but are driven more by the data transactions processed than by accounts on file. In a situation in which a debit transaction uses our network and we are the debit card processor for the financial institution as well as the merchant acquirer for the business, we are eligible to receive one or more of the following:

- a fee from the card issuing financial institution for running the transaction through the *STAR Network*;
- a fee from the card issuer for obtaining the authorization;
- a fee from the business for acquiring the transaction, recognized in the Global Business Solutions segment; and
- a network acquirer fee from the business for accessing the *STAR Network*.

There are other possible configurations of transactions that result in us receiving multiple fees for a transaction, depending on the role we play.

Stored Value Network manages prepaid stored-value card issuance and processing services (i.e. gift cards) for retailers and others. The full-service stored-value/gift card program offers transaction processing services, card issuance, and customer service for over 200 national brands and several thousand small and mid-tier merchants. We also provide program management and processing services for association-branded, bank-issued, open loop (a card that can be used at multiple merchants), stored-value, reloadable, and one time prepaid card products. Revenues are generated from a variety of sources including processing fees for transactions processed and fees for card production and shipments.

Our commercial prepaid offerings are primarily sold to businesses and are comprised of:

- *ValueLink* - Provides card and account issuing, program management, and transaction processing services for a range of prepaid card programs. Our closed-loop prepaid programs include gift, incentive, and rebate cards. We serve over 200 brands globally and several thousand SMBs. Our programs include reloadable and non-reloadable prepaid cards, and may be used with a variety of mobile applications.

- *Money Network* - Provides open-loop electronic payroll distribution solutions that reduce or eliminate an employer's expense associated with traditional paper paychecks and helps employees without bank accounts avoid check cashing fees. The solution also provides important employee security as the funds are stored on the account, not as cash that can be lost or stolen. *Money Network* accounts can be used at any business location that accepts Visa or MasterCard branded cards, includes a packet of checks to be used to pay bills and avoid the cost of money orders, and offers a web portal to track account activity.

- *Gyft* - A leading digital platform that enables consumers to buy, send, manage, and redeem virtual closed-loop cards using mobile devices. The *Gyft* solution, combined with our leadership in prepaid issuing solutions, creates a unique combination to support growth in a rapidly expanding market for virtual cards.

- *Transaction Wireless* - A leading digital platform that enables businesses to sell virtual gift cards online, either to consumers through an integration with their eCommerce storefront, or to other businesses through a proprietary business-to-business solution.

Security and Fraud Solutions provide a range of security, risk, and fraud management solutions that help businesses and financial institutions securely run and grow their business by protecting their data, managing risk, and preventing fraud. Our solutions include *TransArmor*, our encryption, tokenization, and PCI compliance solution for POS data in-transit, *Fraud Predictor Plus*, our solution to detect fraud at the POS through a machine-learning based predictive model, and *TeleCheck*, the industry-leading database of check-writers activity. *TeleCheck* provides check verification, settlement, and guarantee services using our proprietary data-based system. Businesses can use this system to lower the risk of check acceptance or to have all checks guaranteed if approved. Revenues for our security solutions are earned on a licensed basis or per transaction.

Check Verification, Settlement, and Guarantee Services TeleCheck offers check verification, settlement, and guarantee services using our proprietary database system to assist merchants in deciding whether accepting checks at the POS is a reasonable risk, or, further, to guarantee checks presented to merchants if they are approved. These services include risk management services, which utilize software, information, and analysis to assist the merchant in the decision process and include identity fraud prevention and reduction. Revenues are earned by charging merchant fees for check verification or guarantee services.

Network & Security Solutions Competition Our Network & Security Solutions segment competes with networks such as Visa, MasterCard, and Discover for debit network services, and with Fidelity National Information Services for debit network and check verification and guarantee services. We also face competition from regional operators of debit networks. Our portfolio of analytics, information, security and risk management solutions competes with a wide range of providers across multiple disciplines, including Visa, MasterCard, Voltage, Verisk, Equifax, Experian, TransUnion, and Fair Isaac.

The primary competitive factors impacting this segment are system performance and reliability, data security, breadth of features and functionality, platform scalability and flexibility, price, and financial institution consolidation. Other factors impacting this segment include increasingly powerful and affordable technology capacity, improved data management and analytic tools, and emergence of cloud-based delivery models.

Network & Security Solutions Seasonality Our Network & Security Solutions segment experiences a modest level of seasonality, with the first quarter representing the lowest level of sales and the fourth quarter representing the highest level of sales. Over the past eight quarters, our quarterly revenue as a percentage of total yearly revenue has ranged between 23% and 27% each quarter.

Network & Security Solutions Geographic Mix and Revenues Our Network & Security Solutions segment is comprised of more than 99% domestic businesses.

Network & Security Solutions Acquisitions and Dispositions We have recently made the following acquisitions and product developments:

Transaction Wireless Inc. In 2015, we acquired Transaction Wireless, Inc. (TWI) a provider of digital stored value products that offer gift card programs, loyalty incentives, and integrated marketing solutions for retailers, partners, and consumers.

Gyft In 2014, we acquired Gyft, Inc. (*Gyft*), the leading digital platform that enables consumers to buy, send, manage, and redeem gift cards using mobile devices. *Gyft's* exceptional capabilities, combined with our long-standing leadership in prepaid solutions, create a distinct combination in a rapidly growing market for virtual gift cards.

In 2014, we completed the sale of our 30% minority interest in a transportation payments business, Electronic Funds Source LLC (EFS).

Corporate

Corporate operations include corporate-wide governance functions such as our executive management team, aviation, tax, treasury, internal audit, corporate strategy, and certain accounting, human resources and legal costs related to supporting the corporate function. Costs incurred by Corporate that are attributable to a segment are allocated to the respective segment.

Global Regions

Over the past 15 years, we have established a global leadership position. We currently have operations in 36 countries and serve businesses and financial institutions in 118 countries around the world as illustrated on the following map:

We deliver our solutions throughout the world via four regions:

North America

North America (United States and Canada) is our largest region. We are the largest merchant acquirer, issuer processor, independent network services provider in the region. The United States is our largest market in the world and accounts for the majority of our activity in the region. In 2015, we processed approximately 68 billion commercial transactions and acquired $1.7 trillion of payment volume in the United States, accounting for nearly 10% of U.S. GDP.

Europe, Middle East, and Africa (EMEA)

We have operations in 19 countries and serve clients in 65 countries in this region. We are a leading acquirer processor in EMEA and provide our suite of next-generation commerce-enabling solutions to businesses and financial institutions of all sizes and types.

Latin America (LatAm)

We have operations in 7 countries and serve clients in 32 countries in this region. We are a leading merchant acquirer, issuer processor, and eCommerce processor to businesses and financial institutions of all sizes and types in the region.

Asia Pacific (APAC)

We have operations in 8 countries and serve clients in 19 countries in this region. We are a leading merchant acquirer, issuer processor, ATM services provider, and eCommerce processor to businesses and financial institutions of all sizes and types in the region and have begun to introduce other commerce-enabling solutions in selected markets.

Intellectual Property

We own a global portfolio of many trademarks, trade names, patents, and other intellectual property that are important to our future success. The only intellectual property rights that are individually material to us are the *First Data* trademark and trade name, and the *STAR* trademark and trade name. The *STAR* trademark and trade name are used in the Network & Security Solutions segment. The *First Data* trademark and trade name are associated with quality and reliable electronic commerce and payments solutions. Financial institutions and merchants associate the *STAR* trademark and trade name with quality and reliable debit network services and processing services. Loss of the proprietary use of the *First Data* or *STAR* trademarks and trade names or a diminution in the perceived quality associated with these names could harm the growth of our businesses.

Employees and Labor

As of December 31, 2015, we had approximately 24,000 employees. The majority of the employees of our subsidiaries outside of the United States are subject to the terms of individual employment agreements. One of our wholly owned subsidiaries has approximately 1,600 employees in the United Kingdom, a portion of whom are members of the Unite trade union. Employees of our subsidiaries in Vienna, Austria; Frankfurt, Germany; and Nürnberg, Germany are also represented by local work councils. The Vienna workforce and a portion of the Frankfurt workforce are also covered by a union contract. Certain employees of our Korean subsidiary are represented by a Labor-Management council. In Brazil, all employees are unionized and covered by the terms of industry-specific collective agreements. Employees in certain other countries are also covered by the terms of industry-specific national collective agreements. None of our employees are otherwise represented by any labor organization in the United States. We believe that our relations with our employees and the labor organizations identified above are in good standing.

Available Information

Our principal executive offices are located at 225 Liberty Street, 29th Floor, New York, NY 10281, telephone (800) 735-3362. Our annual report on Form 10-K, quarterly reports on Form 10-Q, current reports on Form 8-K, and amendments to those reports are available free of charge to shareholders and other interested parties through the "Investor Relations" portion of our website at http://investor.firstdata.com as soon as reasonably practical after they are filed with the Securities and Exchange Commission (SEC). The SEC maintains a website, www.sec.gov, which contains reports and other information filed electronically with the SEC by us. Various corporate governance documents, including our Audit Committee Charter, Governance, Compensation and Nominations Committee Charter, and Code of Ethics for Senior Financial Officers are available without charge through the "About Us" "Investor Relations" "Corporate Governance" portion of our investor relations website, listed above.

Government Regulations

Various aspects of our service areas are subject to U.S. federal, state, and local regulation, as well as regulation outside the United States. Failure to comply with regulations may result in the suspension or revocation of licenses or registrations, the limitation, suspension or termination of service, and/or the imposition of civil and criminal penalties, including fines. Certain of our services also are subject to rules promulgated by various payment networks and banking authorities as more fully described below.

The Dodd-Frank Act In July 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) was signed into law in the United States. The Dodd-Frank Act has resulted in significant structural and other changes to the regulation of the financial services industry. Among other things, Title X of the Dodd-Frank Act established a new, independent regulatory agency known as the Consumer Financial Protection Bureau (CFPB) to regulate consumer financial products and services (including some offered by our clients). The CFPB may also have authority over us as a provider of services to regulated financial institutions in connection with consumer financial products. Separately, under the Dodd-Frank Act, debit interchange transaction fees that a card issuer receives and are established by a payment card network for an electronic debit transaction are now regulated by the Board of Governors of the Federal Reserve System (Federal Reserve Board), and must be "reasonable and proportional" to the cost incurred by the card issuer in authorizing, clearing, and settling the transaction. Effective October 1, 2011, the Federal Reserve Board capped debit interchange rates for card issuers operating in the United States with assets of $10 billion or more at the sum of $0.21 per transaction and an ad valorem component of 5 basis points to reflect a portion of the issuer's fraud losses plus, for qualifying issuers, an additional $0.01 per transaction in debit interchange for fraud prevention costs. In addition, the new regulations contain non-exclusivity provisions that ban debit payment card networks from prohibiting an issuer from contracting with any other payment card network that may process an electronic debit transaction involving an issuer's debit cards and prohibit card issuers and payment networks from inhibiting the ability of merchants to direct the routing of debit card transactions over any network that can process the transaction. Beginning April 1, 2012, all debit card issuers in the United States were required to participate in at least two unaffiliated debit payment card networks. On April 1, 2013, the ban on network exclusivity arrangements became effective for prepaid card and healthcare debit card issuers, with certain exceptions for prepaid cards issued before that date.

Effective July 22, 2010, merchants were allowed to set minimum dollar amounts (not to exceed $10) for the acceptance of a credit card (while federal governmental entities and institutions of higher education may set maximum amounts for the acceptance of credit cards). They were also allowed to provide discounts or incentives to entice consumers to pay with an alternative payment method, such as cash, checks or debit cards. In addition, the Dodd-Frank Act created a new entity, the Financial Stability Oversight Council, and authorized it to require that a nonbank financial company that is deemed to pose a systemic risk to the U.S. financial system become subject to consolidated, prudential supervision by the Federal Reserve Board. At this point it is unclear whether we would be subject to additional systemic risk related oversight.

Association and Network Rules We are subject to rules of MasterCard, Visa, INTERAC, PULSE, and other payment networks. In order to provide processing services, a number of our subsidiaries are registered with Visa and/or MasterCard as service providers for member institutions. Various subsidiaries of ours are also processor level members of numerous debit and electronic benefits transaction networks or are otherwise subject to various network rules in connection with processing services and other services we provide. As such, we are subject to applicable card association, network, and national scheme rules that could subject us to fines or penalties. We are also subject to network operating rules promulgated by the National Automated Clearing House Association relating to payment transactions processed by us using the Automated Clearing House Network and to various state and federal laws regarding such operations, including laws pertaining to electronic benefits transaction.

Cashcard Australia Limited (Cashcard) is a member of the Australian Consumer Electronic Clearing System (CECS), which is a debit payment system regulated by network operating rules established and administered by Australian Payments Clearing Association Limited, and is a member of the ATM Access Australia Limited and the Electronic Funds Transfer at Point of Sale (eftpos®) Access Australia Limited that administer reciprocal access and interchange arrangements for ATMs and eftpos®, respectively, in Australia. The network operating rules, ATM Access Code and eftpos® Access Code impose a variety of sanctions, including suspension or termination of membership and fines for non-compliance. Cashcard also operates its own network of members, regulated by rules promulgated by Cashcard. To enable Cashcard to settle in CECS directly with banks and financial institutions, Cashcard maintains an Exchange Settlement Account which is supervised by the Reserve Bank of Australia (RBA), and that requires Cashcard to adhere to conditions imposed by RBA.

Our subsidiary in Germany, TeleCash GmbH & Co. KG, is certified and regulated as a processor for domestic German debit card transactions by the Deutsche Kreditwirtschaft (DK), the German banking association. Failure to comply with the technical requirements set forth by the DK may result in suspension or termination of services.

Banking Regulations Because a number of our subsidiary businesses provide data processing services for financial institutions, we are subject to examination by the Federal Financial Institutions Examination Council, which examines large data processors in order to identify and mitigate risks associated with significant service providers.

FDR Limited is authorized and regulated in the United Kingdom by the Financial Conduct Authority, one of the two principal financial markets regulators in the United Kingdom. FDR Limited is authorized by the Financial Conduct Authority to arrange and advise on certain insurance contracts for the purpose of arranging insurance taken out by its issuer clients' cardholders. FDR Limited is also required to obtain permission from the Financial Conduct Authority by March 31, 2016 in respect of certain consumer credit related activities in order to continue to carry on such activities after that date for the purposes of its issuer services and merchant terminal leasing businesses. FDR Limited has applied for this permission and, in the meantime, the Financial Conduct Authority has granted FDR Limited an interim consumer credit permission effective April 1, 2014 (being the date when the Financial Conduct Authority took over as the regulatory body for consumer credit). As a firm authorized by the Financial Conduct Authority, FDR Limited is required to comply with certain prudential, conduct of business and reporting requirements.

As a result of the implementation of the Payment Services Directive (2007/64/EC) in the European Union, a number of our subsidiaries in the Global Business Solutions segment hold payment institution licenses in the European Union member states in which such subsidiaries do business. As payment institutions, we are subject to regulation and oversight in the applicable European Union member state, which includes (amongst other obligations) a requirement to maintain specified regulatory capital. In July 2013, the European Commission proposed legislation in two parts, covering a wide range of proposed regulatory reforms affecting the payments industry across the European Union. The first part was a proposed European Union-wide regulation on interchange fees for card-based payment transactions (Interchange Fee Regulation). The Interchange Fee Regulation (2015/751) was published in May 2015 and entered into effect in June 2015. The second part consisted of a recasting of the Payment Services Directive. The European Commission's PSD2 proposal has been considered by the two other main European Union legislative institutions, the Council of the European Union and the European Parliament. The Council of the European Union published its final compromise proposal on the PSD2 in June 2015.

First Data Trust Company, LLC (FDTC) engages in trust activities previously conducted by the trust department of a former banking subsidiary of ours and is subject to regulation, examination, and oversight by the Division of Banking of the Colorado Department of Regulatory Agencies. Since FDTC is not a "bank" under the Bank Holding Company Act of 1956, as amended (BHCA), our affiliation with FDTC does not cause us to be regulated as a bank holding company or financial holding company under the BHCA.

TeleCheck Payment Systems Limited (TPSL) in Australia holds an Australian Financial Services License under Chapter 7 of the Australian Corporations Act 2001, which regulates the provision of a broad range of financial services in Australia. The license, issued by the Australian Securities and Investments Commission, entitles the Australian operations of TPSL to deal in and provide general financial product advice about its check guarantee and check verification product and requires that TPSL's Australian operations issue product documents that comply with specific content requirements and follow prescribed procedures.

Further, several subsidiaries provide services such as factoring or settlement that make them subject to regulation by local banking agencies, including the National Bank of Slovakia, the National Bank of Poland and the German Federal Financial Supervision Agency.

Privacy and Information Security Regulations We provide services that may be subject to various state, federal, and foreign privacy laws and regulations, including, among others, the Gramm-Leach-Bliley Act and Directive 95/46/EC, the Australian Privacy Act, the Personal Information Protection and Electronic Documents Act in Canada, the Personal Data (Privacy) Ordinance in Hong Kong, the Malaysian Data Protection Act 2010, and the Singapore Data Protection Act 2012. These laws and their implementing regulations restrict certain collection, processing, storage, use, and disclosure of personal information, require notice to individuals of privacy practices, and provide individuals with certain rights to prevent use and disclosure of protected information. These laws also impose requirements for the safeguarding and proper destruction of personal information through the issuance of data security standards or guidelines. Certain federal and state laws impose similar privacy obligations and, in certain circumstances, obligations to notify affected individuals, state officers, the media, and consumer reporting agencies, as well as businesses and governmental agencies that own the information, of security breaches affecting personal information. In addition, there are state laws restricting the ability to collect and utilize certain types of information such as Social Security and driver's license numbers. In February 2013, the European Commission proposed additional European Union-wide legislation regarding cyber security in the form of the proposed Network and Information Security Directive (NIS Directive). The NIS Directive is currently being considered by the two other main European Union legislative institutions, the Council of the European Union and the European Parliament. On June 29, 2015, the Council of the European Union announced that agreement had been reached in informal negotiations on the main principles of the NIS Directive.

Credit Reporting and Debt Collections Regulations *TeleCheck* is subject to the Federal Fair Credit Reporting Act and various similar state laws based on *TeleCheck's* maintenance of a database containing the check-writing histories of consumers and the use of that information in connection with its check verification and guarantee services.

The collection business within TRS Recovery Services, Inc. (TRS) is subject to the Federal Fair Debt Collection Practices Act and various similar state laws. TRS has licenses in a number of states in order to engage in collection in those states. In the United Kingdom, FDR Limited has a license under the Consumer Credit Act of 1974 (CCA) to enable it to undertake, among other things, credit administration and debt collections activities on behalf of its card issuing clients through calls and correspondence with the cardholders. FDR Limited is also licensed under the CCA to carry on the activity of a consumer hire business for the purpose of leasing devices to merchants.

TeleCheck and TRS are subject to regulation, supervision, and examination from the CFPB. Further regulations may be imposed in the future as state governments and federal agencies identify and consider supplementary consumer financial protection, including laws regulating activities with respect to current or emerging technology such as automated dialers or pre-recorded messaging or calls to cellular phones, which could impair the collection by TRS of returned checks and those purchased under *TeleCheck's* guarantee services. Moreover, reducing or eliminating access to and use of information on drivers licenses, requiring blocking of access to credit reports or scores, mandating score or scoring methodology disclosure and proscribing the maintenance or use of consumer databases could reduce the effectiveness of *TeleCheck's* risk management tools or otherwise increase its costs of doing business.

In addition, several of our subsidiaries are subject to comparable local laws regarding collection activities and obtaining credit reports.

Unfair Trade Practice Regulations We and our clients are subject to various federal, state, and international laws prohibiting unfair or deceptive trade practices, such as Section 5 of the Federal Trade Commission Act. Various regulatory enforcement agencies, including the Federal Trade Commission (FTC) and state attorneys general, have authority to take action against parties

that engage in unfair or deceptive trade practices or violate other laws, rules, and regulations and to the extent we are processing payments for a client that may be in violation of laws, rules, and regulations, we may be subject to enforcement actions and incur losses and liabilities that may impact our business. For example, *TeleCheck* and TRS are subject to a consent decree with the FTC which, among other items, addresses the timeliness of certain actions that they take.

Anti-Money Laundering, Anti-Bribery, Sanctions, and Counter-Terrorist Regulations We are subject to anti-money laundering laws and regulations, including the Bank Secrecy Act, as amended by the USA PATRIOT Act of 2001 (collectively, BSA). Among other things, the BSA requires money services businesses (such as money transmitters, issuers of money orders and official checks, and providers of prepaid access) to develop and implement risk-based anti-money laundering programs, report large cash transactions and suspicious activity, and to maintain transaction records. Our subsidiary Money Network Financial LLC provides prepaid access for various open loop prepaid programs for which it is the program manager and therefore must meet the requirements of the Financial Crimes Enforcement Network, the agency that enforces the BSA.

We are also subject to anti-corruption laws and regulations, including the United States Foreign Corrupt Practices Act (FCPA) and other laws, that prohibit the making or offering of improper payments to foreign government officials and political figures and includes anti-bribery provisions enforced by the Department of Justice and accounting provisions enforced by the Securities and Exchange Commission (SEC). The FCPA has a broad reach and requires maintenance of appropriate records and adequate internal controls to prevent and detect possible FCPA violations. Many other jurisdictions where we conduct business also have similar anticorruption laws and regulations. We have policies, procedures, systems, and controls designed to identify and address potentially impermissible transactions under such laws and regulations.

We are also subject to certain economic and trade sanctions programs that are administered by the Treasury Department's Office of Foreign Assets Control (OFAC), which prohibit or restrict transactions to or from or dealings with specified countries, their governments, and in certain circumstances, their nationals, and with individuals and entities that are specially-designated nationals of those countries, narcotics traffickers, and terrorists or terrorist organizations. Other group entities may be subject to additional local sanctions requirements in other relevant jurisdictions.

Similar anti-money laundering and counter terrorist financing and proceeds of crime laws apply to movements of currency and payments through electronic transactions and to dealings with persons specified in lists maintained by the country equivalents to OFAC lists in several other countries and require specific data retention obligations to be observed by intermediaries in the payment process. Our businesses in those jurisdictions are subject to those data retention obligations. In the European Union, for example, certain of our businesses are subject to requirements under the Third Money Laundering Directive (2005/60/EC) (MLD3) as implemented in relevant European Union member states. MLD3 was repealed and replaced by the Fourth Money Laundering Directive ((EU) 2015/849) (MLD4), when the latter entered into force on June 25, 2015. European Union member states are required to implement MLD4 into national law by June 26, 2017.

Money Transmission and Payment Instrument Licensing and Regulations We are subject to various U.S. federal, state, and foreign laws and regulations governing money transmission and the issuance and sale of payment instruments, including some of our prepaid products.

In the United States, most states license money transmitters and issuers of payment instruments. Many states exercise authority over the operations of our services related to money transmission and payment instruments and, as part of this authority, subject us to periodic examinations. Many states require, among other things, that proceeds from money transmission activity and payment instrument sales be invested in high-quality marketable securities before the settlement of the transactions. Such licensing laws also may cover matters such as regulatory approval of consumer forms, consumer disclosures and the filing of periodic reports by the licensee, and require the licensee to demonstrate and maintain levels of net worth. Many states also require money transmitters, issuers of payment instruments, and their agents to comply with federal and/or state anti-money laundering laws and regulations.

Escheat Regulations We are subject to unclaimed or abandoned property (escheat) laws both in the United States and abroad that require us to turn over to certain government authorities the property of others held by us that has been unclaimed for a specified period of time such as, in the Integrated Payment Systems (IPS) business, payment instruments that have not been presented for payment or, in the Global Business Solutions segment, account balances that cannot be returned to a merchant following discontinuation of its relationship with us. A number of our subsidiaries hold property subject to escheat laws and we have an ongoing program to comply with those laws. We are subject to audit by individual U.S. states with regard to our escheatment practices.

Indirect Regulatory Requirements A number of our clients are financial institutions that are directly subject to various regulations and compliance obligations issued by the CFPB, the Office of the Comptroller of the Currency and other agencies responsible for regulating financial institutions. While these regulatory requirements and compliance obligations do not apply directly to us, many

of these requirements materially affect the services we provide to our clients and us overall. To remain competitive, we expend significant resources to assist our clients in meeting their various compliance obligations, including the cost of updating our systems and services as necessary to allow our clients to comply with applicable laws and regulations, and the cost of dedicating sufficient resources to assist our clients in meeting their new and enhanced oversight and audit requirements established by the CFPB, the Office of the Comptroller of the Currency and others. The banking agencies, including the Office of the Comptroller of the Currency, also have imposed requirements on regulated financial institutions to manage their third-party service providers. Among other things, these requirements include performing appropriate due diligence when selecting third-party service providers; evaluating the risk management, information security, and information management systems of third-party service providers; imposing contractual protections in agreements with third-party service providers (such as performance measures, audit and remediation rights, indemnification, compliance requirements, confidentiality and information security obligations, insurance requirements, and limits on liability); and conducting ongoing monitoring of the performance of third-party service providers. Accommodating these requirements applicable to our clients imposes additional costs and risks in connection with our financial institution relationships. We expect to expend significant resources on an ongoing basis in an effort to assist our clients in meeting their legal requirements.

Other Stored-value services we offer to issuers in the United States and internationally are subject to various federal, state, and foreign laws and regulations, which may include laws and regulations related to consumer and data protection, licensing, escheat, anti-money laundering, banking, trade practices and competition, and wage and employment. These laws and regulations are evolving, unclear, and sometimes inconsistent and subject to judicial and regulatory challenge and interpretation, and therefore the extent to which these laws and rules have application to, and their impact on, us, financial institutions, merchants or others is in flux. At this time we are unable to determine the impact that the clarification of these laws and their future interpretations, as well as new laws, may have on us, financial institutions, merchants or others in a number of jurisdictions. These services may also be subject to the rules and regulations of the various international, domestic and regional schemes, networks, and associations in which we and the card issuers participate.

In addition, the Housing Assistance Tax Act of 2008 included an amendment to the Internal Revenue Code that requires information returns to be made for each calendar year by merchant acquiring entities and third-party settlement organizations with respect to payments made in settlement of payment card transactions and third-party payment network transactions occurring in that calendar year. Reportable transactions are also subject to backup withholding requirements. We could be liable for penalties if we are not in compliance with these rules.

ITEM 1A. RISK FACTORS

The following are certain risks that could affect our business and our results of operations. The risks identified below are not all encompassing but should be considered in establishing an opinion of our future operations.

Business and Operational Risks

Global economic, political, and other conditions may adversely affect trends in consumer, business, and government spending, which may adversely impact the demand for our services and our revenue and profitability.

Financial services, payments, and technology industries in which we operate depend heavily upon the overall level of consumer, business, and government spending. A sustained deterioration in the general economic conditions (including distress in financial markets, turmoil in specific economies around the world, and additional government intervention), particularly in the United States or Europe, or increases in interest rates in key countries in which we operate may adversely affect our financial performance by reducing the number or average purchase amount of transactions involving payment cards. A reduction in the amount of consumer spending could result in a decrease of our revenue and profits. The current threats to global economic growth include geopolitical instability in Brazil, Venezuela, Russia, Ukraine, the Middle East and other oil producing countries. Instability in these regions could affect economic conditions in the Eurozone and the U.S.

Adverse economic trends may accelerate the timing, or increase the impact of, risks to our financial performance. Such trends may include, but are not limited to, the following:

- Declining economies, foreign currency fluctuations, and the pace of economic recovery can change consumer spending behaviors, such as cross-border travel patterns, on which a significant portion of our revenues are dependent.
- Low levels of consumer and business confidence typically associated with recessionary environments and those markets experiencing relatively high unemployment, may cause decreased spending by cardholders.
- Budgetary concerns in the United States and other countries around the world could affect the United States and other specific sovereign credit ratings, impact consumer confidence and spending, and increase the risks of operating in those countries.
- Emerging market economies tend to be more volatile than the more established markets we serve in the United States and Europe, and adverse economic trends may be more pronounced in such emerging markets.
- Financial institutions may restrict credit lines to cardholders or limit the issuance of new cards to mitigate cardholder defaults.
- Uncertainty and volatility in the performance of our clients' businesses may make estimates of our revenues, rebates, incentives, and realization of prepaid assets less predictable.
- Our clients may decrease spending for value-added services.
- Government intervention, including the effect of laws, regulations, and /or government investments in our clients, may have potential negative effects on our business and our relationships with our clients or otherwise alter their strategic direction away from our products.

A weakening in the economy could also force some retailers to close, resulting in exposure to potential credit losses and declines in transactions, and reduced earnings on transactions due to a potential shift to large discount merchants. Additionally, credit card issuers may reduce credit limits and become more selective in their card issuance practices. Changes in economic conditions could adversely impact our future revenues and profits and result in a downgrade of our debt ratings, which may lead to termination or modification of certain contracts and make it more difficult for us to obtain new business. Any of these developments could have a material adverse impact on our overall business and results of operations.

Our ability to anticipate and respond to changing industry trends and the needs and preferences of our clients and consumers may affect our competitiveness or demand for our products, which may adversely affect our operating results.

Financial services, payments, and technology industries are subject to rapid technological advancements, new products and services, including mobile payment applications, evolving competitive landscape, developing industry standards, and changing client and consumer needs and preferences. We expect that new services and technologies applicable to the financial services, payments, and technology industries will continue to emerge. These changes in technology may limit the competitiveness of and demand for our services. Also, our clients and their customers continue to adopt new technology for business and personal uses. We must anticipate and respond to these changes in order to remain competitive within our relative markets. For example, our ability to provide innovative point-of-sale technology to our merchant clients could have an impact on our Global Business Solutions business.

Failure to develop value-added services that meet the needs and preferences of our clients could have an adverse effect on our ability to compete effectively in our industry. Furthermore, clients' and their customers' potential negative reaction to our products and services can spread quickly through social media and damage our reputation before we have the opportunity to respond. If we are unable to anticipate or respond to technological changes or evolving industry standards on a timely basis, our ability to remain competitive could be materially adversely affected.

Substantial and increasingly intense competition worldwide in the financial services, payments, and technology industries may materially and adversely affect our overall business and operations.

Financial services, payments, and technology industries are highly competitive and our payment solutions compete against all forms of financial services and payment systems, including cash and checks, and electronic, mobile, and eCommerce payment platforms. If we are unable to differentiate ourselves from our competitors, drive value for our clients and/or effectively align our resources with our goals and objectives, we may not be able to compete effectively. Our competitors may introduce their own value-added or other services or solutions more effectively than we do, which could adversely impact our growth. We also compete against new entrants that have developed alternative payment systems, eCommerce payment systems, and payment systems for mobile devices. Failure to compete effectively against any of these competitive threats could have a material adverse effect on us. In addition, the highly competitive nature of our industry could lead to increased pricing pressure which could have a material impact on our overall business and results of operations.

Potential changes in the competitive landscape, including disintermediation from other participants in the payments value chain, could harm our business.

We expect that the competitive landscape will continue to change, including:

- Rapid and significant changes in technology, resulting in new and innovative payment methods and programs that could place us at a competitive disadvantage and that could reduce the use of our products.
- Competitors, clients, governments, and other industry participants may develop products that compete with or replace our value-added products and services.
- Participants in the financial services, payments, and technology industries may merge, create joint ventures, or form other business combinations that may strengthen their existing business services or create new payment services that compete with our services.
- New services and technologies that we develop may be impacted by industry-wide solutions and standards related to migration to EMV chip technology, tokenization, or other safety and security technologies.

Failure to compete effectively against any of these competitive threats could have a material adverse effect on us.

The market for our electronic commerce services is evolving and may not continue to develop or grow rapidly enough for us to maintain and increase our profitability.

If the number of electronic commerce transactions does not continue to grow or if consumers or businesses do not continue to adopt our services, it could have a material adverse effect on the profitability of our business, financial condition, and results of operations. We believe future growth in the electronic commerce market will be driven by the cost, ease-of-use, and quality of products and services offered to consumers and businesses. In order to consistently increase and maintain our profitability, consumers and businesses must continue to adopt our services, including our merchant suite, *Clover*, *Perka*, and *Gyft* solutions.

We depend, in part, on our merchant relationships and alliances to grow our Global Business Solutions business. If we are unable to maintain these relationships and alliances, our business may be adversely affected.

Our alliance structures take on different forms, including consolidated subsidiaries, equity method investments, and revenue sharing arrangements. Under our alliance program, a bank or other institution forms an alliance with us on an exclusive basis, either contractually or through a separate legal entity. Merchant contracts may be contributed to the alliance by us and/or the bank or institution. The banks and other institutions generally provide card association sponsorship, clearing, and settlement services and typically act as a merchant referral source when the institution has an existing banking or other relationship with such merchant. We provide transaction processing and related functions. Both we and our alliance partners may also provide management, sales, marketing, and other administrative services. The alliance structure allows us to be the processor for multiple financial institutions, any one of which may be selected by the merchant as its bank partner. We rely on the growth of our merchant relationships, alliances, and other distribution channels to support our business. There can be no guarantee that we will achieve this growth. In addition, our contractual arrangements with our merchants and merchant alliance partners are for fixed terms and may also allow for early termination upon the occurrence of certain events. There can be no assurance that we will be able to renew our contractual

arrangements with these merchants or merchant alliance partners on similar terms or at all. The loss of merchant relationships or alliance and financial institution partners could negatively impact our business and result in a reduction of our revenue and profit.

Failure to obtain new clients or renew client contracts on favorable terms could adversely affect results of operations and financial condition.

Most of our sales involve long-term contracts, which generally require a notice period prior to their scheduled expiration if a client chooses not to renew. Some of these contracts may also allow for early termination upon the occurrence of certain events such as a change in control. While a vast majority of our contracts remain in effect through their scheduled expiration, we may face pricing pressure in obtaining and retaining our larger clients. Some of our competitors may offer more attractive fees to our current and prospective clients, or other services that we do not offer. Larger clients may be able to seek lower prices from us when they renew a contract, when a contract is extended, or when the client's business has significant volume changes. They may also reduce services if they decide to move services in-house. Further, our SMB clients may exert pricing pressure due to pricing competition or other economic needs or pressures such clients experience from their customers. On some occasions, this pricing pressure results in lower revenue from a client than we had anticipated based on our previous agreement with that client. This reduction in revenue could result in an adverse effect on our business, operating results, and financial condition.

For potential clients of our business segments, switching from one vendor of core processing or related software and services (or from an internally-developed system) to a new vendor is a significant undertaking. As a result, potential clients often resist change. We seek to overcome this resistance through strategies such as making investments to enhance the functionality of our software. However, there can be no assurance that our strategies for overcoming potential clients' reluctance to change vendors will be successful, and this resistance may adversely affect our growth.

Security breaches or attacks on our systems may have a significant effect on our business.

In order to provide our services, we process, store, and transmit sensitive business information and personal consumer information, including, but not limited to, names, bankcard numbers, home or business addresses. Social Security numbers, driver's license numbers, and bank account numbers. Under the card network rules and various federal and state laws, we are responsible for information provided to us by merchants, ISOs, third-party service providers, and other agents. The confidentiality of such sensitive business information and personal consumer information that resides on our systems is critical to our business because we require such information to approve merchant accounts, process transactions, and protect against fraud. We cannot be certain that the security measures and procedures we have in place to protect this sensitive data will be successful or sufficient to counter all current and emerging technology threats designed to breach our systems in order to gain access to confidential information. The increasing sophistication of cyber criminals may increase the risk of a security breach of our systems. A breach of our products or systems processing or storing sensitive business information or personal consumer information could lead to claims against us, reputational damage, loss of our financial institution sponsorship, loss of clients' and their customers' confidence, as well as imposition of fines and damages, or potential restrictions imposed by card networks on our ability to process transactions, all of which could have a material adverse effect on our revenues, profitability, financial condition, and future growth. In addition, as security threats continue to evolve we may be required to invest additional resources to modify the security of our systems, which could have a material adverse effect on our results of operations.

We may experience breakdowns in our processing systems that could damage client relations and expose us to liability.

Our core business depends heavily on the reliability of our processing systems. A system outage could have a material adverse effect on our business, financial condition, and results of operations. Not only would we suffer damage to our reputation in the event of a system outage, but we may also be liable to third parties. Many of our contractual agreements with financial institutions require us to pay penalties if our systems do not meet certain operating standards. To successfully operate our business, we must be able to protect our processing and other systems from interruption, including from events that may be beyond our control. Events that could cause system interruptions include, but are not limited to, fire, natural disaster, unauthorized entry, power loss, telecommunications failure, computer viruses, terrorist acts, and war. Although we have taken steps to protect against data loss and system failures, there is still risk that we may lose critical data or experience system failures. To help protect against these events, we perform the vast majority of disaster recovery operations ourselves, but we also utilize select third parties for certain operations, particularly outside of the United States. To the extent we outsource our disaster recovery, we are at risk of the vendor's unresponsiveness or other failures in the event of breakdowns in our systems. In addition, our property and business interruption insurance may not be adequate to compensate us for all losses or failures that may occur.

We may experience software defects, computer viruses, and development delays, which could damage client relations, our potential profitability and expose us to liability.

Our products are based on sophisticated software and computing systems that often encounter development delays, and the underlying software may contain undetected errors, viruses, or defects. Defects in our software products and errors or delays in our processing of electronic transactions could result in additional development costs, diversion of technical and other resources from our other development efforts, loss of credibility with current or potential clients, harm to our reputation, fines imposed by card networks, or exposure to liability claims. In addition, we rely on technologies supplied to us by third parties that may also contain undetected errors, viruses or defects that could have a material adverse effect on our business, financial condition and results of operations. Although we attempt to limit our potential liability for warranty claims through disclaimers in our software documentation and limitation-of-liability provisions in our license and other agreements with our clients, we cannot assure that these measures will be successful in limiting our liability.

Our merchants may be unable to satisfy obligations for which we may also be liable.

We are subject to the risk of our merchants being unable to satisfy obligations for which we may also be liable. For example, we and our merchants acquiring alliances may be subject to contingent liability for transactions originally acquired by us that are disputed by the cardholder and charged back to the merchants. If we or the alliance is unable to collect this amount from the merchant because of the merchant's insolvency or other reasons, we or the alliance will bear the loss for the amount of the refund paid to the cardholder. We have an active program to manage our credit risk and often mitigate our risk by obtaining collateral. It is possible, however, that a default on such obligations by one or more of our merchants could have a material adverse effect on our business.

Fraud by merchants or others could have a material adverse effect on our business, financial condition, and results of operations.

We may be subject to potential liability for fraudulent electronic payment transactions or credits initiated by merchants or others. Examples of merchant fraud include when a merchant or other party knowingly uses a stolen or counterfeit credit, debit or prepaid card, card number, or other credentials to record a false sales transaction, processes an invalid card, or intentionally fails to deliver the merchandise or services sold in an otherwise valid transaction. Criminals are using increasingly sophisticated methods to engage in illegal activities such as counterfeiting and fraud. It is possible that incidents of fraud could increase in the future. Failure to effectively manage risk and prevent fraud would increase our chargeback liability or other liability. Increases in chargebacks or other liability could have a material adverse effect on our business, financial condition, and results of operations.

Future consolidation of financial institution clients or other client groups may adversely affect our financial condition.

In recent years, we have been negatively affected by the substantial consolidation in the bank industry. Bank industry consolidation affects existing and potential clients in our service areas. Our alliance strategy could also be negatively affected by consolidations, especially where the banks involved are committed to their internal merchant processing businesses that compete with us. Bank consolidation has led to an increasingly concentrated client base, resulting in a changing client mix as well as increased price compression. Further consolidation in the bank industry or other client base could have a negative impact on us, including a loss of revenue and price compression.

We rely on various financial institutions to provide clearing services in connection with our settlement activities. If we are unable to maintain clearing services with these financial institutions and are unable to find a replacement, our business may be adversely affected.

We rely on various financial institutions to provide clearing services in connection with our settlement activities. If such financial institutions should stop providing clearing services we must find other financial institutions to provide those services. If we are unable to find a replacement financial institution we may no longer be able to provide processing services to certain clients, which could negatively impact our revenue and earnings.

Because we rely on third-party vendors to provide products and services, we could be adversely impacted if they fail to fulfill their obligations.

Our business is dependent on third-party vendors to provide us with certain products and services. The failure of these vendors to perform their obligations in a timely manner could adversely affect our operations and profitability. In addition, if we are unable to renew our existing contracts with our most significant vendors, we might not be able to replace the related product or service at the same cost, which would negatively impact our profitability.

Changes in card association and debit network fees or products could increase costs or otherwise limit our operations.

From time to time, card associations and debit networks increase the organization and/or processing fees (known as interchange fees) that they charge. It is possible that competitive pressures will result in us absorbing a portion of such increases in the future, which would increase our operating costs, reduce our profit margin, and adversely affect our business, operating results, and financial condition. In addition, the various card associations and networks prescribe certain capital requirements. Any increase in the capital level required would further limit our use of capital for other purposes.

Our business may be adversely affected by geopolitical and other risks associated with operations outside of the United States and, as we continue to expand internationally, we may incur higher than anticipated costs and may become more susceptible to these risks.

We offer merchant acquiring, processing and issuing services outside of the United States, including in the United Kingdom, Germany, Argentina, Greece, India, and Australia, where our principal non-U.S. operations are located. Our revenues derived from these and other non-U.S. operations are subject to additional risks, including those resulting from social and geopolitical instability and unfavorable political or diplomatic developments, all of which could negatively impact our financial results.

As we expand internationally and grow our non-U.S. client base, we may face challenges due to the presence of more established competitors and our lack of experience in such non-U.S. markets, and we may also incur higher than anticipated costs. For example, we expanded our presence in Brazil in the third quarter of 2014 by launching our acquiring solution developed specifically for Brazil. If we are unable to successfully manage expenses relating to the international expansion of our business, our financial position and results of operations could be negatively impacted.

Cost savings initiatives may not produce the savings expected and may negatively impact our other initiatives and efforts to grow our business.

In recent years, we have implemented certain measures aimed at improving our profitability and maintaining flexibility in our capital resources, including restructuring efforts to align the business with our strategic objectives and the introduction of cost savings initiatives. For example, in the fourth quarter of 2014, we began an off-shoring initiative to employ lower cost off-shore resources. We have forecasted cost savings from these initiatives based on a number of assumptions and expectations which, if achieved, would improve our profitability and cash flows from operating activities. However, there can be no assurance the expected results will be achieved. In addition, these and any future spending reductions, if any, may negatively impact our other initiatives or our efforts to grow our business, which may negatively impact our future results of operations and increase the burden on existing management, systems, and resources.

The ability to recruit, retain and develop qualified personnel is critical to our success and growth.

All of our businesses function at the intersection of rapidly changing technological, social, economic, and regulatory developments that requires a wide range of expertise and intellectual capital. For us to successfully compete and grow, we must retain, recruit, and develop the necessary personnel who can provide the needed expertise across the entire spectrum of our intellectual capital needs. In addition, we must develop our personnel to provide succession plans capable of maintaining continuity in our business. The market for qualified personnel, however, is competitive and we may not succeed in recruiting additional personnel or may fail to effectively replace current personnel who depart with qualified or effective successors. Our effort to retain and develop personnel may also result in significant additional expenses, which could adversely affect our profitability. We cannot assure that key personnel, including executive officers, will continue to be employed or that we will be able to attract and retain qualified personnel in the future. Failure to retain or attract key personnel could have a material adverse effect on us.

Acquisitions and integrating such acquisitions create certain risks and may affect our operating results.

We have actively acquired businesses and may continue to make acquisitions of businesses or assets in the future. The acquisition and integration of businesses or assets involves a number of risks. The core risks are valuation (negotiating a fair price for the business), integration (managing the process of integrating the acquired company's people, products, technology, and other assets to extract the value and synergies projected to be realized in connection with the acquisition), regulation (obtaining necessary regulatory or other government approvals that may be necessary to complete acquisitions), and diligence (identifying undisclosed or unknown liabilities or restrictions that will be assumed in the acquisition).

In addition, acquisitions outside of the United States often involve additional or increased risks including, for example:

- managing geographically separated organizations, systems and facilities;
- integrating personnel with diverse business backgrounds and organizational cultures;
- complying with non-U.S. regulatory requirements;
- fluctuations in currency exchange rates;
- enforcement of intellectual property rights in some non-U.S. countries;
- difficulty entering new non-U.S. markets due to, among other things, consumer acceptance and business knowledge of these new markets; and
- general economic and political conditions.

The process of integrating operations could cause an interruption of, or loss of momentum in, the activities of one or more of our combined businesses and the possible loss of key personnel. The diversion of management's attention and any delays or difficulties encountered in connection with acquisitions and the integration of the two companies' operations could have an adverse effect on our business, results of operations, financial condition or prospects.

Financial Risks

Our substantial leverage could adversely affect our ability to raise additional capital to fund our operations, limit our ability to react to changes in the economy or our industry, expose us to interest rate risk to the extent of our variable rate debt and prevent us from meeting our debt obligations.

We are highly leveraged. As of December 31, 2015, we had $19.6 billion of total debt. Our high degree of leverage could have important consequences, including:

- increasing our vulnerability to adverse economic, industry or competitive developments;
- requiring a substantial portion of cash flow from operations to be dedicated to the payment of principal and interest on our indebtedness, therefore reducing our ability to use cash flow to fund our operations, capital expenditures, and future business opportunities;
- making it more difficult for us to satisfy our obligations with respect to our indebtedness, and any failure to comply with the obligations of our debt instruments, including restrictive covenants and borrowing conditions, could result in an event of default under the agreements governing such indebtedness;
- restricting us from making strategic acquisitions or causing us to make non-strategic divestitures;
- making it more difficult for us to obtain network sponsorship and clearing services from financial institutions or to obtain or retain other business with financial institutions;
- limiting our ability to obtain additional financing for working capital, capital expenditures, product development, debt service requirements, acquisitions, and general corporate or other purposes; and
- limiting our flexibility in planning for, or reacting to, changes in our business or market conditions and placing us at a competitive disadvantage compared to our competitors who are less highly leveraged and who, therefore, may be able to take advantage of opportunities that our leverage prevents us from exploiting.

Our financial condition and results of operations are dependent in part upon our ongoing ability to refinance our maturing indebtedness at attractive interest rates.

Successful execution of our business strategy is dependent in part upon our ability to manage our capital structure to reduce interest expense and enhance free cash flow generation. Our senior secured revolving credit facility has $1.25 billion in commitments that are scheduled to mature in June 2020. In addition, approximately $8.3 billion of obligations under our existing long term borrowings are scheduled to mature prior to December 31, 2020. We may not be able to refinance our senior secured credit facilities or our other existing indebtedness at or prior to their maturity at attractive rates of interest because of our high levels of debt, debt incurrence restrictions under our debt agreements or because of adverse conditions in credit markets generally.

An increase in interest rates may negatively impact our operating results and financial condition.

Certain of our borrowings, including borrowings under our senior secured credit facilities to the extent the interest rate is not fixed by an interest rate swap, are at variable rates of interest. An increase in interest rates would have a negative impact on our results of operations by causing an increase in interest expense.

As of December 31, 2015, we had $9.6 billion aggregate principal amount of variable rate long-term indebtedness, of which interest rate swaps fix the interest rate on $5.0 billion in notional amount. As a result, as of December 31, 2015, the impact of a

100 basis point increase in interest rates would increase our annual interest expense by approximately $46 million. See the discussion of our interest rate swap transactions in note 13 "Derivative Financial Instruments" to our consolidated financial statements in Part II, Item 8 of this Form 10-K.

Our debt agreements contain restrictions that limit our flexibility in operating our business.

The agreements governing our indebtedness contain various covenants that limit our ability to engage in specified types of transactions. These covenants limit our and certain of our subsidiaries' ability to, among other things:

- incur additional indebtedness or issue certain preferred shares;
- pay dividends on, repurchase, or make distributions in respect of, our capital stock or make other restricted payments;
- make certain investments;
- sell certain assets;
- create liens;
- consolidate, merge, sell, or otherwise dispose of all or substantially all of our assets; and
- enter into certain transactions with our affiliates.

A breach of any of these covenants could result in a default under one or more of these agreements, including as a result of cross-default provisions and, in the case of our senior secured revolving credit facility, permit the lenders to cease making loans to us. Upon the occurrence of an event of default under these agreements, the holders of our debt could elect to declare all amounts outstanding thereunder to be immediately due and payable and, in the case of our senior secured revolving credit facility, terminate all commitments to extend further credit. Such actions by these holders could cause cross-defaults under our other indebtedness. If we were unable to repay those amounts, the lenders under our senior secured credit facilities or holders of our senior secured notes could proceed against the collateral securing such debt. We have pledged a significant portion of our assets as collateral under our senior secured credit facilities and our senior secured notes. If the holders of our debt accelerate the repayment of borrowings, we may not have sufficient assets to repay our senior secured credit facilities or any other debt that may become due as a result of that acceleration and we could experience a material adverse effect on our financial condition and results of operations.

Our consolidated balance sheet includes significant amounts of goodwill and intangible assets. The impairment of a significant portion of these assets would negatively affect our financial condition and results of operations.

Our consolidated balance sheet includes goodwill and intangible assets that represent approximately 60% of our total assets at December 31, 2015. These assets consist primarily of goodwill and client relationship intangible assets associated with our acquisitions. We also expect to engage in additional acquisitions, which may result in our recognition of additional goodwill and intangible assets. Under current accounting standards, we are required to amortize certain intangible assets over the useful life of the asset, while goodwill and certain other intangible assets are not amortized. On a regular basis we assess whether there have been impairments in the carrying value of goodwill and certain intangible assets. If the carrying value of the asset is determined to be impaired, then it is written down to fair value by a charge to operating earnings. An impairment of a significant portion of goodwill or intangible assets could have a material adverse effect on our financial condition and results of operations.

Our results of operations may be adversely affected by changes in foreign currency exchange rates.

We are subject to risks related to the changes in currency rates as a result of our investments in non-U.S. operations and from revenues generated in currencies other than the U.S. dollar. Revenue and profit generated by such non-U.S. operations will increase or decrease compared to prior periods as a result of changes in foreign currency exchange rates. From time to time, we utilize foreign currency forward contracts or other derivative instruments to mitigate the cash flow or market value risks associated with foreign currency-denominated transactions. These hedge contracts may not, however, eliminate all of the risks related to foreign
currency translation. In addition, we may become subject to exchange control regulations that restrict or prohibit the conversion of our other revenue currencies into U.S. dollars. Any of these factors could decrease the value of revenues and earnings we derive from our non-U.S. operations and have a material adverse impact on our business.

Unfavorable resolution of tax contingencies could adversely affect our results of operations and cash flows from operations.

Our tax returns and positions are subject to review and audit by federal, state, local, and international taxing authorities. An unfavorable outcome to a tax audit could result in higher tax expense, thereby negatively impacting our results of operations as well as our cash flows from operations. We have established contingency reserves for material, known tax exposures relating to deductions, transactions, and other matters involving some uncertainty as to the proper tax treatment of the item. These reserves reflect what we believe to be reasonable assumptions as to the likely final resolution of each issue if raised by a taxing authority. While we believe that the reserves are adequate to cover reasonably expected tax risks, there is no assurance that, in all instances,

an issue raised by a tax authority will be finally resolved at a financial cost not in excess of any related reserve. An unfavorable resolution, therefore, could negatively impact our effective tax rate, financial position, results of operations, and cash flows in the current and/or future periods. Refer to note 8 "Income Taxes" to our consolidated financial statements included in Part II, Item 8 of this Form 10-K for more information.

Regulatory and Legal Risks

Failure to comply with, or changes in, laws, regulations and enforcement activities may adversely affect the products, services, and markets in which we operate.

We and our clients are subject to laws and regulations that affect the electronic payments industry in the many countries in which our services are used. In particular, our clients are subject to numerous laws and regulations applicable to banks, financial institutions, and card issuers in the United States and abroad, and, consequently, we are at times affected by these federal, state, and local laws and regulations. The United States government has increased its scrutiny of a number of credit card practices, from which some of our clients derive significant revenue. Regulation of the payments industry, including regulations applicable to us and our clients, has increased significantly in recent years. Failure to comply with laws and regulations applicable to our business may result in the suspension or revocation of licenses or registrations, the limitation, suspension or termination of services, and/or the imposition of consent orders or civil and criminal penalties, including fines which could have an adverse effect on our results of operation and financial condition.

We are subject to U.S. and international financial services regulations, a myriad of consumer protection laws, economic sanctions, laws and regulations, and anti-corruption laws, escheat regulations and privacy and information security regulations to name only a few. Changes to legal rules and regulations, or interpretation or enforcement of them, could have a negative financial effect on us. In particular, the Dodd-Frank Act significantly changed the United States financial regulatory system by, among other things, creating the CFPB to regulate consumer financial products and services (including many offered by our clients), restrict debit card fees paid by merchants to issuer banks and allow merchants to offer discounts for different payment methods. CFPB rules, examinations, and enforcement actions may require us to adjust our activities and may increase our compliance costs. Changing regulations or standards in the area of privacy and data protection could also adversely impact us. In addition, certain of our alliance partners are subject to regulation by federal and state authority and, as a result, could pass through some of those compliance obligations to us.

Failure to comply with the U.S. Foreign Corrupt Practices Act, anti-money laundering, economic and trade sanctions regulations, and similar laws could subject us to penalties and other adverse consequences.

We operate our business around the world, including in certain foreign countries with developing economies, where companies often engage in business practices that are prohibited by U.S. and U.K. regulations, including the FCPA and the U.K. Bribery Act. Such laws prohibit improper payments or offers of payments to foreign governments and their officials and political parties by the U.S. and other business entities for the purpose of obtaining or retaining business. We have implemented policies to discourage such practices; however, there can be no assurance that all of our employees, consultants, and agents, including those that may be based in or from countries where practices that violate U.S. laws may be customary, will not take actions in violation of our policies, for which we may be ultimately responsible.

In addition, we are subject to anti-money laundering laws and regulations, including the BSA. Among other things, the BSA requires money services businesses (such as money transmitters and providers of prepaid access) to develop and implement risk-based anti-money laundering programs, report large cash transactions and suspicious activity, and maintain transaction records. Our subsidiary Money Network Financial LLC provides prepaid access for various open loop prepaid programs for which it is the program manager and therefore must meet the requirements of the Financial Crimes Enforcement Network, the agency that enforces the BSA.

We are also subject to certain economic and trade sanctions programs that are administered by the OFAC which prohibit or restrict transactions to or from or dealings with specified countries, their governments, and in certain circumstances, their nationals, and with individuals and entities that are specially-designated nationals of those countries, narcotics traffickers, and terrorists or terrorist organizations.

Similar anti-money laundering and counter terrorist financing and proceeds of crime laws apply to movements of currency and payments through electronic transactions and to dealings with persons specified in lists maintained by the country equivalents to OFAC lists in several other countries and require specific data retention obligations to be observed by intermediaries in the payment process. Our businesses in those jurisdictions are subject to those data retention obligations.

Failure to comply with any of these laws and regulations or changes in this regulatory environment, including changing interpretations and the implementation of new or varying regulatory requirements by the government, may result in significant financial penalties, reputational harm, or change the manner in which we currently conduct some aspects of our business, which could significantly affect our results of operations or financial condition.

Changes in credit card association or other network rules or standards could adversely affect our business.

In order to provide our transaction processing services, several of our subsidiaries are registered with Visa and MasterCard and other networks as members or service providers for member institutions. As such, we and many of our clients are subject to card association and network rules that could subject us or our clients to a variety of fines or penalties that may be levied by the card associations or networks for certain acts or omissions by us, acquiring clients, processing clients, and merchants. Visa, MasterCard, and other networks, some of which are our competitors, set the rules and standards with which we must comply. The termination of our member registration or our status as a certified service provider, or any changes in card association or other network rules or standards, including interpretation and implementation of the rules or standards, that increase the cost of doing business or limit our ability to provide transaction processing services to or through our clients, could have an adverse effect on our business, results of operations, and financial condition.

Failure to protect our intellectual property rights and defend ourselves from potential patent infringement claims may diminish our competitive advantages or restrict us from delivering our services.

Our trademarks, patents, and other intellectual property are important to our future success. The *First Data* trademark and trade name and the *STAR* trademark and trade name are intellectual property rights which are individually material to us. These trademarks and trade names are widely recognized and associated with quality and reliable service. Loss of the proprietary use of the *First Data* or *STAR* trademarks and trade names or a diminution in the perceived quality associated with them could harm the growth of our businesses. We also rely on proprietary technology. It is possible that others will independently develop the same or similar technology. Further, we use open source architecture in connection with our solutions, in particular our *Clover* open architecture platform. Companies that incorporate open source platforms into their solutions have, from time to time, faced claims challenging the ownership of such platforms. As a result, we could be subject to suits by parties claiming ownership of what we believe to be open source software. We cannot guarantee that we can protect our trade secrets, know-how, or other proprietary information. Our patents could be challenged, invalidated or circumvented by others, and may not be of sufficient scope or strength to provide us with any meaningful protection or advantage. If we are unable to maintain the proprietary nature of our technologies, we could lose competitive advantages and be materially adversely affected. Additionally, the laws of certain non-U.S. countries where we do business or contemplate doing business in the future may not recognize intellectual property rights or protect them to the same extent as do the laws of the United States. Adverse determinations in judicial or administrative proceedings could prevent us from selling our services or prevent us from preventing others from selling competing services, and thereby may have a material adverse effect on the business and results of operations. Additionally, claims have been made, are currently pending, and other claims may be made in the future, with regard to our technology allegedly infringing on a patent or other intellectual property rights. Unfavorable resolution of these claims could either result in us being restricted from delivering the related product or service or result in a settlement that could be materially adverse to us.

Failure to comply with state and federal antitrust requirements could adversely affect our business.

Through our merchant alliances, we hold an ownership interest in several competing merchant acquiring businesses while serving as an electronic processor for those businesses. In order to satisfy state and federal antitrust requirements, we actively maintain an antitrust compliance program. Notwithstanding our compliance program, it is possible that perceived or actual violations of state or federal antitrust requirements could give rise to regulatory enforcement investigations or actions. Regulatory scrutiny of, or regulatory enforcement action in connection with, compliance with state and federal antitrust requirements could have a material adverse effect on our reputation and business.

We are the subject of various legal proceedings which could have a material adverse effect on our revenue and profitability.

We are involved in various litigation matters. We are also involved in or are the subject of governmental or regulatory agency inquiries or investigations and make voluntary self-disclosures to government or regulatory agencies from time to time. Our insurance or indemnities may not cover all claims that may be asserted against us, and any claims asserted against us, regardless of merit or eventual outcome, may harm our reputation. If we are unsuccessful in our defense in these litigation matters, or any other legal proceeding, we may be forced to pay damages or fines, enter into consent decrees, and/or change our business practices, any of which could have a material adverse effect on our revenue and profitability.

Our ability to utilize net operating loss carryforwards could be limited if we were to experience an ownership change as defined in the Internal Revenue Code.

Section 382 of the Internal Revenue Code of 1986, as amended (Code), contains rules that impose an annual limitation on the ability of a company with net operating loss carryforwards that undergoes an ownership change, which is generally any change in ownership of more than 50% of its stock (by value) over a three-year period, to utilize its net operating loss carryforwards in years after the ownership change. These rules generally operate by focusing on ownership changes among holders owning directly or indirectly 5% or more of the shares of stock of a company or any change in ownership arising from a new issuance of shares of stock by such company. If a company's income in any year is less than the annual limitation prescribed by Section 382 of the Code, the unused portion of such limitation amount may be carried forward to increase the limitation (and net operating loss carryforward utilization) in subsequent tax years.

Our initial public offering did not result in an ownership change for purposes of Section 382 of the Code. If, however, we were to undergo an ownership change as a result of future transactions involving our common stock, including a follow-on offering of our common stock or purchases or sales of common stock between 5% holders, our ability to use our net operating loss carryforwards would be subject to the limitations of Section 382 of the Code. As a result, a portion of our net operating loss carryforwards may expire before we would be able to use them. If we are unable to utilize our net operating loss carryforwards, there may be a negative impact on our financial position and results of operations.

In addition to the aforementioned federal income tax implications pursuant to Section 382 of the Code, most states follow the general provisions of Section 382 of the Code, either explicitly or implicitly resulting in separate state net operating loss limitations.

Risks Related to Ownership of Our Class A Common Stock

Failure to maintain effective internal controls in accordance with Section 404 of the Sarbanes-Oxley Act could have a material adverse effect on our business and stock price.

Section 404 of the Sarbanes-Oxley Act requires us to evaluate annually the effectiveness of our internal control over financial reporting as of the end of each fiscal year and to include a management report assessing the effectiveness of our internal control over financial reporting in our annual report. If we fail to maintain the adequacy of our internal controls, we may not be able to ensure that we can conclude on an ongoing basis that we have effective internal control over financial reporting in accordance with Section 404 of the Sarbanes-Oxley Act.

KKR controls us and its interests may conflict with ours or yours in the future.

KKR holds a majority of the combined voting power of our common stock. As a result, KKR has the ability to elect all of the members of our Board and thereby control our policies and operations, including the appointment of management, future issuances of our Class A common stock or other securities, the payment of dividends, if any, on our Class A common stock, the incurrence of debt by us, amendments to our amended and restated certificate of incorporation and amended and restated bylaws, and the entering into of extraordinary transactions and the interests of KKR may not in all cases be aligned with your interests.

In addition, KKR may have an interest in pursuing acquisitions, divestitures and other transactions that, in its judgment, could enhance its investment, even though such transactions might involve risks to you. For example, KKR could cause us to make acquisitions that increase our indebtedness or cause us to sell revenue-generating assets. KKR is in the business of making investments in companies and may from time to time acquire and hold interests in businesses that compete directly or indirectly with us. Our amended and restated certificate of incorporation will provide that none of KKR or any director who is not employed by us (including any nonemployee director who serves as one of our officers in both his or her director and officer capacities) or his or her affiliates will have any duty to refrain from engaging, directly or indirectly, in the same business activities or similar business activities or lines of business in which we operate. KKR also may pursue acquisition opportunities that may be complementary to our business, and, as a result, those acquisition opportunities may not be available to us.

So long as KKR continues to beneficially own a sufficient number of shares of Class B common stock, even if it beneficially owns significantly less than 50% of the shares of our outstanding common stock, it will continue to be able to effectively control our decisions. For example, if our Class B common stock amounted to 15% of our outstanding common stock, beneficial owners of our Class B common stock (including KKR), would collectively control 64% of the voting power of our common stock. The shares of our Class B common stock beneficially owned by KKR may be transferred to an unrelated third party if the holders of a majority of the shares of Class B common stock have consented to such transfer in writing in advance.

In addition, KKR will be able to determine the outcome of all matters requiring stockholder approval and will be able to cause or prevent a change of control of our Company or a change in the composition of our Board and could preclude any acquisition of our Company. This concentration of voting control could deprive you of an opportunity to receive a premium for your shares of Class A common stock as part of a sale of our Company and ultimately might affect the market price of our Class A common stock.

ITEM 1B. UNRESOLVED STAFF COMMENTS

None.

ITEM 2. PROPERTIES

As of December 31, 2015, we and our subsidiaries owned or leased 66 domestic properties and 90 international properties. These facilities are used for operational, sales and administrative purposes, and are substantially all currently being utilized.

	Leased Facilities		Owned Facilities	
	No.	Sq. Ft.	No.	Sq. Ft.
Facilities in the United States	52	2,016,597	14	2,037,362
International Facilities	80	926,872	10	410,011

Global Business Solutions' principal operations are conducted in New York, New York; Coral Springs, Florida; Hagerstown, Maryland; London, United Kingdom; São Paulo, Brazil; and Atlanta, Georgia. Global Financial Solutions' principal operations are located in Omaha, Nebraska; Chesapeake, Virginia; and Wilmington, Delaware. Network & Security Solutions' principal operations are located in Atlanta, Georgia; Omaha, Nebraska; Sugar Land, Texas; and Greenwood Village, Colorado. Our Corporate facilities include New York, New York; Atlanta, Georgia; and Greenwood Village, Colorado.

We believe that our facilities are suitable and adequate for our current business; however, we periodically review our space requirements and may acquire new space to meet the needs of our businesses or consolidate and dispose of or sublet facilities which are no longer required.

ITEM 3. LEGAL PROCEEDINGS

From time to time, we are involved in various litigation matters arising in the ordinary course of our business. None of these matters, individually or in the aggregate, currently is material to us.

ITEM 4. MINE SAFETY DISCLOSURES

Not applicable.

PART II

ITEM 5. MARKET FOR REGISTRANT'S COMMON EQUITY, RELATED STOCKHOLDER MATTERS AND ISSUER PURCHASES OF EQUITY SECURITIES

Our Class A common stock has traded on the New York Stock Exchange under the symbol "FDC" since October 15, 2015. Prior to that date, there was no public trading market for our common stock.

Price Range of Class A common stock

The information presented in the table below represents the high and low closing sales prices per share of Class A common stock as reported on the NYSE for the periods indicated. There is currently no established public trading market for our Class B common stock.

2015	High	Low
Fourth quarter (beginning October 15, 2015)	$ 17.80	$ 15.36

There were 16 holders of record of our Class A common stock and 226 holders of record of our Class B common stock as of January 31, 2016. The number of beneficial owners of our Class A common stock is substantially greater than the number of record holders, because a large portion of our Class A common stock is held in "street name" by banks and brokers.

Dividend Policy

In 2015, we paid three dividends totaling $4 million to First Data Holdings Inc., our direct parent prior to the IPO. In 2014, we paid five dividends totaling $686 million to FDH. We do not currently anticipate declaring or paying any cash dividends on our common stock. Because a significant portion of our operations is through our subsidiaries, our ability to pay dividends depends in part on our receipt of cash dividends from our operating subsidiaries, which may further restrict our ability to pay dividends as a result of the laws of their jurisdiction of organization, agreements of our subsidiaries or covenants under any existing and future outstanding indebtedness we or our subsidiaries incur. In addition, the senior secured revolving credit facility, senior secured term loan facility, and the indentures governing the senior notes limit our ability to pay dividends. See "Management's Discussion and Analysis of Financial Condition and Results of Operations - Capital Resources and Liquidity" included in Part II, Item 7 and note 5 "Stockholders' Equity and Redeemable Noncontrolling Interest" to our consolidated financial statements in Part II, Item 8 of this Form 10-K.

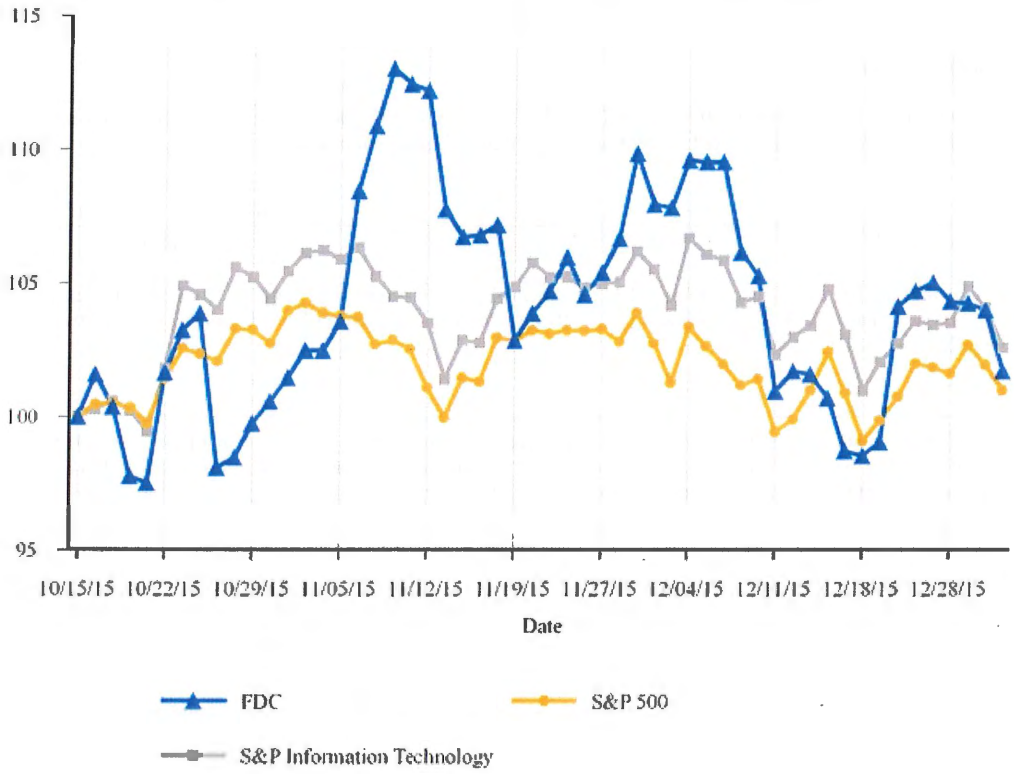
Use of Proceeds

On October 14, 2015, our registration statement on Form S-1 (File No. 333-205750) was declared effective by the Securities and Exchange Commission (SEC) for our initial public offering pursuant to which we sold an aggregate of 176,076,869 shares of our Class A common stock at a price to the public of $16.00 per share. There has been no material change in the planned use of proceeds from our initial public offering as described in our final prospectus filed with the SEC on October 14, 2015 pursuant to Rule 424(b).

Stock Performance Graph

The following graph shows a comparison from October 15, 2015 (the date our Class A common stock commenced trading on the NYSE) through December 31, 2015 of the cumulative total return for our Class A common stock, the S&P 500 Index and the S&P Information Technology Index. Data for the S&P 500 Index and the S&P Information Technology Index assume reinvestment of dividends. Note that historic stock price performance is not necessarily indicative of future stock price performance.

COMPARISON OF CUMULATIVE TOTAL RETURN SINCE IPO
Among First Data Corporation, the S&P 500 Index, and the S&P Information Technology Index



This performance graph shall not be deemed "soliciting material" or to be "filed" with the Securities and Exchange Commission for purposes of Section 18 of the Securities Exchange Act of 1934, as amended, or otherwise subject to the liabilities under that Section, and shall not be deemed to be incorporated by reference into any filing of First Data Corporation under the Securities Act of 1933, as amended.

ITEM 6. SELECTED FINANCIAL DATA

The following table sets forth our selected consolidated financial data as of the dates and for the periods indicated. The selected financial data as of December 31, 2015 and 2014 and for the years ended December 31, 2015, 2014, and 2013 have been derived from our audited consolidated financial statements and related notes appearing in Part II, Item 8 of this Form 10-K. The selected consolidated financial data as of December 2013, 2012, and 2011 and for the years ended December 2012 and 2011 have been derived from our audited consolidated financial statements and related notes thereto not included in this Form 10-K.

The results of operations for any period are not necessarily indicative of the results to be expected for any future period. The selected consolidated financial data set forth below should be read in conjunction with, and are qualified by reference to "Management's Discussion and Analysis of Financial Condition and Results of Operations" and the consolidated financial statements and related notes thereto included in Part II, Item 8 of this Form 10-K.

The notes to our consolidated financial statements in Part II, Item 8 of this Form 10-K contain additional information about various acquisitions, dispositions, and certain charges and benefits resulting from other operating expenses, and other income (expense) which affect the comparability of information presented. Amounts below include acquisitions since the date acquired.

	December 31,				
(in millions, except shares and per share data)	**2015**	**2014**	**2013**	**2012**	**2011**
Statement of operations data (Year-end):					
Revenues	$ 11,451	$ 11,152	$ 10,809	$ 10,680	$ 10,714
Total revenues (excluding reimbursables)	7,764	7,548	7,302	7,318	7,182
Operating expenses (a)	10,228	9,701	9,629	9,578	9,728
Other operating expenses, net (b)	53	13	56	28	44
Total expenses (excluding reimbursables)	6,594	6,110	6,178	6,244	6,240
Interest expense, net	(1,537)	(1,728)	(1,856)	(1,887)	(1,825)
Net loss	(1,268)	(265)	(775)	(562)	(336)
Net loss attributable to First Data Corporation	(1,481)	(458)	(952)	(736)	(516)
Depreciation and amortization (c)	1,133	1,163	1,212	1,331	1,344
Net loss per share (e):					
Basic	(7.70)	(458,000)	(952,000)	(736,000)	(516,000)
Diluted	(7.70)	(458,000)	(952,000)	(736,000)	(516,000)
Weighted average common shares outstanding (e):					
Basic	192,263,793	1,000	1,000	1,000	1,000
Diluted	192,263,793	1,000	1,000	1,000	1,000
Balance sheet data (As of year-end):					
Total assets (f)	$ 34,362	$ 34,034	$ 34,962	$ 37,617	$ 39,911
Total current and long-term settlement assets	8,151	7,558	7,557	9,228	10,839
Total liabilities (f)	30,625	31,434	33,318	34,959	36,436
Settlement obligations	8,150	7,557	7,553	9,226	10,838
Long-term borrowings (f)	18,737	20,697	22,499	22,365	22,252
Other long-term liabilities (d) (f)	1,243	1,223	1,202	1,249	1,364
Redeemable noncontrolling interest	77	70	69	67	67
Total equity	3,660	2,530	1,575	2,591	3,408

(a) Operating expenses include Cost of services; Cost of products sold; Selling, general, and administrative; Reimbursable PIN debit fees, postage and other; and Depreciation and amortization.

(b) Other operating expenses, net includes restructuring, net; impairments; and litigation and regulatory settlements; as applicable to the periods presented.

(c) Includes amortization of initial payments for new contracts, which is recorded as a contra-revenue within "Transaction and processing service fees" and amortization related to equity method investments, which is netted within "Equity earnings in affiliates" in our consolidated statements of operations.

(d) Other long-term liabilities include Deferred tax liabilities.

(e) As a result of the HoldCo Merger, all outstanding shares of FDH were converted into Class B common stock, which are entitled to ten votes per share. All of FDC's outstanding common stock was eliminated upon the merger. We accounted for the HoldCo Merger as a transfer of assets between entities under common control and have reflected the transactions impact on net loss per share and weighted average shares on a prospective basis.

(f) Prior year amounts have been retrospectively adjusted to reflect adoption of new accounting guidance as discussed within note 1 "Summary of Significant Accounting Policies-New Accounting Guidance " to our consolidated financial statements in Part II, Item 8 of this Form 10-K

ITEM 7. MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

The following contains management's discussion and analysis of our financial condition and results of operations and should be read together with "Selected Financial Data," included in Part II, Item 6 of this Form 10-K and our consolidated financial statements and related notes thereto included in Part II, Item 8 of this Form 10-K. This discussion contains forward-looking statements and involves numerous risks and uncertainties. Our actual results may differ materially from those anticipated in any forward-looking statements as a result of many factors, including those set forth under "Forward-Looking Statements," "Risk Factors," and elsewhere in this Form 10-K.

Executive Overview

We sit at the center of global electronic commerce. We believe we offer our clients the most complete array of integrated solutions in the industry, covering their needs across next generation commerce technologies, merchant acquiring, issuing, and network solutions. We serve our clients in 118 countries, reaching approximately 6 million business locations over the course of a year and over 4,000 financial institutions. We believe we have the industry's largest distribution network, driven by our partnerships with many of the world's leading financial institutions, our direct sales force, and a network of distribution partners. We are the largest merchant acquirer, issuer processor, and independent network services provider in the world, enabling businesses to accept electronic payments, helping financial institutions issue credit, debit and prepaid cards, and routing secure transactions between them. In 2015, we processed 79 billion transactions globally, or over 2,500 per second, and processed 28% of the world's eCommerce volume. In our largest market, the United States, we acquired $1.7 trillion of payment volume, accounting for nearly 10% of U.S. GDP last year.

Our business is characterized by transaction related fees, multi-year contracts, and a diverse client base, which allows us to grow alongside our clients. Our multi-year contracts allow us to achieve a high level of recurring revenues with the same clients. While the contracts typically do not specify fixed revenues to be realized thereunder, they do provide a framework for revenues to be generated based on volume of services provided during such contract's term. Our business also generally requires minimal incremental capital expenditures and working capital to support additional revenue within our existing business lines.

Segment Discussion

We operate three reportable segments; Global Business Solutions (GBS), Global Financial Solutions (GFS), and Network & Security Solutions (NSS). Our segments are designed to establish global lines of businesses that support our global client base and allow us to further globalize our solutions while working seamlessly with our geographic teams across our regions: the United States and Canada (North America); Europe, Middle East, and Africa (EMEA); Latin America (LATAM); and Asia Pacific (APAC) and be supported by a corporate team focused on company wide issues.

In examining our performance, management places particular focus on our segment revenue and adjusted EBITDA by segment, as well as the operating metrics described in "Segment Results".

Global Business Solutions Our largest segment, Global Business Solutions, provides businesses of all sizes and types with a wide range of solutions at the point of sale, including merchant acquiring, eCommerce, mobile commerce, POS technology, and other business solutions. Over the course of a year, we serve approximately 3.3 million business locations in the United States and 2.3 million outside the United States. Our largest service in this segment is merchant acquiring, which facilitates the acceptance of commercial transactions at the point of sale, including retail transactions at physical business locations, mobile commerce transactions through mobile or tablet devices, or eCommerce transactions over the Internet. In 2015, we acquired $1.7 trillion of payment volume in the United States and $178 billion of payment volume outside the United States.

The Global Business Solutions segment generates approximately 78% of its revenues from clients in our North America region, 13% from clients in our EMEA region, 5% from clients in our APAC region, and 4% from clients in our LATAM region. The Global Business Solutions segment's revenues and earnings are impacted by the number of transactions, payment volume, the mix of credit cards, debit cards, stored value cards, and checks at the POS, and the size of the client. GBS generally experiences increased activity during the traditional holiday shopping period in the fourth quarter, the back-to-school buying period in the third quarter, and certain holidays.

Global Financial Solutions Our Global Financial Solutions segment provides financial institutions, which include bank and non-bank issuers such as retailers with proprietary card portfolios, with a broad range of solutions that enable them to offer financial products and solutions to their customers. Our Global Financial Solutions segment serves approximately 1,400 financial institutions globally and deliver value to clients through a variety of channels, including end-to-end outsourced processing, managed services,

and various software delivery models utilizing our proprietary *VisionPLUS* application. Our solutions include credit, retail, commercial card and loan processing, and related supporting services. In 2015, we processed 7.4 billion transactions on our platforms.

The Global Financial Solutions segment generates approximately 59% of its revenues from clients in our North America region, 29% from clients in our EMEA region, 7% from clients in our LATAM region, and 5% from clients in our APAC region. Within the United States, revenues are diversified across financial institutions of all sizes, which are spread across the country. The Global Financial Solutions segment's revenues and earnings are impacted by the number of consumer, commercial, and retail private label credit card accounts that are issued and actively in use. Revenue and profit growth comes primarily from increased card usage, issuance of new cards from growth in existing clients and sales to new clients, and the related account conversions.

Network & Security Solutions Our Network & Security Solutions segment provides a wide range of network services and security, risk and fraud management solutions to business and financial institution clients in our Global Business Solutions and Global Financial Solutions segments and independently to other financial institutions, businesses, governments, processors, and other clients. Our largest service in this segment is our *STAR Network*, which enables clients to encrypt, route, and decrypt various types of financial data, process debit and ATM transactions, and provide access to demand deposit accounts.

Our Network & Security Solutions segment is comprised of more than 99% domestic business and is divided into four product lines: EFT Network, Stored Value Network, Security and Fraud, and Other.

Components of Revenue

We generate revenue by providing commerce-enabling solutions. Set forth below is a description of our revenues by segment and factors impacting total revenues.

Global Business Solutions

Our Global Business Solutions segment revenues are primarily derived from processing credit and debit card transactions for business clients and also include fees for providing processing, loyalty and software services, and sales and leases of POS devices. Revenues are generated from a variety of sources:

- Discount fees, net of credit and PIN debit card interchange and assessment fees charged by the payment networks. The discount fee is typically either a percentage of the purchase amount or an interchange fee plus a fixed dollar amount;
- Processing fees charged to our alliances;
- Processing fees charged to merchant acquirers who have outsourced their transaction processing to us;
- Sales and leases of POS devices;
- Fees from providing reporting and other services; and
- Software fees such as security and *Clover* related fees

Global Business Solutions revenue is presented net of interchange fees and assessments but includes reimbursable PIN debit fees and other, which is also included as an expense.

A substantial portion of our business within the Global Business Solutions segment is conducted through merchant alliances between us and financial institutions. If we have majority ownership and management control over an alliance, then the alliance's financial statements are consolidated with ours and the related processing fees are treated as an intercompany transaction and eliminated upon consolidation. If we do not have a controlling ownership interest in an alliance, we use the equity method of accounting to account for our investment in the alliance. As a result, our consolidated revenues include certain processing fees charged to alliances accounted for under the equity method.

A large portion of GBS's revenue is derived from transaction and processing related services. This business is dependent on macroeconomic consumer trends and global economic conditions that affect the volume of consumer spending and the use of electronic payments and changes in these factors have in the past, impacted, and may in the future impact, our ability to grow this portion of the business. We have begun to implement recent initiatives, such as the introduction of several new products and expansion of our sales force, in an effort to grow this business versus prior periods.

Global Financial Solutions

Our Global Financial Solutions revenues are primarily derived from outsourced credit and retail card processing services, software solutions for clients to support in-house card processing, statement and letters printing, plastics personalization, and check

remittance processing provided to financial institutions. Revenues for Global Financial Solutions services are typically generated on the basis of number of active card accounts on file, number of statements/letters printed and mailed, number of plastics personalized, and licensing fees.

Network & Security Solutions

Our Network & Security Solutions revenues are primarily derived from network services such as Electronic Funds Transfer (EFT) Network Solutions, Stored Value Network Solutions, and Security and Fraud Management Solutions.

Recent Developments

New Products and Markets

Over the last few years, we launched new products to help our clients grow their businesses. For example:

- *Clover Station* - our tablet based integrated POS solution that simplifies the way SMBs operate.
- *Clover Mobile* - allows our clients to accept payments wherever their business takes them.
- *Clover Mini* - redefines the payment terminal. In addition to its sleek design, cloud-based software, elegant ease of use, and ability to accept most payment types (including swipe, PIN debit, EMV, and near-field communication (NFC) transactions), it provides access to the *Clover App Market* - designed to do for the small business owner what the smartphone did for the consumer. *Clover* has not yet had an opportunity to have a material impact on our financial performance to date, but we believe that *Clover* can play a significant role in our future growth.
- *Clover Go*, securely and reliably accepts both credit and debit cards – including EMV® chip cards –right from your personal smartphone or tablet.
- *Insightics* - an innovative cloud-based software that unlocks the power of big data behind payment transactions to give SMBs the ability to monitor key business metrics affecting their business, better understand customers to engage effectively, and derive more value from marketing and loyalty programs to grow revenue.
- *Perka* - a digital loyalty marketing platform, an alternative to traditional paper and plastic card-based incentive programs. With *Perka*, virtually any business can customize and launch a mobile loyalty program that works on all cell phones, creating customer loyalty and driving growth.
- *Gyft* - a leading digital platform that enables consumers to buy, send, manage, and redeem gift cards using mobile devices. *Gyft's* capabilities, combined with our long-standing experience in prepaid solutions, create a distinct combination in a rapidly growing market for virtual gift cards. Additionally, in October 2014 *Gyft* became the first gift card solution to enable consumers to buy virtual gift cards with Apple Pay's in-app payment functionality.
- *STAR Pinless* - Star Pinless allows merchants to except pinless debit transactions which enable digital commerce

We also recently announced a global alliance with a leading technology consultant to develop next generation payment technology software using our *VisionPLUS* platform.

In June 2015, we acquired TWI, a digital gift card distribution platform. TWI's cloud-based, digital gift card distribution platform supports comprehensive open and closed loop prepaid, store-branded gift card program management, offering end-to-end card management, and business to business and business to customer distribution solutions for retailers, distributors and resellers. TWI is reported as part of our Network & Security Solutions segment.

Factors and Trends Impacting Our Business and Results of Operations

We believe there are a number of factors that impact our business, results of operations and financial condition. In general, revenues across our Global Business Solutions, Global Financial Solutions and Network & Security Solutions segments are impacted by factors such as global economic and consumer spending trends, foreign exchange rates, geopolitical events, the pace of adoption of commerce-enablement and payment solutions, types and quantities of products and services provided to enterprises, timing and length of contract renewals, new enterprise wins, retention rates, mix of payment solution types employed by consumers, changes in interchange rates and size of enterprise served.

We also believe our results of operations could be impacted by changes to our expense structure as a result of capital structure modifications, operational efficiencies, investments in new products and solutions, advancements in technology, foreign exchange rates, geographic expansion, acquisitions and divestitures.

Factors Affecting the Comparability of Our Results of Operations

As a result of a number of factors, our historical results of operations are not comparable from period to period and may not be comparable to our financial results of operations in future periods. Key factors affecting the comparability of our results of operations are summarized below.

Currency Impact

A portion of our revenues and expenses are in foreign currencies. As a result, changes in foreign currencies against the U.S. dollar can impact our results of operations. Additionally, we have intercompany debts in foreign currencies, which impacts our results of operations. In recent periods, the U.S. dollar has appreciated significantly against most foreign currencies, which has negatively impacted our revenues generated in foreign currencies as presented in U.S. dollars in our consolidated financial statements. We have presented changes related to our segment results of operations on a constant currency basis in "-Operating revenues overview."

Interest Expense and Debt Extinguishment Costs

As a result of our 2014 and 2015 capital market activities, we have lowered the average interest rate of our outstanding debt from 7.4% at December 31, 2014 to 5.6% at December 31, 2015 and incurred $1.1 billion and $274 million in loss on debt extinguishment during 2015 and 2014, respectively.

Sale of Electronic Funds Source LLC

The sale of EFS in the second quarter of 2014 resulted in a pretax gain of $98 million and we no longer generate the revenues or EBITDA that were associated with the EFS business.

TeleCheck

The amount of revenue generated from our *TeleCheck* business continues to drop steadily. Our *TeleCheck* business involves the verification and guaranteeing of checks. The revenue generated by this business is decreasing with the general decline in the use of checks.

Share-Based Compensation Expense

Directly associated with our initial public offering, we have incurred approximately $254 million in share-based compensation expense during 2015 and expect to recognize approximately $70 million during the first quarter of 2016. See note 4 "Stock Compensation Plans" to our consolidated financial statements in Part II, Item 8 of this Form 10-K for additional information about our stock compensation plans. Furthermore, we will incur ongoing share-based compensation expense as employee awards are expensed over the requisite service period.

Management Fee Expenses

In connection with our initial public offering, our Management Agreement (as defined herein) with KKR was terminated and we incurred a $78 million expense associated with the termination. Going forward, we will not incur annual expenses related to this agreement.

Restructuring and Cost Management Initiatives

In connection with our announced cost management initiatives, we expect to incur $75 million of restructuring charges of which we incurred $53 million during 2015 primarily related to severance costs. We expect to achieve approximately $200 million in annualized gross savings by the middle of 2016 from such initiatives.

Results of Operations

Consolidated results should be read in conjunction with note 7 "Segment Information" to our consolidated financial statements in Part II, Item 8 of this Form 10-K, which provides more detailed discussions concerning certain components of our consolidated statements of operations. All significant intercompany accounts and transactions have been eliminated within the consolidated results.

Overview

Revenue for the year ended December 31, 2015 increased 3% to $11.5 billion from $11.2 billion in 2014 while operating profits decreased 19% to $1.2 billion from $1.4 billion in 2014. On a constant currency basis, revenue was up, driven by all segments. Foreign currency negatively impacted total revenue and operating profit by 2 percentage points.

Net loss attributable to First Data Corporation for the year ended December 31, 2015 increased to $1.5 billion from $458 million. The decline was primarily driven by a $794 million increase in debt extinguishment charges associated with the debt restructuring activity during the year, as well as one-time IPO-triggered expenses amounting to $332 million, comprising $254 million related to the vesting of certain previously granted equity based compensation and $78 million to terminate the KKR management fee.

Segment Results

We operate three reportable segments: GBS, GFS, and NSS. Our segments are designed to establish global lines of businesses that work seamlessly with our teams in our regions North America, EMEA, LATAM, and APAC. Our Corporate operations (as described below) are not discussed separately as any changes that had a significant impact on operating results are included in our consolidated results.

The business segment measurements provided to and evaluated by the chief operating decision maker are computed in accordance with the principles listed below.

- The accounting policies of the operating segments are the same as those described in the summary of significant accounting policies.
- Intersegment revenues are eliminated in the segment that sells directly to the end market.
- Segment revenue excludes reimbursable PIN debit fees, postage, and other revenue.
- Adjusted EBITDA by segment includes equity earnings in affiliates and excludes depreciation and amortization expense, net income attributable to noncontrolling interests, other operating expenses, and other income (expense). Additionally, adjusted EBITDA is adjusted for items similar to certain of those used in calculating our compliance with debt covenants. The additional items that are adjusted to determine adjusted EBITDA are:
    - share-based compensation and related expense is excluded;
    - debt issuance costs are excluded and represent costs associated with issuing debt and modifying our debt structure; and
    - KKR related items including annual sponsor and other fees for management, consulting, financial, contract termination, and other advisory services are excluded.
- For significant affiliates, segment revenue and adjusted EBITDA are reflected based on our proportionate share of the results of our investments in businesses accounted for under the equity method and consolidated subsidiaries with noncontrolling ownership interests. For other affiliates, we include equity earnings in affiliates, excluding amortization expense, in segment revenue and adjusted EBITDA. In addition, our Global Business Solutions segment measures reflect revenue-based commission payments to ISOs and sales channels, which are treated as an expense in the consolidated statements of operations, as contra revenue.
- Corporate operations include corporate-wide governance functions such as our executive management team, aviation, tax, treasury, internal audit, corporate strategy, and certain accounting, human resources and legal costs related to supporting the corporate function. Costs incurred by Corporate that are attributable to a segment are allocated to the respective segment.
- Certain measures exclude the estimated impact of foreign currency changes (constant currency). To present this information, monthly results during the periods presented for entities reporting in currencies other than U.S. dollars are translated into U.S. dollars at the average exchange rates in effect during the corresponding month of the prior fiscal year, rather than the actual average exchange rates in effect during the current fiscal year. Once translated, each month during the periods presented is added together to calculate the constant currency results for the periods presented.

Operating revenues overview

(in millions)	Year ended December 31, 2015	2014	2013	Percent Change 2015 vs. 2014	2014 vs. 2013	Constant Currency Percent Change 2015 vs. 2014	2014 vs. 2013
Revenues:							
Global Business Solutions	$ 4,089	$ 4,046	$ 3,938	1%	3%	4%	4%
Global Financial Solutions	1,495	1,489	1,384	—%	8%	6%	9%
Network & Security Solutions	1,464	1,369	1,362	7%	1%	7%	1%
Total segment revenue	7,048	6,904	6,684	2%	3%	5%	4%
Adjustments to reconcile to consolidated revenue:							
Adjustments for non wholly owned entities	74	57	39	30%	46%	35%	43%
Independent sales organizations (ISOs) commissions	642	587	579	9%	1%	12%	3%
Total revenues (excluding reimbursable items)	7,764	7,548	7,302	3%	3%	6%	5%
Reimbursable PIN debit fees, postage, and other	3,687	3,604	3,507	2%	3%	2%	3%
Total revenues	$ 11,451	$ 11,152	$ 10,809	3%	3%	5%	4%

Global Business Solutions Segment results

The following table displays total segment revenue by region and illustrates, on a percentage basis, the impact of foreign currency fluctuations on revenue growth.

(in millions)	Year ended December 31, 2015	2014	2013	Percent Change 2015 vs. 2014	2014 vs. 2013	Constant Currency Percent Change 2015 vs. 2014	2014 vs. 2013
Revenues:							
North America	$ 3,204	$ 3,117	$ 3,060	3 %	2 %	3 %	2%
EMEA	541	583	537	(7)%	9 %	7 %	7%
APAC	180	207	197	(13)%	5 %	(3)%	9%
LATAM	164	139	144	18 %	(3)%	35 %	31%
Total segment revenue	$ 4,089	$ 4,046	$ 3,938	1 %	3 %	4 %	4%
Key indicators:							
North America merchant transactions (a)	43,362	41,453	40,445	5 %	2 %		
International merchant transactions (b)	6,867	6,030	5,338	14 %	13 %		

(a) North America merchant transactions include acquired Visa and MasterCard credit and signature debit, American Express and Discover, PIN-debit, electronic benefits transactions, processed-only and gateway customer transactions at the POS. North American merchant transactions reflect 100% of alliance transactions.

(b) International merchant transactions include Visa, MasterCard, and other payment network merchant acquiring transactions for clients outside the U.S. and Canada. Transactions include credit, signature debit, PIN-debit POS, POS gateway, and ATM transactions.

Global Business Solutions Segment revenue increased 4% on a constant currency basis in 2015 compared to 2014 led by growth in our North America, EMEA, and LATAM regions. North America revenue growth was driven by growth in equipment sales of approximately $70 million and an increase in software sales of approximately $20 million. The growth in equipment sales excludes approximately $50 million in deferred revenue related to our *Clover* suite of terminal devices during 2015, which will be recognized over 36 months along with the direct costs associated with *Clover* sales. Equipment sales and leases increased as our clients continue to adopt our EMV solutions. Software sales increased as a result of investments in our merchant suite of products, including the roll-out of our Transarmor Solutions which commenced in the fourth quarter of 2014. North America acquiring revenue remained flat in 2015 compared to 2014. Constant currency revenue growth in our EMEA region was driven by volume growth partially offset by the impact of a $12 million sale of a merchant portfolio in Poland during 2014. Constant currency revenue growth in our LATAM region was driven by revenue growth in our Brazil market of approximately $12 million and

inflation in Argentina of approximately $28 million. The increase in prices in Argentina is a result of rising costs which we are generally able to pass through to our clients. Constant currency revenue decline in our APAC region was driven by declines in our ATM business in Australia.

North America transaction growth in 2015 compared to 2014 was driven by growth in our distribution systems. International transaction growth in 2015 compared to 2014 outpaced revenue growth due to the impact of foreign currency exchange rate movements.

Global Business Solutions Segment revenue increased 4% on a constant currency basis in 2014 compared to 2013 led by growth in our North America and EMEA regions. North America segment growth was driven by net pricing increases resulting in an increase of approximately $20 million for regional merchants and network routing incentives. In addition, our North America revenue growth was positively impacted by approximately $25 million in equipment sales and approximately $15 million in software sales growth. EMEA growth was driven by growth in our merchant acquiring alliances business and the impact of a $12 million sale of a merchant portfolio in Poland during the fourth quarter of 2014 . Constant currency growth in our LATAM region was driven primarily by inflation.

North America transaction growth in 2014 compared to 2013 was driven by growth in our national and ISO merchants, partially offset by lost business at Walmart as they shifted from using us as their sole processor to a dual processor strategy in the first quarter of 2014. The Walmart shift resulted in a revenue decline of $16 million compared to the prior year. This decline was partially offset by volume growth from other clients. International transaction growth in 2014 compared to 2013 outpaced revenue growth due to changes in transaction mix and the impact of foreign currency exchange rate movements.

Global Financial Solutions segment results

The following table displays total revenue by segment region and illustrates, on a percentage basis, the impact of foreign currency fluctuations on revenue growth.

	Year ended December 31,			Percent Change		Constant Currency Percent Change	
(in millions)	2015	2014	2013	2015 vs. 2014	2014 vs. 2013	2015 vs. 2014	2014 vs. 2013
Revenues:							
North America	$ 883	$ 815	$ 757	8 %	8 %	8 %	8%
EMEA	435	490	440	(11)%	11 %	— %	9%
APAC	75	87	92	(14)%	(5)%	(1)%	—%
LATAM	102	97	95	5 %	2 %	14 %	20%
Total segment revenue	$ 1,495	$ 1,489	$ 1,384	— %	8 %	6 %	9%
Key indicators:							
North America card accounts on file (a)	813	714	692	14 %	3 %		
International card accounts on file (b)	146	132	115	11 %	15 %		

(a) North America card accounts on file reflect the total number of bankcard credit and retail credit accounts as of the end of the periods presented.
(b) International card accounts on file reflect total bankcard and retail accounts outside the United States and Canada as of the end of the periods presented.

Global Financial Solutions Segment revenue increased 6% on a constant currency basis in 2015 compared to 2014 led by growth in our North America region. North America revenue growth was split evenly between our print, plastics, and remittance services businesses and our credit and retail card processing businesses. Growth in print, plastics, and remittance services was driven by higher print volumes and plastics growth resulting from EMV card issuances. Credit and retail processing growth was driven by an increase in card accounts tied to growth from existing customers and new business. EMEA was flat on a constant currency basis as new and existing business growth was offset by lost business in the United Kingdom of $13 million and price compression in Germany of $19 million. Germany price compression was driven by the renewal of one large client at the end of 2014. We do not anticipate the renewal of any large clients in Germany through 2019. LATAM constant currency revenue growth was driven by inflation in Argentina.

North America card accounts on file increased in 2015 compared to 2014 from net new account conversions and growth from existing clients. International accounts on file increased 2015 compared to 2014 due to new portfolios of existing clients in the United Kingdom.

Global Financial Solutions Segment revenue increased 9% on a constant currency basis in 2014 compared to 2013 led by our North America, EMEA, and LATAM regions. North America revenue growth was driven by a $34 million increase in credit and retail card processing and an increase in print, plastics, and remittance services revenue. Credit and retail processing growth was driven by an increase in card accounts tied to growth from existing customers and new business growth. Growth in print, plastics, and remittance services was driven by higher print volumes, and plastics growth resulting from EMV card issuances. EMEA revenue increased due to new business from existing clients in the United Kingdom and Greece. LATAM constant currency revenue growth was driven by volume growth in Argentina.

North America card accounts on file increased in 2014 compared to 2013 from net new account conversions and growth from existing clients. International accounts on file increased 2014 compared to 2013 due to new portfolios of existing clients in the United Kingdom.

Network & Security Solutions segment results

The following table displays total revenue by product. Our Network & Security Solutions segment is comprised of more than 99% domestic businesses with no material foreign exchange impact on reported results.

	Year ended December 31,			Percent Change	
(in millions)	**2015**	**2014**	**2013**	**2015 vs. 2014**	**2014 vs. 2013**
Revenues:					
EFT Network	$ 491	$ 466	$ 449	5%	4 %
Stored Value Network	359	332	347	8%	(4)%
Security and Fraud	412	384	386	7%	(1)%
Other (a)	202	187	180	8%	4 %
Segment revenue	$ 1,464	$ 1,369	$ 1,362	7%	1 %
Key indicators:					
Network transactions (EFT and Stored Value) (b)	18,918	17,435	16,763	9%	4 %

(a) Other revenue is primarily comprised of revenue generated from our Government and Online banking businesses
(b) Network transactions include the debit issuer processing transactions, *STAR Network* issuer transactions, and closed loop and open loop transactions.

Network & Security Solutions revenue increased 7% in 2015 compared to 2014 driven by strong growth within all of our product categories. EFT Network revenue increased due to growth from new and existing clients of $28 million, partially offset by pricing changes. Stored Value Network revenue increased due to growth in open loop prepaid card transactions, partially offset by the disposition of a noncore transportation payments joint venture, EFS, in the second quarter of 2014 which had an approximate $20 million negative impact on segment revenue for the year. Stored Value Network revenue also benefited by $10 million driven by a change in contract terms for one client. Security and Fraud revenue increased $28 million due to a growth of $50 million due to security and fraud products excluding *Telecheck*, that includes the roll-out of our Transarmor Solutions to SMB which commenced in the fourth quarter of 2014. The growth was partially offset by a decline in *TeleCheck* revenue. Other revenue increased due to growth from a new short-term government contract that was awarded during the first quarter of 2015.

Network & Security Solutions revenue increased 1% in 2014 compared to 2013 driven by a 4% growth in our EFT Network business, partially offset by a 4% decrease in our Stored Value Network business. Security and Fraud revenue decreased 1% as continued declines in check revenue of $24 million were partially offset by growth in our portfolio of fraud solutions products.

EFT Network revenue increased due to internal growth and a new transaction routing program that was introduced in the first quarter of 2014, which positively impacted growth by $17 million in 2014 compared to 2013. Stored Value Network revenue decreased due to the disposition of EFS that occurred in late May 2014 and had an approximate $30 million negative impact on segment revenue. The impact of the EFS disposition was partially offset by higher payment volumes within the open loop payroll distribution program related to existing clients and new business.

Reimbursable PIN debit fees, postage, and other

Revenue increased in 2015 compared to 2014 due to transaction and volume growth related to PIN debit fees of $26 million and print and plastics remittance services.

Revenue increased in 2014 compared to 2013 due to transaction and volume growth related to PIN debit fees partially offset by changes in regulated financial institution mix.

Operating expenses overview

(in millions)	Year ended December 31, 2015	2014	2013	Percent Change 2015 vs. 2014	2014 vs. 2013
Cost of services (exclusive of items shown below)	$ 2,871	$ 2,668	$ 2,723	8 %	(2)%
Cost of products sold	356	330	328	8 %	1 %
Selling, general, and administrative	2,292	2,043	1,980	12 %	3 %
Depreciation and amortization	1,022	1,056	1,091	(3)%	(3)%
Other operating expenses, net	53	13	56	308 %	(77)%
Total expenses (excluding reimbursable items)	6,594	6,110	6,178	8 %	(1)%
Reimbursable PIN debit fees, postage, and other	3,687	3,604	3,507	2 %	3 %
Total expenses	$ 10,281	$ 9,714	$ 9,685	6 %	— %

Cost of services

Cost of services expense increased in 2015 compared to 2014 driven by a $128 million increase in stock compensation expense which was primarily triggered by our IPO and a $40 million increase in contractor and employee expenses related to product matters. Cost of services was also negatively impacted by $24 million related to various customer matters. Both 2015 and 2014 include a benefit of approximately $15 million from gains on the revaluation of U.S. dollar denominated assets and liabilities in Argentina. Foreign currency positively impacted cost of services expense by approximately $90 million.

Cost of services expense decreased in 2014 compared to 2013 due to our focus on operational and processing efficiencies including lower headcount and changes in compensation programs which resulted in $60 million in savings, a $10 million tax recovery in Australia, lower credit card authorization expenses of $19 million, a $15 million gain on the revaluation of U.S. dollar denominated assets and liabilities in Argentina, and positive foreign currency impact, partially offset by development initiatives of $26 million and a $22 million reserve for uncollectible receivables in Latin America.

Cost of products sold

Cost of products sold expense increased in 2015 compared to 2014 due to growth in equipment sales driven by adoption of our EMV compatible solutions.

Cost of products sold expense was flat in 2014 compared to 2013.

Selling, general, and administrative

(in millions)	Year ended December 31, 2015	2014	2013	Percent Change 2015 vs. 2014	2014 vs. 2013
Salaries, wages, bonus, and other	$ 896	$ 741	$ 742	21 %	— %
Independent sales organizations (ISOs) commissions	642	587	579	9 %	1 %
Outside professional services	295	216	196	37 %	10 %
Commissions	158	147	136	7 %	8 %
Other	301	352	327	(14)%	8 %
Selling, general, and administrative expense	$ 2,292	$ 2,043	$ 1,980	12 %	3 %

Selling, general, and administrative expense increased $249 million in 2015 compared to 2014 driven by $228 million in charges related to our initial public offering ($150 million related to stock compensation expense, which is included in salaries, wages, bonus and other and $78 million in one-time KKR management termination fees, which is included within outside professional

services). In addition, we incurred a $55 million increase in payments to independent sales organizations resulting from growth within this channel. The items noted previously, were partially offset by a reduction of $49 million in other expenses driven by cost management initiatives. Foreign currency positively impacted selling, general, and administrative expenses by approximately $60 million.

Selling, general, and administrative expense increased in 2014 compared to 2013 largely due to growth in payments to independent sales organizations resulting from increased transactions and volumes, higher legal fees of $6 million, and expenses incurred throughout 2014 related to the transition of several corporate functions from Denver to Atlanta in the amount of $6 million. Other, which includes advertising and promotional expenses, business travel and entertainment expenses, and other selling expenses, increased mainly due to increased marketing expenditures of $22 million related to new products. Internal sales commissions expense increased due to increased sales.

Depreciation and amortization

	Year ended December 31,			Percent Change	
(in millions)	2015	2014	2013	2015 vs. 2014	2014 vs. 2013
Depreciation expense	$ 290	$ 286	$ 288	1 %	(1)%
Amortization expense (a)	732	770	803	(5)%	(4)%
Depreciation and amortization	$ 1,022	$ 1,056	$ 1,091	(3)%	(3)%

(a) Decrease driven by a reduction in amortization expense on acquisition intangibles.

Other operating expenses, net includes restructuring, litigation and regulatory settlements, impairments, and other as applicable to the periods presented. Refer to note 10 "Restructuring" to our consolidated financial statements in Part II, Item 8 of this Form 10-K for details regarding restructuring charges and our restructuring program. Pursuant to our announced expense management initiative, we expect to achieve $200 million in gross annualized savings by mid-2016. We expect to incur $75 million of restructuring charges of which we incurred $53 million during 2015, principally related to severance costs.

Reimbursable PIN debit fees, postage, and other

Expense increased in 2015 compared to 2014 due to transaction and volume growth related to PIN debit fees of $26 million and print and plastics remittance services.

Expense increased in 2014 compared to 2013 due to transaction and volume growth related to PIN debit fees, partially offset by changes in regulated financial institution mix.

Interest expense, net

	Year ended December 31,			Percent Change	
(in millions)	2015	2014	2013	2015 vs. 2014	2014 vs. 2013
Interest expense, net	$ (1,537)	$ (1,728)	$ (1,856)	(11)%	(7)%

Interest expense, net decreased in 2015 compared to 2014 and 2014 compared to 2013 due to lower outstanding debt balances as a result of debt extinguishments and lower interest rates as a result of debt exchanges and refinancing's. Refer to note 2 "Borrowings" to our consolidated financial statements in Part II, Item 8 of this Form 10-K.

Loss on debt extinguishment

	Year ended December 31,			Percent Change	
(in millions)	2015	2014	2013	2015 vs. 2014	2014 vs. 2013
Loss on debt extinguishment	$ (1,068)	$ (274)	$ (79)	290%	247%

Refer to note 2 "Borrowings" to our consolidated financial statements in Part II, Item 8 of this Form 10-K for additional information.

Other income (expense)

(in millions)	Year ended December 31, 2015	2014	2013
Investment gains and (losses)	$ —	$ 100	$ 2
Derivative financial instruments gains and (losses)	(17)	—	(24)
Divestitures, net	5	2	(5)
Non-operating foreign currency gains and (losses)	41	59	(20)
Other income (expense)	$ 29	$ 161	$ (47)

Investment gains in 2014 relate to the sale of our 30% minority interest in EFS which resulted in a pretax gain of $98 million.

Losses on derivative financial instruments in 2015 were driven by fair value adjustments on our non designated forward step up swaps as interest rate swap rates decreased during the period. The net loss in 2013, was due to fair value adjustments for interest rate swaps and cross currency swaps that are not designated as accounting hedges.

Non-operating foreign currency gains and (losses) amounts represent net gains and losses related to currency translations on our intercompany loans and euro-denominated debt. The gain during 2015 and 2014 was driven by the U.S. dollar strengthening against the Euro. We designated all of our euro-denominated debt as a hedge against our net investment in euro business as of January 1, 2016, which would have eliminated an income statement gain of $70 million recorded in 2015, if the hedge was fully effective during the period.

Income taxes

(in millions)	Year ended December 31, 2015	2014	2013
Income tax expense	$ 101	$ 82	$ 105
Effective income tax rate	(9)%	(45)%	(16)%

The effective tax rates in each year differ from the statutory rates as a result of recognizing tax expense in jurisdictions with pretax income while being precluded from recognizing deferred tax benefits on pre-tax losses in the U.S. and certain foreign jurisdictions that are subject to deferred tax valuation allowances. In each year, the negative impact from the deferred tax valuation allowance was partially offset by us not having to record tax expense attributable to the noncontrolling interest portion of pretax income from pass through entities.

Following the recognition of significant deferred tax valuation allowances in 2012, we have regularly experienced substantial volatility in our effective tax rate in interim periods and across years. This is due to deferred income tax benefits not being recognized in several jurisdictions, most notably in the United States, and changes in the amount, mix, and timing of pretax earnings in tax paying jurisdictions that can have a significant impact on the overall effective tax rate. This interim and full year volatility is likely to continue in future periods until the deferred tax valuation allowances can be released.

Since 2007, we have been and continue to be in a net operating loss position in the U.S. federal and combined state jurisdictions. These net operating losses caused our net deferred tax assets to exceed our net deferred tax liabilities as of December 31, 2015. This net deferred tax asset position, combined with the history of operating losses, is significant negative evidence that the more likely than not criteria requires us to record a deferred tax valuation allowance against our net deferred tax assets. Further, we are not able to record a benefit related to tax losses in many separate filing states and certain foreign countries, requiring the establishment of deferred tax valuation allowances.

We, or one or more of our subsidiaries, file income tax returns in the U.S. federal jurisdiction and various state and foreign jurisdictions. As of December 31, 2015, we were no longer subject to income tax examination by the U.S. federal jurisdiction for years before 2005. State and local examinations are substantially complete through 2006. Foreign jurisdictions generally remain subject to examination by their respective authorities from 2008 forward, none of which are considered major jurisdictions. Refer to note 8 "Income Taxes" to our consolidated financial statements in Part II, Item 8 of this Form 10-K for additional information.

Equity earnings in affiliates

(in millions)	Year ended December 31, 2015	2014	2013	Percent Change 2015 vs. 2014	2014 vs. 2013
Equity earnings in affiliates	$ 239	$ 220	$ 188	9%	17%

Equity earnings in affiliates relate to the earnings of our merchant alliance partnerships and increased in 2015 and 2014 due to higher volumes, pricing initiatives, and increased terminal revenues.

Net income attributable to noncontrolling interests and redeemable noncontrolling interest

(in millions)	Year ended December 31, 2015	2014	2013	Percent Change 2015 vs. 2014	2014 vs. 2013
Net income attributable to noncontrolling interests and redeemable noncontrolling interest	$ 213	$ 193	$ 177	10%	9%

Net income attributable to noncontrolling interests and redeemable noncontrolling interest relates to the interests of our merchant partners in our consolidated merchant alliances. Net income attributable to noncontrolling interests and redeemable noncontrolling interest increased in 2015 compared to 2014 due to net volume growth within our Bank of America Merchant Services alliance.

Net income attributable to noncontrolling interests and redeemable noncontrolling interest increased in 2014 compared to 2013 due to net volume growth and lower credit losses from our consolidated alliances particularly within our Bank of America Merchant Services alliance.

Adjusted EBITDA Overview

The following table displays adjusted *EBITDA* by segment for the periods indicated:

(in millions)	Year ended December 31, 2015	2014	2013	Percent Change 2015 vs. 2014	2014 vs. 2013
Adjusted EBITDA:					
Global Business Solutions	$ 1,681	$ 1,687	$ 1,644	—%	3%
Global Financial Solutions	550	529	404	4 %	31%
Network & Security Solutions	639	608	549	5 %	11%
Corporate	(140)	(161)	(148)	(13)%	9%
Total Adjusted EBITDA	$ 2,730	$ 2,663	$ 2,449	3 %	9%

The following table displays adjusted *EBITDA* margin by segment for the periods indicated:

	Year ended December 31, 2015	2014	2013	Change 2015 vs. 2014	2014 vs. 2013
Adjusted EBITDA Margin:					
Global Business Solutions	41.1%	41.7%	41.7%	(60) bps	0 bps
Global Financial Solutions	36.8%	35.5%	29.2%	130 bps	630 bps
Network & Security Solutions	43.6%	44.4%	40.3%	(80) bps	410 bps
Total Adjusted EBITDA	38.7%	38.6%	36.6%	10 bps	200 bps

Global Business Solutions

Global Business Solutions Adjusted EBITDA remained flat in 2015 compared to 2014 primarily driven by the revenue items noted previously within "*Global Business Solutions segment results*", specifically the revenue growth within our merchant suite of software and hardware products while expenses increased due to investments in our sales channels. Both 2015 and 2014 adjusted EBITDA were impacted by approximately $10 million from gains on the revaluation of U.S dollar denominated assets and liabilities in Argentina and a $10 million tax recovery in Australia during 2014. Currency translation negatively impacted segment adjusted

EBITDA by $31 million compared to the prior year period.

Global Business Solutions Adjusted EBITDA increased 3% in 2014 compared to 2013 from the impact of the revenue items noted within "*Global Business Solutions segment results*" above as well as a $10 million tax recovery in Australia. Additionally, adjusted
EBITDA benefited by approximately $10 million from gains on the revaluation of U.S. dollar denominated assets and liabilities in Argentina during 2014. Expenses were flat in 2014 compared to 2013 as a result of cost reduction efforts, primarily in operations costs, that were reinvested into product investment costs.

Global Financial Solutions

Global Financial Solutions Adjusted EBITDA increased in 2015 compared to 2014 due to the impact of the revenue items noted within "*Global Financial Solutions segment results*" above. Both 2015 and 2014 adjusted EBITDA benefited by approximately $5 million from gains on the revaluation of U.S. dollar denominated assets and liabilities in Argentina. Currency translation negatively impacted segment adjusted EBITDA by $23 million compared to the prior year period.

Global Financial Solutions Adjusted EBITDA increased significantly in 2014 compared to 2013 due to the impact of the revenue items noted within "*Global Financial Solutions segment results*" above as well as decreased operating expenses as a result of lower headcount and changes in compensation programs. Additionally, adjusted EBITDA benefited by approximately $5 million from gains on the revaluation of U.S. dollar denominated assets and liabilities in Argentina during 2014.

Network & Security Solutions

Network & Security Solutions Adjusted EBITDA increased in 2015 compared to 2014 due to the revenue items noted within "*Network & Security Solutions segment results*". The contract amendment discussed previously positively impacted adjusted EBITDA by $8 million. The revenue items were partially offset by increased operating expenses related to our purchases of Gyft and TWI of $24 million, investments of approximately $6 million for new *STAR Network* functionality, and the disposition of EFS which had a negative impact of approximately $10 million on segment adjusted EBITDA.

Network & Security Solutions Adjusted EBITDA increased in 2014 compared to 2013 due to the revenue items noted within "*Network & Security Solutions*" above as well as decreased operating expenses as a result of lower headcount and changes in compensation programs. In addition, the EFS disposition had a negative impact of approximately $15 million on adjusted EBITDA in 2015.

Corporate

Corporate Adjusted EBITDA improved in 2015 compared to 2014 due to a decrease in incentive compensation expense.

Corporate Adjusted EBITDA increased in 2014 compared to 2013 due to a $44 million investment in outside professional services and contractor costs, partially offset by decreased bonus and benefit expenses.

Liquidity and Capital Resources

Our source of liquidity is principally cash generated from operating activities supplemented as necessary on a short-term basis by borrowings against our senior secured revolving credit facility. We believe our current level of cash and short-term financing capabilities along with future cash flows from operations are sufficient to meet the needs of the business.

Over the past few years, we completed various amendments and modifications to certain of our debt agreements in an effort to extend our debt maturities and lower interest rates. Furthermore, First Data Holdings (FDH) completed a $3.5 billion private placement in 2014 and we completed a $2.7 billion initial public offering in 2015. Proceeds from these equity transactions were used to repay certain tranches of debt. These transactions have reduced our current annualized cash interest costs to $1 billion compared to approximately $1.8 billion in 2015. Details regarding our debt structure are provided in note 2 "Borrowings" to our consolidated financial statements in Part II, Item 8 of this Form 10-K.

As of February 25, 2016, our long-term corporate family rating from Moody's was B2 (positive outlook). The long-term local issuer credit rating from Standard and Poor's was B+ (stable). The long-term issuer default rating from Fitch was B (positive). A decrease in our credit ratings could affect our ability to access future financing, which could result in increased interest expense in the future.

Cash and cash equivalents Investments (other than those included in settlement assets) with original maturities of three months or less (that are readily convertible to cash) are considered to be cash equivalents and are stated at cost, which approximates market value. As of December 31, 2015 and 2014, we held $429 million and $358 million in cash and cash equivalents, respectively.

Included in cash and cash equivalents are amounts held by BAMS and IPS that are not available to fund operations outside of those subsidiaries. As of December 31, 2015 and 2014, the cash and cash equivalents held by these subsidiaries totaled $136 million and $152 million, respectively. All other domestic cash balances, to the extent available, are used to fund our short-term liquidity needs.

Cash and cash equivalents also includes amounts held outside of the United States totaling $161 million and $171 million as of December 31, 2015 and 2014, respectively. As of December 31, 2015, there was approximately $106 million of cash and cash equivalents held outside of the United States that was unavailable for general corporate purposes. We plan to fund any international cash needs in 2016 within our international operations with cash held by our international entities, but if necessary, could fund such needs using cash from the United States, subject to satisfying debt covenant restrictions.

Cash flows

	Year ended December 31,		
Source/(use) (in millions)	**2015**	**2014**	**2013**
Net cash provided by operating activities	$ 795	$ 1,035	$ 715
Net cash used in investing activities	(685)	(329)	(353)
Net cash used in financing activities	(16)	(743)	(532)

Cash flows from operating activities

Cash flows provided by operating activities for the periods presented resulted from normal operating activities and reflect the timing of our working capital requirements.

Our operating cash flow is significantly impacted by our level of debt. Approximately $1.8 billion, $1.7 billion, and $1.8 billion in cash interest, net of swap settlements, was paid during 2015, 2014, and 2013, respectively. The increase in cash interest in 2015 compared to 2014 is due to the acceleration of $271 million of cash interest payments as a result of our 2015 debt extinguishments.

Using December 31, 2015 balances for variable rate debt and applicable interest rate swaps, a 100 basis point increase in the applicable London Interbank Offered Rate (LIBOR) index on an annualized basis would increase our annual interest expense by approximately $46 million.

The chart below reconciles the change in operating cash flows for the years ended December 31, 2014 to December 31, 2015 and December 31, 2013 to December 31, 2014.

Source/(use) (in millions)	**Year ended December 31, 2015**	**Year ended December 31, 2014**
Net cash provided by operating activities, previous period	$ 1,035	$ 715
Increases (decreases) in:		
Net income, excluding other operating expenses and other income (a)	240	473
Depreciation and amortization	(30)	(49)
Working capital	(450)	(104)
Net cash provided by operating activities, end of period	$ 795	$ 1,035

(a) Excludes loss on debt extinguishment, share-based compensation expense and other non-cash items.

In 2015 compared to 2014, net income, excluding other operating expenses and other income increased due to the items noted previously within "Results of Operations". Working capital decreased primarily due to $268 million from lower interest accruals as a result of our debt restructurings and accelerated interest payments on called debt. In addition, we experienced growth in our product sales and other revenue streams which lowered net loss but negatively impacted working capital by approximately $134 million, as these revenues streams typically have longer payment terms. Additionally, timing of prepayments and vendor payments negatively impacted working capital by $111 million. These items were partially offset by $96 million from two supplier signing bonuses received during the year.

In 2014 compared to 2013, net income, excluding other operating expenses and other income increased due to the items noted within "Results of Operations". Working capital decreased primarily due to $53 million in lower interest accruals as a result of debt restructurings.

Cash flows from investing activities

Cash flows used in investing activities increased in 2015 compared to 2014 due to the sale of our 30% minority interest in a transportation payments business, EFS, for $264 million in cash in 2014, increases in capital expenditures due to customer signing bonuses and investments in technology, and the acquisition in 2015 of TWI for $62 million, a provider of digital stored value products that offer gift card programs, loyalty incentives, and integrated marketing solutions for retailers, partners, and consumers.

Cash flows used in investing activities decreased in 2014 compared to 2013 due to the sale of our 30% minority interest in EFS for $264 million in cash, partially offset by increases in capital expenditures due to technology additions and international ATM and POS additions, and the acquisition of Gyft, Inc.

For a more detailed discussion on the acquisitions and disposition discussed above refer to note 12 "Acquisitions and Dispositions" to our consolidated financial statements in Part II, Item 8 of this Form 10-K.

Cash flows from financing activities

Cash flows used in financing activities decreased in 2015 compared to 2014 due to $2.7 billion of net proceeds from our initial public offering and new debt issuances, partially offset by debt paydowns, payments of debt-related costs and a decrease in capital transactions with our former parent FDH, relating primarily to a $2.5 billion capital contribution in 2014.

Cash flows used in financing activities increased in 2014 compared to 2013 due to a decrease in proceeds from the issuance of long-term debt, $686 million of dividends paid to FDH, and payments of debt-related costs, partially offset by a $2.5 billion capital contribution from FDH and a decrease in debt principal payments.

Debt

In 2015, we made significant progress in refinancing our debt structure, see note 2 "Borrowings" to our consolidated financial statements in Part II, Item 8 of this Form 10-K for additional information on our restructuring activity. As a result of the restructuring activity, we significantly lowered our weighted average interest rate from 7.4% as of December 31, 2014 to 5.6% as of December 31, 2015. Approximately 77% of our debt, including debt swapped from variable to fixed rates, was at a fixed rate, providing a measure of protection if interest rates begin to rise. We have $5 billion in notional interest rate swaps that all expire during September 2016.

Senior secured revolving credit facility

On June 2, 2015, we terminated and replaced our previous $1.0 billion senior secured revolving credit facility with a new $1.25 billion facility. The new revolving credit facility matures on June 2, 2020, subject to certain earlier springing maturity provisions in certain circumstances. Besides the letters of credit discussed below, we had no amounts outstanding and $10 million outstanding against the facilities as of December 31, 2015 and 2014, respectively. As of December 31, 2015, $1.2 billion remained available under the facility. Excluding the letters of credit, the maximum amount outstanding against this facility during 2015 was approximately $526 million while the average amount outstanding during 2015 was approximately $154 million.

The senior secured revolving credit facility can be used for working capital and general corporate purposes. We utilize our senior secured revolving credit facility to fund investing or operating activities when cash flows from operating activities are not sufficient. We believe cash on hand and cash flow generated through our normal operating activities in conjunction with the capacity under our senior secured revolving credit facility will be sufficient to meet our liquidity needs.

There are multiple institutions that have commitments under this facility with none representing more than 18% of the remaining capacity.

Accounts receivable securitization agreement

On December 31, 2015, the Company established a new fully consolidated and wholly owned subsidiary, First Data Receivables, LLC (FDR). FDR and FDC entered into an agreement where certain wholly owned subsidiaries of FDC agreed to transfer and contribute receivables to FDR. FDR's assets are not available to satisfy obligations of any other entities or affiliates of FDC. FDR's

creditors will be entitled, upon its liquidation, to be satisfied out of FDR's assets prior to any assets or value in FDR becoming available to FDR's equity holders. FDR entered into an agreement with an external party, which expires in 2019, to borrow $240 million secured by liens on the receivables contributed to FDR by the wholly owned subsidiaries of FDC. Loans under the Agreement bear interest based upon LIBOR plus 200 basis points or a base rate equal to the highest of (i) the applicable lender's prime rate, or (ii) the federal funds rate plus 0.50%. As of December 31, 2015, we had no debt outstanding under the Securitization Agreement. In January 2016, FDC and its wholly owned subsidiaries transferred approximately $326 million in receivables to FDR as part of its Securitization Program. FDR utilized the receivables as collateral in borrowings of $240 million under this agreement. The $240 million in gross proceeds was utilized to redeem a portion of the Company's 8.75% senior secured second lien notes on January 15, 2016.

Letters, lines of credit, and other

	Total Available (a)		Total Outstanding	
	As of December 31,		As of December 31,	
(in millions)	2015	2014	2015	2014
Letters of credit (b)	$ 250	$ 500	$ 42	$ 43
Lines of credit and other (c)	245	349	43	68

(a) Total available without giving effect to amounts outstanding.
(b) Outstanding letters of credit are held in connection with lease arrangements, bankcard association agreements, and other security agreements. The largest amount of letters of credit outstanding during 2015 was approximately $46 million. All letters of credit expire on or prior to December 31, 2016 with a one-year renewal option. We expect to renew most of the letters of credit prior to expiration.
(c) As of December 31, 2015, represents $228 million of committed lines of credit as well as certain uncommitted lines of credit and other agreements that are available in various currencies to fund settlement and other activity. We cannot use these lines of credit for general corporate purposes. Certain of these arrangements are uncommitted but, as of the dates presented, we had borrowings outstanding against them.

In the event one or more of the aforementioned lines of credit becomes unavailable, we will utilize our existing cash, cash flows from operating activities or our senior secured revolving credit facility to meet our liquidity needs.

Guarantees and covenants All obligations under the senior secured revolving credit facility and our senior secured term loan facilities are unconditionally guaranteed by most of our existing and future, direct and indirect, wholly owned, material domestic subsidiaries. The senior secured facilities contain a number of covenants that, among other things, restrict our ability to incur additional indebtedness; create liens; enter into sale-leaseback transactions; engage in mergers or consolidations; sell or transfer assets; pay dividends and distributions or repurchase our capital stock; make investments, loans or advances; prepay certain indebtedness; make certain acquisitions; engage in certain transactions with affiliates; amend material agreements governing certain indebtedness; and change our lines of business. The senior secured facilities also require us to not exceed a maximum senior secured leverage ratio and contain certain customary affirmative covenants and events of default, including a change of control. The senior secured term loan facility also requires mandatory prepayments based on a percentage of excess cash flow generated by us.

All obligations under the senior secured notes, senior notes, and senior subordinated notes are similarly guaranteed in accordance with their terms by each of our domestic subsidiaries that guarantee obligations under our senior secured term loan facility described above. These notes and facilities also contain a number of covenants similar to those described for the senior secured obligations noted above.

Although all of the above described instruments of indebtedness contain restrictions on our ability to incur additional indebtedness, these restrictions are subject to numerous qualifications and exceptions, including the ability to incur indebtedness in connection with our settlement operations. We believe that the indebtedness that can be incurred under these exceptions as well as additional credit under the existing senior secured revolving credit facility are sufficient to satisfy our needs for the foreseeable future.

Covenant compliance Under the senior secured revolving credit and term loan facilities, certain limitations, restrictions, and defaults could occur if we are not able to satisfy and remain in compliance with specified financial ratios. We have agreed that we will not permit the Consolidated Senior Secured Debt to Covenant EBITDA (both as defined in the agreement) Ratio for any 12 month period (last four fiscal quarters) to be greater than 6.0 to 1.0.

The breach of this covenant could result in a default under the senior secured revolving credit facility and the senior secured term loan credit facility and the lenders could elect to declare all amounts borrowed due and payable. Any such acceleration could also result in a default under the indentures for the senior secured notes, senior notes, and senior subordinated notes. As of December 31, 2015, we were in compliance with all applicable covenants, including our sole financial covenant with Consolidated Senior Secured Debt of $12.8 billion, Covenant EBITDA of $3.2 billion and a Ratio of 4.0 to 1.0.

In determining Covenant EBITDA, EBITDA is calculated by reference to net income (loss) from continuing operations plus interest and other financing costs, net, provision for income taxes, and depreciation and amortization. Covenant EBITDA is calculated by adjusting EBITDA to exclude unusual items as permitted in calculating covenant compliance under the credit facilities. Covenant EBITDA is further adjusted to add net income attributable to noncontrolling interests and redeemable noncontrolling interest of certain non wholly owned subsidiaries and exclude other miscellaneous adjustments that are used in calculating covenant compliance under the agreements governing our senior secured credit facilities. We believe that the inclusion of supplementary adjustments to EBITDA applied in presenting Covenant EBITDA are appropriate to provide additional information to investors to demonstrate our ability to comply with our financing covenants. Because not all companies use identical calculations, this presentation of Covenant EBITDA may not be comparable to other similarly titled measures of other companies.

The calculation of Covenant EBITDA under our senior secured facilities is as follows:

(in millions)	Last twelve months ended December 31, 2015
Net loss attributable to First Data Corporation	$ (1,481)
Interest expense, net	1,537
Income tax expense	101
Depreciation and amortization (1)	1,133
EBITDA	1,290
Loss on debt extinguishment	1,068
Share-based compensation	329
Net income attributable to noncontrolling interests and redeemable noncontrolling interest	213
Projected near-term cost savings and revenue enhancements (2)	118
KKR related items	100
Restructuring, net	53
Non-operating foreign currency (gains) and losses	(41)
Litigation and regulatory settlements	20
Derivative financial instruments (gains) and losses	17
Equity entities taxes, depreciation and amortization (3)	11
Debt issuance costs	4
Other (4)	37
Covenant EBITDA	$ 3,219

(1) Includes amortization of initial payments for new contracts which is recorded as a contra-revenue within "Transaction and processing service fees" of $51 million and amortization related to equity method investments, which is netted within the "Equity earnings in affiliates" line of $60 million.
(2) Reflects cost savings and revenue enhancements projected to be realized as a result of specific actions as if they were achieved on the first day of the period. Includes cost savings initiatives associated with the business optimization projects and other technology initiatives. We may not realize the anticipated cost savings pursuant to our anticipated timetable or at all.
(3) Represents our proportional share of income taxes, depreciation and amortization on equity method investments.
(4) Includes items such as impairments, customer disputes, earnouts, cost of alliance conversions and other technology initiatives, and other as applicable to the period presented.

Off-Balance Sheet Arrangements

During 2015, 2014, and 2013, we did not engage in any off-balance sheet financing activities other than those included in the "Contractual Obligations" discussion below and those reflected in note 14 "Commitments and Contingencies" to our consolidated financial statements in Part II, Item 8 of this Form 10-K.

Contractual Obligations

Our contractual obligations as of December 31, 2015 are as follows:

	Payments Due by Period				
(in millions)	Total	Less than 1 year	1-3 years	3-5 years	After 5 years
Borrowings (a)	$ 25,455	$ 1,798	$ 7,672	$ 2,850	$ 13,135
Capital lease obligations (b)	213	81	109	15	8
Operating leases	309	56	85	58	110
Purchase obligations (c):					
Technology and telecommunications (d)	644	323	253	68	—
All other (e)	95	46	35	8	6
Other long-term liabilities	116	36	70	9	1
Total (f) (g)	$ 26,832	$ 2,340	$ 8,224	$ 3,008	$ 13,260

(a) Includes future principal and cash interest payments on long-term borrowings through scheduled maturity dates. Includes $4.6 billion of variable rate debt (including the impact of interest rate swaps). Includes $32 million in contractual call premiums to expire our 8.75% senior-secured-second lien notes due 2022 during January 2016. Borrowings and interest rate swaps are discussed in note 2 "Borrowings" and note 13 "Derivative Financial Instruments", respectively, to our consolidated financial statements in Part II, Item 8 of this Form 10-K. Interest payments for the variable rate debt and the associated interest rate swaps were calculated using interest rates as of December 31, 2015 .

(b) Represents future payments on existing capital leases, including interest expense, through scheduled expiration dates.

(c) Many of our contracts contain clauses that allow us to terminate the contract with notice, and with or without a termination penalty. Termination penalties are generally an amount less than the original obligation. Certain contracts also have an automatic renewal clause if we do not provide written notification of our intent to terminate the contract. Obligations under certain contracts are usage-based and are, therefore, estimated in the above amounts. Historically, we have not had any significant defaults of our contractual obligations or incurred significant penalties for termination of our contractual obligations.

(d) Technology and telecommunications represents obligations related to hardware purchases, including purchases of ATMs and terminals, as well as software licenses, hardware and software maintenance and support, technical consulting services, and telecommunications services.

(e) All other includes obligations related to materials, data, non-technical contract services, facility security, investor management fees, maintenance, and marketing promotions.

(f) We evaluate the need to make contributions to our pension plans after considering the funded status of the pension plans, movements in the discount rates, performance of the plan assets and related tax consequences. Expected contributions to our pension plan have not been included in the table as such amounts are dependent upon the considerations discussed above, and may result in a wide range of amounts. See note 15 "Employee Benefit Plans" to our consolidated financial statements in Part II, Item 8 of this Form 10-K.

(g) As of December 31, 2015, we had approximately $277 million of tax contingencies comprised of approximately $261 million reported in long-term income taxes payable in the "Other long-term liabilities" line of our consolidated balance sheets, including approximately $4 million of income tax liabilities for which The Western Union Company (Western Union) is required to indemnify us, and approximately $16 million recorded as an increase of our deferred tax liability. These amounts have been excluded from the table because the settlement period cannot be reasonably estimated. The timing of these payments will ultimately depend on the progress of tax examinations with the various tax authorities.

Critical Accounting Policies

Goodwill Goodwill represents the excess of cost over the fair value of net assets acquired, including identifiable intangible assets, and has been allocated to reporting units. Our reporting units are businesses at the operating segment level or one level below the operating segment level for which discrete financial information is prepared and regularly reviewed by management.

We test goodwill annually for impairment, as well as upon an indicator of impairment, using a fair value approach at the reporting unit level. The fair value of our reporting units is based on a discounted cash flow models involving several assumptions. When appropriate we consider assumptions that we believe a hypothetical marketplace participant would use in estimating future cash flows. The key assumptions include adjusted EBITDA growth and weighted average cost of capital (discount rate). We determined adjusted EBITDA growth based on management estimates and business plans. Discount rate assumptions are based on an assessment of the risk inherent in future cash flows of the respective reporting unit as well as cost of debt and equity.

If it is determined that the fair value of the reporting unit is less than its carrying value, we would estimate the fair value of all of the reporting unit's assets and liabilities and calculate an implied fair value of goodwill, which is the difference between the reporting unit's fair value and the fair value of all its other assets and liabilities. If the implied fair value of goodwill is less than its carrying value, the shortfall is recognized as impairment. The methodology for estimating fair value varies by asset; however, the most significant assets are intangible assets. We estimate the fair value of the intangible assets using the excess earnings method, royalty savings method, or cost savings method, all of which are a form of a discounted cash flow analysis. An impairment charge of a reporting unit's goodwill could have a material adverse effect on our financial results. An impairment charge may be caused by changes in the underlying business and economic conditions, the most relevant of which would be a deterioration in global economic conditions. Deterioration in global economic conditions could cause us to experience a decrease in our adjusted EBITDA.

Furthermore, volatility in the debt markets which impacted our debt yields, could affect these estimates used in the analysis discussed above, which in turn could affect the fair value of the reporting unit. Thus, it is possible for reporting units that record impairments to record additional impairments in the future. All key assumptions and valuations are determined by and are the responsibility of management. The factors used in the impairment analysis are inherently subject to uncertainty. We believe that we have made reasonable estimates and assumptions to determine the fair value of our reporting units, if actual results are not consistent with these estimates and assumptions, goodwill and other intangible assets may be overstated which could trigger an impairment charge.

As of December 31, 2015, the carrying value of goodwill was $16.8 billion of which $14.2 billion was related to our Global Business Solutions reporting unit. As of October 1, 2015, the most recent impairment analysis date, the fair value of our reporting units exceeded their carrying value by more than 50% with the exception of our Global Business Solutions and Global Financial Solutions reporting units. Our Global Business Solutions and Global Financial Solutions reporting unit's carrying value exceeded fair value by 25% and 35%, respectively. Examples of events or circumstances that could reasonably be expected to negatively affect the underlying key assumptions and ultimately impact the estimated fair value of our reporting units may include such items as the following:

- Global economic, political, and other conditions may adversely affect trends in consumer, business, and government spending, which may adversely impact the demand for our services and our revenue and profitability;
- Our ability to anticipate and respond to changing industry trends and the needs and preferences of our clients and consumers may affect our competitiveness or demand for our products, which may adversely affect our operating results;
- Substantial and increasingly intense competition worldwide in the financial services, payments, and technology industries may materially and adversely affect our overall business and operations;
- Potential changes in the competitive landscape, including disintermediation from other participants in the payments value chain, could harm our business;
- The market for our electronic commerce services is evolving and may not continue to develop or grow rapidly enough for us to maintain and increase our profitability;
- If we are unable to maintain merchant relationships and alliances, our business may be adversely affected;
- Failure to obtain new clients or renew client contracts on favorable terms could adversely affect results of operations and financial condition; and
- Cost savings initiatives may not produce the savings expected and may negatively impact our other initiatives and efforts to grow our business.

See "Risk Factors" in Part I, Item 1A of this Form 10-K for further discussions of risks that could affect our business.

An additional analysis was performed for our Global Business Solutions and Global Financial Solutions reporting units, which sensitized the base discount rate by an additional 50 basis points. Global Business Solutions and Global Financial Solutions passing by a margin of 14% and 24%, respectively. We also sensitized EBITDA growth by a reduction of 100 basis points with Global Business Solutions and Global Financial Solutions passing by a margin of 21% and 28%, respectively. Refer to note 1 "Summary of Significant Accounting Policies" to our consolidated financial statements in Part II, Item 8 of this Form 10-K for additional information regarding goodwill.

Reserve for merchant credit losses and check guarantees With respect to the merchant acquiring business, our merchant clients (or those of our unconsolidated alliances) have the liability for any charges properly reversed by the cardholder. In the event, however, that we are not able to collect such amounts from the merchants due to merchant fraud, insolvency, bankruptcy or another reason, we may be liable for any such reversed charges. Our risk in this area primarily relates to situations where the cardholder has purchased goods or services to be delivered in the future and which have yet to be delivered, such as airline tickets.

Our obligation to stand ready to perform is minimal in relation to the total dollar volume processed. We require cash deposits, guarantees, letters of credit or other types of collateral from certain merchants to minimize this obligation. The amounts of collateral held by us and our unconsolidated alliances are as follows:

	As of December 31,	
(in millions)	**2015**	**2014**
Cash and cash equivalents collateral	$ 544	$ 440
Collateral in the form of letters of credit	108	100
Total collateral	$ 652	$ 540

We also utilize a number of systems and procedures to manage merchant risk. Despite these efforts, we historically have experienced some level of losses due to merchant defaults.

Our contingent obligation relates to imprecision in our estimates of required collateral. A provision for this obligation is recorded based primarily on historical experience of credit losses and other relevant factors such as economic downturns or increases in merchant fraud. The following table presents the aggregate merchant credit losses incurred compared to total dollar volumes processed:

	Year ended December 31,		
	2015	2014	2013
First Data and consolidated and unconsolidated alliances credit losses (in millions)	$ 67	$ 63	$ 54
First Data and consolidated alliances credit losses (in millions)	55	55	48
Total dollar volume acquired (in billions)	1,885	1,876	1,779

The reserve recorded on our consolidated balance sheets only relates to the business conducted by our consolidated subsidiaries. The reserve for unconsolidated alliances is recorded only in the alliances' respective financial statements. We have not recorded any reserve for estimated losses in excess of reserves recorded by the unconsolidated alliances nor have we identified needs to do so. The following table presents the aggregate merchant credit loss reserves:

	As of December 31,	
(in millions)	2015	2014
First Data and consolidated and unconsolidated alliances merchant credit loss reserves	$ 26	$ 24
First Data and consolidated alliances merchant credit loss reserves	22	20

The credit loss reserves, both for us and our unconsolidated alliances, are comprised of amounts for known losses and a provision for losses incurred but not reported (IBNR). These reserves primarily are determined by performing a historical analysis of chargeback loss experience. Other factors are considered that could affect that experience in the future. Such items include the general economy and economic challenges in a specific industry or those affecting certain types of clients. Once these factors are considered, we or the unconsolidated alliance establishes a rate (percentage) that is calculated by dividing the expected chargeback (credit) losses by dollar volume processed. This rate is then applied against the dollar volume processed each month and charged against earnings. The resulting reserve balance is then compared to requirements for known losses and estimates for IBNR items. Historically, this estimation process has proven to be materially accurate and we believe the recorded reserve approximates the fair value of the contingent obligation.

The majority of the *TeleCheck* business involves the guarantee of checks received by merchants. If the check is returned, *TeleCheck* is required to purchase the check from the merchant at its face value and pursue collection from the check writer. A provision for estimated check returns, net of anticipated recoveries, is recorded at the transaction inception based on recent history. The following table presents the accrued warranty and recovery balances:

	As of December 31,	
(in millions)	2015	2014
Accrued warranty balances	$ 6	$ 9
Accrued recovery balances	21	25

We establish an incremental liability (and deferred revenue) for the fair value of the check guarantee. The liability is relieved and revenue is recognized when the check clears, is presented to *TeleCheck*, or the guarantee period expires. The majority of the guarantees are settled within 30 days. The incremental liability was approximately $1 million as of December 31, 2015 and 2014. The following table details the check guarantees of *TeleCheck*.

	Year ended December 31,		
	2015	2014	2013
Aggregate face value of guaranteed checks (in billions)	$ 32	$ 36	$ 39
Aggregate amount of checks presented for warranty (in millions)	216	253	285
Warranty losses net of recoveries (in millions)	61	67	66

The maximum potential future payments under the guarantees were estimated by us to be approximately $903 million as of December 31, 2015 which represented an estimate of the total uncleared checks at that time.

Income taxes The determination of our provision for income taxes requires management's judgment in the use of estimates and the interpretation and application of complex tax laws. Judgment is also required in assessing the timing and amounts of deductible and taxable items. We establish contingency reserves for material, known tax exposures relating to deductions, transactions, and other matters involving some uncertainty as to the proper tax treatment of the item. Our reserves reflect our judgment as to the resolution of the issues involved if subject to judicial review. Several years may elapse before a particular matter, for which we have established a reserve, is audited and finally resolved or clarified. While we believe that our reserves are adequate to cover reasonably expected tax risks, issues raised by a tax authority may be finally resolved at an amount different than the related reserve. Such differences could materially increase or decrease our income tax provision in the current and/or future periods. When facts and circumstances change (including a resolution of an issue or statute of limitations expiration), these reserves are adjusted through the provision for income taxes in the period of change. As the result of the interest expense that we incur, we are currently in a tax net operating loss position. Judgment is required to determine whether some portion or all of the resulting deferred tax assets will not be realized. To the extent we determine that we will not realize the benefit of some or all of our deferred tax assets, then these assets are adjusted through our provision for income taxes in the period in which this determination is made.

We are currently in a tax net operating loss position in several jurisdictions in which we operate, including the United States, resulting in significant deferred tax assets. We establish a valuation allowance against our deferred tax assets when, based upon the weight of all available evidence, we believe it is more likely than not that some portion or all of the deferred tax assets will not be realized. We believe that a significant portion of the deferred tax assets will be realized because of the existence of sufficient taxable income within the carryforward period available under the tax law, but have established valuation allowances for those deferred tax assets that in our judgment will not be realized. In making this determination, we have considered the relative impact of all of the available positive and negative evidences regarding future sources of taxable income and tax planning strategies. However, there could be material impact to our effective tax rate if there is a significant change in our judgment. It is reasonably likely that our judgment would change with respect to the United States federal jurisdiction if our financial performance in that jurisdiction substantially improves. We do not believe that this is reasonably likely in the next 12 months. If and when our judgment changes, then the valuation allowances are adjusted through the provision for income taxes in the period in which this determination is made. Refer to note 8 "Income Taxes" to our consolidated financial statements in Part II, Item 8 of this Form 10-K for additional information regarding our income tax provision.

New Accounting Guidance

Refer to note 1 "Summary of Significant Accounting Policies" to our consolidated financial statements included in Part II, Item 8 of this Form 10-K for new accounting guidance.

ITEM 7A. QUANTITATIVE AND QUALITATIVE DISCLOSURES ABOUT MARKET RISK

Interest Rate Risk

We are exposed to market risk from changes in interest rates. Our assets include cash equivalents as well as both fixed and floating rate interest-bearing securities. These investments arise primarily from settlement funds held by us pending settlement.

Our interest rate-sensitive liabilities are our debt instruments. Our senior secured term loan facility is subject to variable interest rates. We have interest rate swaps on $5.0 billion of our variable rate debt that convert the debt to fixed rates. The interest rate swaps expire during September 2016. Therefore, as of December 31, 2015, we have approximately $4.6 billion of variable rate debt that is not subject to a fixed rate swap.

Based on the December 31, 2015 balances, a 100 basis point increase in short-term interest rates on an annualized basis compared to the interest rates as of December 31, 2015, which for the three month LIBOR was 0.6127%, and a corresponding and parallel shift in the remainder of the yield curve, would result in a decrease to pretax income of $28 million. The $28 million decrease to

pretax income (due to a 100 basis point increase in variable rates as of December 31, 2015) is due to a $46 million increase in interest expense related to our balance of variable interest rate debt, net of interest rate swaps. The increase in interest expense would be partially offset by a $18 million increase in interest income. A decrease in interest rates would result in an increase to pretax income. Actual interest rates could change significantly more than 100 basis points. There are inherent limitations in the sensitivity analysis presented, primarily due to the assumption that interest rate movements are linear and instantaneous. As a result, the analysis is unable to reflect the potential effects of more complex market changes that could arise, which may positively or negatively affect income.

Foreign Currency Risk

We are exposed to changes in currency rates as a result of our investments in foreign operations, revenues generated in currencies other than the U.S. dollar and foreign currency-denominated loans. Revenue and profit generated by international operations will increase or decrease compared to prior periods as a result of changes in foreign currency exchange rates. Refer to note 13 "Derivative Financial Instruments" to our consolidated financial statements in Part II, Item 8 of this Form 10-K for additional information regarding the changes in foreign currency exchange rates.

A hypothetical uniform 10% weakening in the value of the U.S. dollar relative to all the currencies in which our revenues and profits are denominated would result in a decrease to pretax income of approximately $34 million. The decrease results from a $59 million decrease related to euro-denominated term loans held by us. This decrease is partially offset by a $17 million increase related to foreign exchange on foreign currency earnings, assuming consistent operating results as the twelve months preceding September 30, 2015, and a $8 million increase related to foreign exchange on intercompany loans. Subsequent to December 31, 2015, we designated $750 million in Euro Term debt as a hedge, with changes in fair value recognized through accumulated other comprehensive income prospectively from the date of designation if the hedge remains effective. Subsequent to such designation, a 10% weakening in the value of the U.S. dollar relative to all other currencies in which our revenues and profits are denominated would have resulted in an increase to pretax income of approximately $24 million. There is inherent limitation in the sensitivity analysis presented, primarily due to the assumption that foreign exchange movements are linear and instantaneous. As a result, the analysis is unable to reflect the potential effects of more complex market changes that could arise, which may positively or negatively affect income.

Regulatory

Through its merchant alliances, the Global Business Solutions segment holds an ownership interest in several competing merchant acquiring businesses while serving as the electronic processor for those businesses. In order to satisfy state and federal antitrust requirements, we actively maintain an antitrust compliance program.

ITEM 8. FINANCIAL STATEMENTS AND SUPPLEMENTARY DATA

FIRST DATA CORPORATION

INDEX TO FINANCIAL STATEMENTS
COVERED BY REPORT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

First Data Corporation and Subsidiaries:

Consolidated Financial Statements:

Report of Ernst & Young LLP, Independent Registered Public Accounting Firm	57
Consolidated Statements of Operations for the years ended December 31, 2015, 2014, and 2013	58
Consolidated Statements of Comprehensive Income (Loss) for the years ended December 31, 2015, 2014, and 2013	59
Consolidated Balance Sheets as of December 31, 2015 and 2014	60
Consolidated Statements of Cash Flows for the years ended December 31, 2015, 2014, and 2013	61
Consolidated Statements of Equity for the years ended December 31, 2015, 2014, and 2013	62
Notes to the Consolidated Financial Statements	63

Schedules:

Schedule II—Valuation and Qualifying Accounts	108

Report of Independent Registered Public Accounting Firm

The Board of Directors and Stockholders of First Data Corporation

We have audited the accompanying consolidated balance sheets of First Data Corporation as of December 31, 2015 and 2014, and the related consolidated statements of operations, comprehensive income (loss), cash flows and equity for each of the three years in the period ended December 31, 2015. Our audits also include the financial statement schedule listed in the Index at Item 15(a). These financial statements and schedule are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements and schedule based on our audits.

We conducted our audits in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the consolidated financial position of First Data Corporation at December 31, 2015 and 2014, and the consolidated results of its operations and its cash flows for each of the three years in the period ended December 31, 2015, in conformity with U.S. generally accepted accounting principles. Also, in our opinion, the related financial statement schedule, when considered in relation to the basic financial statements taken as a whole, presents fairly in all material respects the information set forth therein.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), First Data Corporation's internal control over financial reporting as of December 31, 2015, based on criteria established in Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework) and our report dated February 25, 2015 expressed an unqualified opinion thereon.

/s/ Ernst & Young LLP

Atlanta, Georgia
February 25, 2016

FIRST DATA CORPORATION
CONSOLIDATED STATEMENTS OF OPERATIONS

(in millions, except per share and share amounts)	Year ended December 31, 2015	2014	2013
Revenues:			
Transaction and processing service fees (a)	$ 6,597	$ 6,510	$ 6,345
Product sales and other (a)	1,167	1,038	957
Total revenues (excluding reimbursable items)	7,764	7,548	7,302
Reimbursable PIN debit fees, postage, and other	3,687	3,604	3,507
Total revenues	11,451	11,152	10,809
Expenses:			
Cost of services (exclusive of items shown below)	2,871	2,668	2,723
Cost of products sold	356	330	328
Selling, general, and administrative	2,292	2,043	1,980
Depreciation and amortization	1,022	1,056	1,091
Other operating expenses	53	13	56
Total expenses (excluding reimbursable items)	6,594	6,110	6,178
Reimbursable PIN debit fees, postage, and other	3,687	3,604	3,507
Total expenses	10,281	9,714	9,685
Operating profit	1,170	1,438	1,124
Interest expense, net	(1,537)	(1,728)	(1,856)
Loss on debt extinguishment	(1,068)	(274)	(79)
Other income (expense)	29	161	(47)
Loss before income taxes and equity earnings in affiliates	(1,406)	(403)	(858)
Income tax expense	101	82	105
Equity earnings in affiliates	239	220	188
Net loss	(1,268)	(265)	(775)
Less: Net income attributable to noncontrolling interests and redeemable noncontrolling interest	213	193	177
Net loss attributable to First Data Corporation	$ (1,481)	$ (458)	$ (952)
Net loss per share, basic and diluted	$ (7.70)	$ (458,000)	$ (952,000)
Weighted-average shares used to compute basic and diluted net loss per share	192,263,793	1,000	1,000

(a) Includes processing fees, administrative service fees, and other fees charged to merchant alliances accounted for under the equity method of $205 million, $181 million, and $164 million for the years ended December 31, 2015, 2014, and 2013, respectively.

See notes to consolidated financial statements.

FIRST DATA CORPORATION
CONSOLIDATED STATEMENTS OF COMPREHENSIVE INCOME (LOSS)

(in millions)	Year ended December 31, 2015	2014	2013
Net loss	$ (1,268)	$ (265)	$ (775)
Other comprehensive income (loss), net of tax:			
Unrealized gains (losses) on securities	3	(7)	1
Pension liability adjustments	(13)	(36)	40
Foreign currency translation adjustment	(290)	(308)	(77)
Total other comprehensive loss, net of tax	(300)	(351)	(36)
Comprehensive loss	(1,568)	(616)	(811)
Less: Comprehensive income attributable to noncontrolling interests and redeemable noncontrolling interest	203	182	178
Comprehensive loss attributable to First Data Corporation	$ (1,771)	$ (798)	$ (989)

See notes to consolidated financial statements.

FIRST DATA CORPORATION
CONSOLIDATED BALANCE SHEETS

(in millions, except common stock share amounts)	As of December 31, 2015	As of December 31, 2014
ASSETS		
Current assets:		
Cash and cash equivalents	$ 429	$ 358
Accounts receivable, net of allowance for doubtful accounts of $71 and $62	1,826	1,741
Settlement assets	8,150	7,555
Other current assets	381	203
Total current assets	10,786	9,857
Property and equipment, net of accumulated depreciation of $1,367 and $1,233	951	930
Goodwill	16,846	17,017
Customer relationships, net of accumulated amortization of $5,299 and $4,871	2,136	2,604
Other intangibles, net of accumulated amortization of $2,134 and $1,965	1,783	1,745
Investment in affiliates	1,048	1,101
Other long-term assets	812	780
Total assets	$ 34,362	$ 34,034
LIABILITIES AND EQUITY		
Current liabilities:		
Accounts payable and accrued liabilities	$ 1,639	$ 1,796
Short-term and current portion of long-term borrowings	856	161
Settlement obligations	8,150	7,557
Total current liabilities	10,645	9,514
Long-term borrowings	18,737	20,697
Deferred tax liabilities	431	435
Other long-term liabilities	812	788
Total liabilities	30,625	31,434
Commitments and contingencies (See note 14)		
Redeemable noncontrolling interest	77	70
First Data Corporation stockholders' equity (deficit):		
Common stock, $0.01 par value; no shares and 1,000 shares authorized and issued as of December 31, 2015 and 2014, respectively	—	—
Class A Common stock, $0.01 par value; 1,600,000,000 shares and no shares authorized as of December 31, 2015 and 2014, respectively; 179,873,244 shares and no shares issued and outstanding as of December 31, 2015 and 2014, respectively	2	—
Class B Common stock, $0.01 par value; 800,000,000 shares and no shares authorized as of December 31, 2015 and 2014, respectively; 719,330,114 shares and no shares issued and outstanding as of December 31, 2015 and 2014, respectively	7	—
Additional paid-in capital	12,910	9,906
Accumulated loss	(11,032)	(9,547)
Accumulated other comprehensive loss	(1,219)	(929)
Total First Data Corporation stockholders' equity (deficit)	668	(570)
Noncontrolling interests	2,992	3,100
Total equity	3,660	2,530
Total liabilities and equity	$ 34,362	$ 34,034

See notes to consolidated financial statements.

FIRST DATA CORPORATION
CONSOLIDATED STATEMENTS OF CASH FLOWS

(in millions)	Year ended December 31, 2015	2014	2013
CASH FLOWS FROM OPERATING ACTIVITIES			
Net loss	$ (1,268)	$ (265)	$ (775)
Adjustments to reconcile to net cash provided by operating activities:			
Depreciation and amortization (including amortization netted against equity earnings in affiliates and revenues)	1,133	1,163	1,212
Charges (gains) related to other operating expenses and other income (expense)	24	(148)	103
Loss on debt extinguishment	1,068	274	79
Share-based compensation expense	329	51	39
Other non-cash and non-operating items, net	32	33	26
(Decrease) increase in cash, excluding the effects of acquisitions and dispositions, resulting from changes in:			
Accounts receivable, current and long-term	(184)	(50)	63
Other assets, current and long-term	(183)	(11)	(43)
Accounts payable and other liabilities, current and long-term	(162)	1	(1)
Income tax accounts	6	(13)	12
Net cash provided by operating activities	795	1,035	715
CASH FLOWS FROM INVESTING ACTIVITIES			
Proceeds from dispositions, net of expenses paid	4	270	18
Additions to property and equipment	(282)	(308)	(194)
Payments to secure customer service contracts, including outlays for conversion, and capitalized systems development costs	(320)	(259)	(185)
Acquisitions, net of cash acquired	(89)	(31)	(12)
Proceeds from sale of property and equipment	17	3	12
Purchase of investments	(17)	—	—
Other investing activities	2	(4)	8
Net cash used in investing activities	(685)	(329)	(353)
CASH FLOWS FROM FINANCING ACTIVITIES			
Short-term borrowings, net	(31)	12	(109)
Proceeds from issuance of long-term debt	10,258	1,830	4,472
Payment of call premiums and debt issuance cost	(1,062)	(355)	(111)
Principal payments on long-term debt	(11,568)	(3,751)	(4,506)
Proceeds from issuance of common stock	2,718	—	—
Distributions and dividends paid to noncontrolling interests and redeemable noncontrolling interest	(312)	(266)	(224)
Purchase of noncontrolling interest	—	(1)	(24)
Capital transactions with parent, net	(19)	1,788	(30)
Net cash used in financing activities	(16)	(743)	(532)
Effect of exchange rate changes on cash and cash equivalents	(23)	(30)	(13)
Change in cash and cash equivalents	71	(67)	(183)
Cash and cash equivalents at beginning of period	358	425	608
Cash and cash equivalents at end of period	$ 429	$ 358	$ 425
SUPPLEMENTAL CASH FLOW INFORMATION:			
Income tax payments, net of refunds received	$ 95	$ 96	$ 93
Interest paid	1,815	1,729	1,802
Distributions received from equity method investments	289	278	261
NON-CASH TRANSACTIONS:			
Capital leases, net of trade-ins	$ 83	$ 128	$ 112

See notes to consolidated financial statements.

FIRST DATA CORPORATION
CONSOLIDATED STATEMENTS OF EQUITY

(in millions, except common stock share amounts)	First Data Corporation Stockholders'								
	Common Stock								
	Class A		Class B		Additional Paid-In Capital	Accumulated Loss	Accumulated Other Comprehensive Income (Loss)	Noncontrolling Interest	Total
	Shares	Amount	Shares	Amount					
Balance, December 31, 2012 (a)	1,000	$ —	—	$ —	$ 7,341	$ (7,423)	$ (552)	$ 3,225	$2,591
Distributions and dividends paid to noncontrolling interests	—	—	—	—	—	—	—	(189)	(189)
Net (loss) income (b)	—	—	—	—	—	(952)	—	143	(809)
Other comprehensive (loss) income	—	—	—	—	—	—	(37)	1	(36)
Adjustments to redemption value of redeemable noncontrolling interest	—	—	—	—	(2)	—	—	—	(2)
Stock compensation expense and other	—	—	—	—	32	—	—	—	32
Capital contributed by Parent	—	—	—	—	7	—	—	—	7
Cash dividends paid by First Data Corporation to Parent	—	—	—	—	—	(28)	—	—	(28)
Purchase of noncontrolling interest	—	—	—	—	6	—	—	3	9
Balance, December 31, 2013 (a)	1,000	—	—	—	7,384	(8,403)	(589)	3,183	1,575
Distributions and dividends paid to noncontrolling interests	—	—	—	—	—	—	—	(231)	(231)
Net (loss) income (b)	—	—	—	—	—	(458)	—	159	(299)
Other comprehensive loss	—	—	—	—	—	—	(340)	(11)	(351)
Adjustments to redemption value of redeemable noncontrolling interest	—	—	—	—	(2)	—	—	—	(2)
Stock compensation expense and other	—	—	—	—	43	—	—	—	43
Capital contributed by Parent	—	—	—	—	2,482	—	—	—	2,482
Cash dividends paid by First Data Corporation to Parent	—	—	—	—	—	(686)	—	—	(686)
Purchase of noncontrolling interest	—	—	—	—	(1)	—	—	—	(1)
Balance, December 31, 2014 (a)	1,000	—	—	—	9,906	(9,547)	(929)	3,100	2,530
Distributions and dividends paid to noncontrolling interests	—	—	—	—	—	—	—	(277)	(277)
Net (loss) income (b)	—	—	—	—	—	(1,481)	—	179	(1,302)
Other comprehensive loss	—	—	—	—	—	—	(290)	(10)	(300)
Adjustment to redemption value of redeemable noncontrolling interest	—	—	—	—	(8)	—	—	—	(8)
Stock compensation expense and other	—	—	—	—	316	—	—	—	316
Cash dividends paid by First Data Corporation to Parent	—	—	—	—	—	(4)	—	—	(4)
Holding Company Merger (a)	(1,000)	—	719,330,114	7	(20)	—	—	—	(13)
Initial Public Offering	179,873,244	2	—	—	2,716	—	—	—	2,718
Balance, December 31, 2015	179,873,244	$ 2	719,330,114	$ 7	$ 12,910	$ (11,032)	$ (1,219)	$ 2,992	$3,660

(a) 1,000 shares relates to common stock without a class that was eliminated upon the merger with First Data Holdings.

(b) The total net loss presented in the consolidated statements of equity for the years ended December 31, 2015, 2014, and 2013 is $34 million in each year greater than the amount presented on the consolidated statements of operations due to the net income attributable to the redeemable noncontrolling interest not included in equity.

See notes to consolidated financial statements.

Note 1: Summary of Significant Accounting Policies

Business Description

First Data Corporation (FDC or the Company) is a global leader in commerce-enabling technology and solutions, for merchants, financial institutions, and card issuers. The services the Company provides include merchant transaction processing and acquiring; credit, retail, and debit card issuing and processing; prepaid services; and check verification, settlement and guarantee services. Over the last few years, the Company launched new products to help clients grow their businesses, including the Company's *Clover* line of payment solutions as well as other small and medium sized business (SMB) solutions including *Insightics*, cloud-based software to enable monitoring of key business metrics, and *Perka*, a digital loyalty marketing platform.

On October 15, 2015, the Company filed its Prospectus with the Securities and Exchange Commission pursuant to Rule 424(b). The Company issued 176,076,869 shares of Class A common stock and began trading on the New York Stock Exchange under the symbol "FDC". The net proceeds to the Company from the offering, after deducting underwriting discounts and commissions were $2.7 billion. The Company used the net proceeds from the offering to redeem all $510 million aggregate principal amount of its 11.25% senior unsecured notes due 2021, approximately $1.9 billion aggregate principal amount of its 12.625% senior unsecured notes due 2021, to pay applicable premiums and related fees and expenses, and for general corporate purposes.

On October 13, 2015, First Data Holdings Inc. (FDH), the Company's direct parent company, merged with and into First Data Corporation, with First Data Corporation being the surviving entity (HoldCo Merger). All outstanding shares of FDH were converted into Class B common stock, which are entitled to ten votes per share. All outstanding common stock of First Data Corporation were eliminated upon the merger. The Company accounted for the HoldCo Merger as a transfer of assets between entities under common control and reflected the transaction in its financial statements on a prospective basis.

On October 13, 2015, the Company amended its certificate of incorporation which affected a reverse stock split of the Company's authorized, issued and outstanding Class B common stock, on the basis of 1 new share of Class B common stock for each 3.16091 old shares of common stock. Note 4 "Stock Compensation Plans" of these consolidated financial statements has been retrospectively adjusted to reflect the impact of the reverse stock split. The shares on the Company's consolidated balance sheet have not been adjusted because the shares of First Data Corporation stock were not subject to the stock split.

Consolidation

The accompanying consolidated financial statements include the accounts of the Company and its controlled subsidiaries. All significant intercompany accounts and transactions have been eliminated. Investments in unconsolidated affiliated companies are accounted for under the equity method and are included in "Investment in affiliates" in the accompanying consolidated balance sheets. The Company generally utilizes the equity method of accounting when it has an ownership interest of between 20% and 50% in an entity, provided the Company is able to exercise significant influence over the investee's operations.

The Company consolidates an entity's financial statements when the Company has a controlling financial interest in the entity. Control is normally established when ownership interests exceed 50% in an entity; however, when the Company does not exercise control over a majority-owned entity as a result of other investors having rights over the management and operations of the entity, the Company accounts for the entity under the equity method. As of December 31, 2015 and 2014, there were no greater-than-50%-owned affiliates whose financial statements were not consolidated or entities that the Company owned less than 50% that are consolidated.

Use of Estimates

The preparation of financial statements in conformity with accounting principles generally accepted in the United States requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. Actual results could differ from those estimates.

Presentation

Depreciation and amortization presented as a separate line item on the Company's consolidated statements of operations does not include amortization of initial payments for new contracts which is recorded as a contra revenue within "Transaction and processing

service fees." Also not included is amortization related to equity method investments which is netted within the "Equity earnings in affiliates" line.

The following table presents the amounts associated with such amortization for the periods presented:

	Year ended December 31,		
(in millions)	2015	2014	2013
Amortization of initial payments for new contracts	$ 51	$ 45	$ 42
Amortization related to equity method investments	60	62	79

Revenue Recognition

The majority of the Company's revenues are comprised of: 1) transaction-based fees, which typically constitute a percentage of dollar volume processed; 2) fees per transaction processed; 3) fees per account on file during the period; or 4) some combination thereof.

In multiple-element transactions, revenue is allocated to the separate units of accounting provided each element has stand-alone value to the customer. Stand-alone value is based on the relative selling price of any undelivered items for which delivery is probable and substantially within the Company's control.

In the case of client contracts that the Company owns and manages, revenue is comprised of fees charged to the client, net of interchange and assessments charged by the credit card associations, and is recognized at the time the client accepts a point of sale transaction. The fees charged to the client are a percentage of the credit card and signature based debit card transaction's dollar value, a fixed amount or a combination of the two. Personal identification number based debit (PIN-debit) network fees are recognized in "Reimbursable PIN debit fees, postage, and other" revenues and expenses in the consolidated statements of operations. *STAR Network* access fees charged to clients are assessed on a per transaction basis. Interchange fees and assessments charged by credit card associations to the Company's consolidated subsidiaries and network fees related to PIN-debit transactions charged by debit networks are as follows for the periods presented:

	Year ended December 31,		
(in millions)	2015	2014	2013
Interchange fees and assessments	$ 21,711	$ 20,406	$ 19,368
PIN debit fees	2,991	2,965	2,915

The Company charges processing fees to its merchant alliances. In situations where an alliance is accounted for under the equity method, the Company's consolidated revenues include the processing fees charged to the alliance, as presented on the face of the consolidated statements of operations.

Revenue from check verification, settlement, and guarantee services is recognized at the time of sale less the fair value of the guarantee. The fair value of the guarantee is deferred and recognized at the later of the Company being called upon to honor the guarantee or the expiration of the guarantee. Check verification fees generally are a fixed amount per transaction while check guarantee fees generally are a percentage of the check amount.

The purchase and sale of merchant contracts is an ordinary element of the Company's businesses, and therefore, the gains from selling these revenue-generating assets are included within the "Product sales and other" component of revenues.

Fees based on cardholder accounts on file are recognized after the requisite services or period has occurred. Fees for PIN-debit transactions where the Company is the debit card processor for the financial institution are recognized on a per transaction basis. Revenues for output services are derived primarily on a per piece basis and consist of fees for the production, materials, and postage related to mailing finished products and recognized as the services are provided.

The sale and leasing of POS devices (terminals) are reported in "Product sales and other". Revenue for terminals sold or sold under a sales-type lease transaction is recognized when the following four criteria are met: evidence of an agreement exists, delivery has occurred, the selling price or minimum lease payments are fixed or determinable, and collection of the selling price or minimum lease payments is reasonably assured. Revenue for operating leases is recognized on a straight-line basis over the lease term.

Services not specifically described above are generally transaction based fees that are recognized at the time the transactions are processed or programming services that are recorded as work is performed.

The Company records deferred revenue when it receives payments or invoices in advance of the delivery of products or the performance of services. The deferred revenue is recognized into earnings when underlying performance obligations are achieved. As of December 31, 2015 and December 31, 2014, current deferred revenue included within "Accounts payable and accrued liabilities" in the Company's consolidated balance sheets was $140 million and $84 million, respectively. As of December 31, 2015 and December 31, 2014, noncurrent deferred revenue included within "Other long-term liabilities" in the Company's consolidated balance sheets was $146 million and $118 million, respectively.

Share-Based Compensation

Share-based compensation to employees is measured at the grant date fair values of the respective stock options and restricted stock awards. For awards without certain liquidity or employment triggers, expense is recognized over the requisite service periods and for awards with certain liquidity or employment triggers, expense is recognized upon the occurrence of such events. An estimate of forfeitures is applied when calculating compensation expense. The Company recognizes compensation cost on awards with graded vesting on a straight-line basis over the requisite service period for the entire award. Refer to note 4 "Stock Compensation Plans" of these consolidated financial statements for details regarding the Company's share-based compensation plan.

Foreign Currency Translation

The U.S. dollar is the functional currency for most of the Company's U.S.-based businesses and certain foreign-based businesses. Significant operations with a local currency as their functional currency include operations in the United Kingdom, Australia, Germany, Ireland, Greece, and Argentina. Foreign currency-denominated assets and liabilities for these units and other less significant operations are translated into U.S. dollars based on exchange rates prevailing at the end of the period, and revenues and expenses are translated at average exchange rates during each monthly period. The effects of foreign exchange gains and losses arising from the translation of assets and liabilities of those entities where the functional currency is not the U.S. dollar are included as a component of Other Comprehensive Income (OCI). Intercompany loans are generally not considered invested on a long-term basis and such foreign currency gains and losses are recorded in income. Transaction gains and losses related to operating assets and liabilities are included in the "Cost of services" and "Selling, general, and administrative" lines of the consolidated statements of operations and were immaterial. Non-operating transaction gains and losses derived from non-operating assets and liabilities are included in the "Other income (expense)" line of the consolidated statements of operations and are separately disclosed in note 16 "Supplemental Financial Information" of these consolidated financial statements.

Derivative Financial Instruments

The Company is exposed to various financial and market risks, including those related to changes in interest rates and foreign currency exchange rates, that exist as part of its ongoing business operations. The Company uses derivative instruments (i) to mitigate cash flow risks with respect to changes in interest rates (forecasted interest payments on variable rate debt), (ii) to maintain a desired ratio of fixed rate and floating rate debt, and (iii) to protect the net investment in certain foreign subsidiaries and/or affiliates with respect to changes in foreign currency exchange rates. The Company's objective is to engage in risk management strategies that provide adequate downside protection.

Derivative instruments are entered into for periods consistent with related underlying exposures. The Company applies strict policies to manage each of these risks, including prohibition against derivatives trading, derivatives market-making or any other speculative activities. Although most of the Company's derivatives either do not qualify or are not designated for hedge accounting, they are maintained for economic hedge purposes and are not considered speculative.

The Company formally documents all relationships between hedging instruments and the underlying hedged items, as well as its risk management objective and strategy for undertaking various hedge transactions. This process includes linking all derivatives that have been designated as cash flow hedges to forecasted transactions and net investment hedges to the underlying investment in a foreign subsidiary or affiliate. For designated hedges, the Company formally assesses, both at inception of the hedge and on an ongoing basis, whether the hedge is highly effective in offsetting changes in cash flows or foreign currency exposure of the underlying hedged items. The Company also performs an assessment of the probability of the forecasted transactions on a periodic basis. If it is determined that a derivative ceases to be highly effective during the term of the hedge or if the forecasted transaction is no longer probable, the Company discontinues hedge accounting prospectively for such derivative.

The Company monitors the financial stability of its derivative counterparties and all counterparties remain highly-rated (in the "A" category or higher). The credit risk inherent in these agreements represents the possibility that a loss may occur from the nonperformance of a counterparty to the agreements. The Company performs a review at inception of the hedge, as circumstances warrant, and at least on a quarterly basis, of the credit risk of these counterparties. The Company also monitors the concentration

of its contracts with individual counterparties. The Company's exposures are in liquid currencies (primarily in U.S. dollars, euros, Australian dollars, British pounds, and Canadian dollars), so there is minimal risk that appropriate derivatives to maintain the hedging program would not be available in the future.

The Company recognizes all derivative financial instruments in the consolidated balance sheets as assets or liabilities at fair value. Such amounts are recorded in "Other current assets", "Other long-term assets", "Accounts payable and accrued liabilities" or "Other long-term liabilities" in the consolidated balance sheets. The Company's policy is to present all derivative balances on a gross basis, without regard to counterparty master netting agreements or similar arrangements. Changes in fair value of derivative instruments are recognized immediately in earnings unless the derivative is designated and qualifies as a hedge of future cash flows or a hedge of a net investment in a foreign operation. For derivatives that qualify as hedges of future cash flows, the effective portion of changes in fair value is recorded temporarily in equity as a component of OCI and then recognized in earnings in the same period or periods during which the hedged item affects earnings. For derivatives that qualify as a hedge of a net investment in a foreign operation, the gain or loss is reported in OCI as part of the cumulative translation adjustment to the extent the hedge is effective. Any ineffective portions of cash flow hedges and net investment hedges are recognized in the "Other income (expense)" line in the consolidated statements of operations during the period of change. Additional discussion of derivative instruments is provided in note 13 "Derivative Financial Instruments" of these consolidated financial statements.

Noncontrolling and Redeemable Noncontrolling Interests

Noncontrolling interests represent the minority shareholders' share of the net income or loss and equity in consolidated subsidiaries. Substantially all of the Company's noncontrolling interests are presented pretax in the consolidated statements of operations as "Net income attributable to noncontrolling interests and redeemable noncontrolling interest" because the majority of the Company's non wholly owned consolidated subsidiaries are flow through entities for tax purposes. Noncontrolling interests are presented as a component of equity in the consolidated balance sheets and reflect the original investments by these noncontrolling shareholders in the consolidated subsidiaries, along with their proportionate share of the earnings or losses of the subsidiaries, net of dividends or distributions. Noncontrolling interests that are redeemable at the option of the holder are presented outside of equity and are carried at their estimated redemption value. Refer to note 5 "Stockholders' Equity and Redeemable Noncontrolling Interest" of these consolidated financial statements for more information. A noncontrolling interest is recorded on the date of acquisition based on the total fair value of the acquired entity and the noncontrolling interest's share of that value.

Reserve for Merchant Credit Losses and Check Guarantees

With respect to the merchant acquiring business, the Company's merchant customers (or those of its unconsolidated alliances) have the liability for any charges properly reversed by the cardholder. In the event, however, that the Company is not able to collect such amounts from the merchants due to merchant fraud, insolvency, bankruptcy or another reason, the Company may be liable for any such reversed charges. The Company's risk in this area primarily relates to situations where the cardholder has purchased goods or services to be delivered in the future such as airline tickets.

The Company's obligation to stand ready to perform is minimal in relation to the total dollar volume processed. The Company requires cash deposits, guarantees, letters of credit or other types of collateral from certain merchants to minimize this obligation. Collateral held by the Company is classified within "Settlement assets" and the obligation to repay the collateral if it is not needed is classified within "Settlement obligations" on the Company's consolidated balance sheets. The Company also utilizes a number of systems and procedures to manage merchant risk. Despite these efforts, the Company historically has experienced some level of losses due to merchant defaults.

The Company's contingent obligation relates to imprecision in its estimates of required collateral. A provision for this obligation is recorded based primarily on historical experience of credit losses and other relevant factors such as economic downturns or increases in merchant fraud. Merchant credit losses are included in "Cost of services" in the Company's consolidated statements of operations. The amount of the reserves attributable to entities consolidated by the Company was $22 million and $20 million as of December 31, 2015 and 2014, respectively.

The majority of the *TeleCheck* business involves the guarantee of checks received by merchants. If the check is returned, TeleCheck is required to purchase the check from the merchant at its face value and pursue collection from the check writer. A provision for estimated check returns, net of anticipated recoveries, is recorded at the transaction inception based on recent history. The following table presents the accrued warranty and recovery balances:

(in millions)	As of December 31, 2015	2014
Accrued warranty balances	$ 6	$ 9
Accrued recovery balances	21	25

Accrued warranties are included in "Accounts payable and accrued liabilities" and accrued recoveries are included in "Accounts receivable, net" in the consolidated balance sheets. The maximum potential future payments under the guarantees were estimated by the Company to be approximately $903 million as of December 31, 2015 which represented an estimate of the total uncleared checks at that time.

Income Taxes

The Company and its domestic subsidiaries file a consolidated U.S. income tax return. The Company's foreign operations file income tax returns in their local jurisdictions. Income taxes are computed in accordance with current accounting guidance and reflect the net tax effects of temporary differences between the financial reporting carrying amounts of assets and liabilities and the corresponding income tax amounts. The Company has deferred tax assets and liabilities and maintains valuation allowances where it is more likely than not that all or a portion of deferred tax assets will not be realized. To the extent the Company determines that it will not realize the benefit of some or all of its deferred tax assets, then these deferred tax assets will be adjusted through the Company's provision for income taxes in the period in which this determination is made.

The Company recognizes the tax benefits from uncertain tax positions only when it is more likely than not, based on the technical merits of the position, that the tax position will be sustained upon examination, including the resolution of any related appeals or litigation. The tax benefits recognized in the consolidated financial statements from such a position are measured as the largest benefit that has a greater than fifty percent likelihood of being realized upon ultimate resolution.

Cash and Cash Equivalents

Investments (other than those included in settlement assets) with original maturities of three months or less (that are readily convertible to cash) are considered to be cash equivalents and are stated at cost, which approximates market value. Cash and cash equivalents that were restricted from use due to regulatory requirements are included in "Other long-term assets" in the consolidated balance sheets and were immaterial as of December 31, 2015 and 2014.

Accounts Receivable and Leasing Receivables

Accounts receivable balances are stated net of allowance for doubtful accounts. Historically, the Company has infrequently incurred significant write-offs. The Company records allowances for doubtful accounts when it is probable that the accounts receivable balance will not be collected. Long-term accounts receivable balances are included in "Other long-term assets" in the consolidated balance sheets.

The Company has receivables associated with its POS terminal leasing businesses. Leasing receivables are included in "Accounts receivable" and "Other long-term assets" in the consolidated balance sheets. The Company recognizes interest income on its leasing receivables using the effective interest method. Interest income from leasing receivables is included in "Product sales and other" in the consolidated statements of operations. For direct financing leases, the interest rate used incorporates initial direct costs included in the net investment in the lease. For sales type leases, initial direct costs are expensed as incurred.

Property and Equipment

Property and equipment are stated at cost less accumulated depreciation. Depreciation expense is computed using the straight-line method over the lesser of the estimated useful life of the related assets (generally three years to 10 years for equipment, furniture, and leasehold improvements, and 30 years for buildings) or the lease term. Maintenance and repairs which do not extend the useful life of the respective assets are charged to expense as incurred. The following table presents the amounts charged to expense for the depreciation and amortization of property and equipment, including equipment under capital lease:

Year ended December 31, (in millions)	Amount
2015	$ 290
2014	286
2013	288

Goodwill and Other Intangibles

Goodwill represents the excess of purchase price over tangible and intangible assets acquired less liabilities assumed arising from business combinations. Goodwill is generally allocated to reporting units based upon relative fair value (taking into consideration other factors such as synergies) when an acquired business is integrated into multiple reporting units. The Company's reporting units are at the operating segment level or one level below the operating segment level for which discrete financial information is prepared and regularly reviewed by management. When a business within a reporting unit is disposed of, goodwill is allocated to the disposed business using the relative fair value method. Relative fair value is estimated using a discounted cash flow analysis.

The Company tests goodwill annually for impairment, as well as upon an indicator of impairment, using a fair value approach at the reporting unit level. The Company estimates the fair value of each reporting unit using a discounted cash flow analysis. The Company performed its annual goodwill impairment test in the fourth quarters of 2015 and 2014. As of October 1, 2015, the most recent impairment analysis date, the fair value of each reporting unit exceeded its carrying value. The Company did not record any goodwill impairment charges in 2015 or 2014.

Customer relationships represent the estimated value of the Company's relationships with customers, primarily merchants and financial institutions, to which it provides services. Customer relationships are amortized based on the pattern of undiscounted cash flows for the period as a percentage of total projected undiscounted cash flows. The Company selected this amortization method for these customer relationships based on a conclusion that the projected undiscounted cash flows could be reliably determined.

The Company capitalizes initial payments for new contracts, contract renewals, and conversion costs associated with customer processing relationships to the extent recoverable through cash flows from future operations, contractual minimums, and/or penalties in the case of early termination. The Company's accounting policy is to limit the amount of capitalized costs for a given contract to the lesser of the estimated ongoing future cash flows from the contract or the termination fees the Company would receive in the event of early termination of the contract by the customer. The initial payments for new contracts and contract renewals are amortized over the term of the contract as a reduction of the associated revenue (transaction and processing service fees). Conversion costs are also amortized over the term of the contract but are recorded as an expense in "Depreciation and amortization" in the consolidated statements of operations.

The Company develops software that is used in providing processing services to customers. To a lesser extent, the Company also develops software to be sold or licensed to customers. Costs incurred during the preliminary project stage are expensed as incurred. Capitalization of costs begins when the preliminary project stage is completed and management, with the relevant authority, authorizes and commits to funding the project and it is probable that the project will be completed and the software will be used to perform the function intended. Capitalization of costs ceases when the software is substantially complete and ready for its intended use. Software development costs are amortized using the straight-line method over the estimated useful life of the software, which is generally 5 years. Software acquired in connection with business combinations is amortized using the straight-line method over the estimated useful life of the software which generally ranges from three years to 10 years.

In addition to capitalized contract and software development costs, other intangibles include copyrights, patents, purchased software, trademarks, and non-compete agreements acquired in business combinations. Other intangibles, except for the First Data trade name discussed in note 3 "Goodwill and Other Intangibles" of these consolidated financial statements, are amortized on a straight-line basis over the length of the contract or benefit period, which generally ranges from three years to 25 years.

Assets and Liabilities Measured at Fair Value on a Recurring Basis

Fair value is defined by accounting guidance as the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date. The Company uses the hierarchy prescribed in the accounting guidance for fair value measurements, based upon the available inputs to the valuation and the degree to which they are observable or not observable in the market. The Company maximizes the use of relevant observable inputs and minimizes the use of unobservable inputs. The three levels in the hierarchy are as follows:

- Level 1 Inputs—Quoted prices (unadjusted) for identical assets or liabilities in active markets that are accessible as of the measurement date.
- Level 2 Inputs—Inputs other than quoted prices within Level 1 that are observable either directly or indirectly, including but not limited to quoted prices in markets that are not active, quoted prices in active markets for similar assets or liabilities, and observable inputs other than quoted prices such as interest rates or yield curves.

- Level 3 Inputs—Unobservable inputs reflecting the Company's own assumptions about the assumptions that market participants would use in pricing the asset or liability, including assumptions about risk.

Assets and Liabilities Measured at Fair Value on a Non-Recurring Basis

During the years ended December 31, 2015 and 2014, the Company did not record any adjustments over $5 million to the carrying value of existing assets based on non-recurring fair value measurements.

Net Loss Per Share

Basic net loss per share is calculated by dividing net loss by the weighted-average shares outstanding during the period, without consideration for any potential dilutive shares. For any period where Net loss attributable to First Data Corporation is presented, shares used in the diluted EPS calculation represent basic shares because using diluted shares would be anti-dilutive to the calculation.

Reclassifications

Certain amounts for prior years have been reclassified to conform with the current-year financial statement presentation.

New Accounting Guidance

In May 2014, the Financial Accounting Standards Board (FASB) issued guidance that requires companies to recognize revenue to depict the transfer of goods or services to customers in amounts that reflect the consideration to which the company expects to be entitled in an exchange for those goods or services. It also requires enhanced disclosures about revenue, provides guidance for transactions that were not previously addressed comprehensively, and improves guidance for multiple-element arrangements. The guidance applies to any entity that either enters into contracts with customers to transfer goods or services or enters into contracts for the transfer of nonfinancial assets unless those contracts are within the scope of other standards. As amended in August 2015, the guidance is effective for public companies for annual periods beginning after December 15, 2017 as well as interim periods within those annual periods using either the full retrospective approach or modified retrospective approach. The FASB also permitted early adoption of the standard, but not before December 15, 2016. The Company is currently evaluating the impacts of the new guidance on its consolidated financial statements.

In April 2015, the FASB issued guidance that requires companies to present debt issuance costs related to a recognized debt liability on the balance sheet as a direct deduction from the debt liability, similar to the presentation of debt discounts. Debt issuance costs will continue to be amortized to interest expense using the effective interest method. The Company early adopted, on a retrospective basis, the standard to all periods presented within the consolidated financial statements. The adoption did not have a material impact on the Company's consolidated financial statements. For quantification of the impact of adoption, refer to note 2 "Borrowings" of these consolidated financial statements.

In November 2015, the FASB issued guidance that requires companies to classify all deferred tax assets and liabilities as noncurrent on the balance sheet instead of separating deferred taxes into current and noncurrent amounts. The Company early adopted, on a retrospective basis, the standard to all periods presented within the consolidated financial statements. The adoption resulted in all deferred tax assets and liabilities being presented as noncurrent on the consolidated balance sheets. For quantification of the impact of adoption, refer to note 8 "Income Taxes" of these consolidated financial statements.

Note 2: Borrowings

(in millions)	As of December 31, 2015	2014
Short-term borrowings:		
Foreign lines of credit and other arrangements	$ 43	$ 68
Senior secured revolving credit facility	—	10
Total Short-term borrowings	43	78
Current portion of long-term borrowings:		
8.75% Senior secured second lien notes due 2022 (a)	750	—
4.95% Unsecured notes due 2015	—	10
Unamortized discount and unamortized deferred financing costs (b)	(10)	—
Capital lease obligations	73	73
Total Current portion of long-term borrowings	813	83
Total Short-term and current portion of long-term borrowings	856	161
Long-term borrowings:		
Senior secured term loan facility due March 2017 at LIBOR and euro LIBOR plus 3.5% or, solely with respect to U.S. dollar-denominated term loans, a base rate plus 2.5%	—	1,461
Senior secured term loan facility due March 2018 at LIBOR and euro LIBOR plus 3.5% or, solely with respect to U.S. dollar-denominated term loans, a base rate plus 2.5%	4,938	4,977
Senior secured term loan facility due September 2018 at LIBOR plus 3.5% or a base rate plus 2.5%	1,008	1,008
Senior secured term loan facility due March 2021 at LIBOR and euro LIBOR plus 4.0% or, solely with respect to U.S. dollar-denominated term loans, a base rate plus 3.0%	1,171	1,191
Senior secured term loan facility due July 2022 at LIBOR and euro LIBOR plus 3.75% or, solely with respect to U.S. dollar-denominated term loans, a base rate plus 2.75%	2,464	—
7.375% Senior secured first lien notes due 2019	—	1,595
8.875% Senior secured first lien notes due 2020	—	510
6.75% Senior secured first lien notes due 2020	1,398	1,398
5.375% Senior secured first lien notes due 2023	1,210	—
5.0% Senior secured first lien notes due 2024	1,000	—
8.25% Senior secured second lien notes due 2021	—	2,000
8.75% Senior secured second lien notes due 2022	—	1,000
5.75% Senior secured second lien notes due 2024	2,200	—
12.625% Senior unsecured notes due 2021	—	3,000
10.625% Senior unsecured notes due 2021	—	530
11.25% Senior unsecured notes due 2021	—	510
7.0% Senior unsecured notes due 2023	3,400	—
11.75% Senior unsecured subordinated notes due 2021	—	1,609
Unamortized discount and unamortized deferred financing costs (b) (c)	(174)	(226)
Capital lease obligations	122	134
Total Long-term borrowings	18,737	20,697
Total Borrowings (d) (e)	$ 19,593	$ 20,858

(a) On November 16, 2015, the Company exercised its option to call for early redemption of its outstanding 8.75% Senior secured second lien notes due 2022. The notes were subsequently redeemed on January 15, 2016. Refer to "8.25% and 8.75% Senior Secured Second Lien Notes" below for additional information.

(b) Unamortized deferred financing costs are amortized on a straight-line basis, which approximates the interest method, over the remaining term of the respective debt. In addition, certain lenders fees associated with debt transactions were capitalized as discounts and are similarly being amortized on a straight-line basis, which approximates the effective interest method, over the remaining term of the respective debt.

(c) Unamortized deferred financing costs include $62 million as of December 31, 2014 that was previously recorded as an asset within "Other long-term assets" on the Company's consolidated balance sheets. Refer to note 1 "Summary of Significant Accounting Policies " of these consolidated financial statements for additional information on the change in accounting principle based upon the adoption of new accounting guidance.

(d) As of December 31, 2015 and 2014, the fair value of the Company's long-term borrowings was $19.6 billion and $22.1 billion, respectively. The estimated fair value of the Company's long-term borrowings was primarily based on market trading prices and is considered to be a Level 2 measurement.

(e) The effective interest rate is not substantially different than the coupon rate on any of the Company's debt tranches

Foreign Lines of Credit and Other Arrangements

As of December 31, 2015 and 2014, the Company had approximately $245 million and $349 million, respectively, available under short-term lines of credit and other arrangements with foreign banks and alliance partners primarily to fund settlement activity. As of December 31, 2015 and 2014, the Company had a $75 million and $150 million, respectively, committed line of credit for one of its U.S. alliances and the remainder of these arrangements is primarily associated with international operations and are in various functional currencies, the most significant of which are the Australian dollar, the Polish zloty, and the euro. Of the amounts outstanding as of December 31, 2015 and 2014, $17 million and $67 million were uncommitted. The weighted average interest rate associated with foreign lines of credit was 2.6% and 3.2% for the years ended December 31, 2015 and 2014, respectively. Commitment fees for the committed foreign lines of credit range from 0.16% to 0.8%.

Senior Secured Revolving Credit Facility

On June 2, 2015, the Company terminated and replaced its previous $1.0 billion senior secured revolving credit facility maturing September 24, 2016 with a new $1.25 billion senior secured revolving credit facility maturing on June 2, 2020 subject to certain earlier springing maturity provisions in certain circumstances. Up to $250 million of the new senior secured revolving credit facility is available for letters of credit of which $42 million and $43 million of letters of credit were issued under these facilities as of December 31, 2015 and 2014, respectively. As of December 31, 2015, $1.2 billion remained available.

Interest on the new senior secured revolving credit facility is payable at a rate equal to, at Company's option, either (a) LIBOR for deposits in the applicable currency plus 350 basis points or (b) solely with respect to revolving loans denominated in U.S. dollars, a base rate plus 250 basis points. The weighted-average interest rate on these facilities was 4.60% and 5.14% for the years ended December 31, 2015 and 2014, respectively. The commitment fee rate for the unused portion of the new facility is 0.50% per year, though it may be reduced by the Company's leverage ratio.

Senior Secured Term Loan Facility

The Company has amounts outstanding under its senior secured term loan facility under separate tranches as described below. A portion of each tranche is denominated in euro with the exception of the September 2018 term loan. Interest is payable based upon LIBOR or euro LIBOR plus an applicable margin.

As of December 31, 2015, the Company held interest rate swaps to mitigate exposure to variability in interest payments on the outstanding variable rate senior secured term loan. Refer to note 13 "Derivative Financial Instruments" of these consolidated financial statements for a discussion of the Company's derivatives.

The original terms of the Company's senior secured term loan facility required the Company to pay equal quarterly installments in aggregate annual amounts equal to 1% of the original principal amount. However, in conjunction with debt modifications and amendments over the last several years, proceeds from the issuance of the notes were used to prepay portions of the principal balances of the Company's senior secured term loans which satisfied the future quarterly principal payments. Therefore, the Company made no scheduled principal payments during 2015 or 2014.

The senior secured term loan facility also requires mandatory prepayments based on a percentage of excess cash flow generated by the Company. All obligations under the senior secured loan facility are fully and unconditionally guaranteed by most of the domestic, wholly owned material subsidiaries of the Company, subject to certain exceptions.

On January 1, 2016, the Company designated the euro-denominated portions of the Senior secured term loan facility due March 2018, Senior secured term loan facility due March 2021, and the July 2015 issuance of the Senior secured term loan facility due July 2022 as non-derivative hedges of net investments in foreign operations. As such, foreign currency gains and losses on the euro-denominated portions of these terms loans will be recorded within Foreign currency translation adjustment on the Company's consolidated statements of comprehensive income (loss) to the extent the hedges are effective. Foreign currency gains and losses on the euro-denominated portions of these term loans were previously recorded within Other income (expense) on the Company's consolidated statements of operations.

Senior Secured Term Loan Facility Due March 2017

The Company used the proceeds from the amendment of the Senior secured term loan facility due July 2022 in November 2015, discussed below, to redeem its outstanding Senior secured term loan facility due March 2017. Associated with the redemption, the Company incurred $5 million in loss on debt extinguishment.

Senior Secured Term Loan Facility Due July 2022

On July 10, 2015, the Company entered into an amendment of its senior secured credit facilities providing for $725 million in U.S. dollar-denominated term loans and €250 million in euro-denominated term loans maturing in July 2022 (July 2022 Term Loan).

The proceeds from the July 10, 2015 issuance of the July 2022 Term Loan were used to redeem $955 million of the Company's 7.375% senior secured first lien notes due 2019 and to pay related fees and expenses.

On November 24, 2015, the Company entered into an amendment of its senior secured credit facilities providing for an additional $1.3 billion in U.S. dollar-denominated term loans and €200 million in euro-denominated term loans maturing in July 2022 (Additional July 2022 Term Loan).

The euro-denominated portion of the Additional July 2022 Term Loan was designated by the Company as a non-derivative hedge of net investments in foreign operations. As such, foreign currency gains and losses on the euro-denominated portion of the Additional July 2022 Term Loan are recorded within Foreign currency translation adjustment on the Company's consolidated statements of comprehensive income (loss) to the extent the hedge is effective.

The proceeds from the issuance of the Additional July 2022 Term Loan were used to redeem the Company's outstanding Senior secured term loan facility due March 2017 and to pay related fees and expenses.

7.375% Senior Secured First Lien Notes

The Company used proceeds from the issuance of the July 2022 Term Loan, discussed above, to redeem $955 million of the Company's outstanding 7.375% senior secured first lien notes. Associated with the redemption, the Company incurred $45 million in loss on debt extinguishment.

The Company used proceeds from the issuance of its 5.375% senior secured first lien notes due 2023, discussed below, to redeem the remaining outstanding 7.375% senior secured first lien notes. Associated with the redemption, the Company incurred $31 million in loss on debt extinguishment.

8.875% Senior Secured First Lien Notes

The Company used proceeds from the issuance of its 5.375% senior secured first lien notes due 2023, discussed below, to redeem all outstanding 8.875% senior secured first lien notes. Associated with the redemption, the Company incurred $32 million in loss on debt extinguishment.

5.375% Senior Secured First Lien Notes

On August 11, 2015, the Company issued approximately $1.2 billion aggregate principal amount of 5.375% senior secured first lien notes due August 15, 2023. Interest on the notes will be payable semi-annually in cash on February 15 and August 15 of each year, commencing on February 15, 2016. The Company used the proceeds from the offering to redeem and repurchase all outstanding 7.375% senior secured first lien notes due 2019 and 8.875% senior secured first lien notes due 2020 and pay related fees and expenses.

The Company may redeem the notes, in whole or in part, prior to August 15, 2018 at a price equal to 100% of the notes redeemed plus accrued and unpaid interest to the redemption date and a "make-whole premium". Thereafter, the Company may redeem the notes, in whole or in part, at established redemption prices.

5.0% Senior Secured First Lien Notes

On November 25, 2015, the Company issued $1.0 billion aggregate principal amount of 5.0% senior secured first lien notes due January 15, 2024. Interest on the notes will be payable semi-annually in cash on January 15 and July 15 of each year, commencing on July 15, 2016. The Company used the proceeds from the offering together with proceeds from the November 25, 2015 offering of its 5.75% senior secured second lien notes to redeem $250 million of its outstanding 8.75% senior secured second lien notes due 2022 and all outstanding 8.25% second lien notes due 2021 and pay related fees and expenses.

The Company may redeem the notes, in whole or in part, prior to January 15, 2019 at a price equal to 100% of the notes redeemed plus accrued and unpaid interest to the redemption date and a "make-whole premium". Thereafter, the Company may redeem the notes, in whole or in part, at established redemption prices.

8.25% and 8.75% Senior Secured Second Lien Notes

The Company used proceeds from the issuance of its 5.0% senior secured first lien notes due 2024, discussed above, and 5.75% senior secured second lien notes due 2024, discussed below, to redeem all outstanding 8.25% second lien notes and $250 million of the Company's 8.75% senior secured second lien notes. Associated with the redemption, the Company incurred $138 million in loss on debt extinguishment.

On January 15, 2016, the Company redeemed its remaining outstanding 8.75% senior secured second lien notes. Associated with the redemption, the Company incurred $43 million in loss on debt extinguishment.

5.75% Senior Secured Second Lien Notes

On November 25, 2015, the Company issued $2.2 billion aggregate principal amount of 5.75% senior secured second lien notes due January 15, 2024. Interest on the notes will be payable semi-annually in cash on January 15 and July 15 of each year, commencing on July 15, 2016. The Company used the proceeds from the offering together with proceeds from the November 25, 2015 offering of its 5.0% senior secured first lien notes to redeem $250 million of its outstanding 8.75% senior secured second lien notes due 2022 and all outstanding 8.25% second lien notes due 2021 and pay related fees and expenses.

The Company may redeem the notes, in whole or in part, prior to January 15, 2019 at a price equal to 100% of the notes redeemed plus accrued and unpaid interest to the redemption date and a "make-whole premium". Thereafter, the Company may redeem the notes, in whole or in part, at established redemption prices.

12.625% Senior Unsecured Notes

The Company used proceeds from its initial public offering and proceeds from the issuance of its 7.0% senior unsecured notes due 2023, discussed below, to redeem all outstanding 12.625% senior unsecured notes. Associated with the redemption, the Company incurred $466 million in loss on debt extinguishment.

10.625% Senior Unsecured Notes Due 2021

The Company used proceeds from the issuance of its 7.0% senior secured first lien notes due 2023, discussed below, to redeem all outstanding 10.625% senior unsecured notes due 2021. Associated with the redemption, the Company incurred $62 million in loss on debt extinguishment.

11.25% Senior Unsecured Notes Due 2021

The Company used proceeds from its initial public offering to redeem all outstanding 11.25% senior unsecured notes due 2021. Associated with the redemption, the Company incurred $62 million in loss on debt extinguishment.

7.0% Senior Unsecured Notes Due 2023

On November 18, 2015, the Company issued $3.4 billion aggregate principal amount of 7.0% senior unsecured notes due December 1, 2023. Interest on the notes will be payable semi-annually in cash on June 1 and December 1 of each year, commencing on June 1, 2016. The Company used the proceeds from the offering to redeem its outstanding 12.625% senior unsecured notes due 2021, 10.625% senior unsecured notes due 2021, and 11.75% senior subordinated notes due 2021 and pay related fees and expenses.

The Company may redeem the notes, in whole or in part, prior to December 1, 2018 at a price equal to 100% of the notes redeemed plus accrued and unpaid interest to the redemption date and a "make-whole premium". Thereafter, the Company may redeem the notes, in whole or in part, at established redemption prices.

11.75% Senior Unsecured Subordinated Notes Due 2021

The Company used proceeds from the issuance of its 7.0% unsecured notes due 2023, discussed above, to redeem all outstanding 11.75% senior unsecured subordinated notes due 2021. Associated with the redemption, the Company incurred $227 million in loss on debt extinguishment.

Accounts receivable securitization agreement

On December 31, 2015, the Company established a new fully consolidated and wholly owned subsidiary, First Data Receivables, LLC (FDR). FDR and FDC entered into an agreement where certain wholly owned subsidiaries of FDC agreed to transfer and contribute receivables to FDR. FDR's assets are not available to satisfy obligations of any other entities or affiliates of FDC. FDR's creditors will be entitled, upon its liquidation, to be satisfied out of FDR's assets prior to any assets or value in FDR becoming available to FDR's equity holders. FDR entered into an agreement with an external party, which expires in 2019, to borrow $240 million secured by liens on the receivables contributed to FDR by the wholly owned subsidiaries of FDC. Loans under the Agreement bear interest based upon LIBOR plus 200 basis points or a base rate equal to the highest of (i) the applicable lender's prime rate, or (ii) the federal funds rate plus 0.50%. As of December 31, 2015, the Company had no debt outstanding under the Securitization Agreement. In January 2016, FDC and its wholly-owned subsidiaries initially transferred approximately $326 million in receivables to FDR as part of its Securitization Program. FDR utilized the receivables as collateral in borrowings of $240 million under this agreement. The $240 million in gross proceeds was utilized to redeem a portion of the Company's 8.75% senior secured second lien notes on January 15, 2016.

Maturities

The following table presents the future aggregate annual maturities of long-term debt excluding unamortized discounts and deferred financing costs:

Year ended December 31, (in millions)	Par Amount
2016	$ 823
2017	75
2018	5,973
2019	11
2020	1,399
Thereafter	11,453
Total	$ 19,734

Guarantees and Covenants

All obligations under the senior secured revolving credit facility and senior secured term loan facility are unconditionally guaranteed by most of the existing and future, direct and indirect, wholly owned, material domestic subsidiaries of the Company. The senior secured facilities contain a number of covenants that, among other things, restrict the Company's ability to incur additional indebtedness; create liens; enter into sale and leaseback transactions; engage in mergers or consolidations; sell or transfer assets; pay dividends and distributions or repurchase the Company's capital stock; make investments, loans or advances; prepay certain indebtedness; make certain acquisitions; engage in certain transactions with affiliates; amend material agreements governing certain indebtedness; and change its lines of business. The senior secured facilities also require the Company to not exceed a maximum senior secured leverage ratio and contain certain customary affirmative covenants and events of default, including a change of control. The senior secured term loan facility also requires mandatory prepayments based on a percentage of excess cash flow generated by the Company. The Company is in compliance with all applicable covenants.

All senior secured notes are guaranteed on a senior secured basis by each of the Company's existing and future direct and indirect wholly owned domestic subsidiaries that guarantees the Company's senior secured credit facilities. Each of the guarantees of the notes is a general senior obligation of each guarantor and rank senior in right of payment to all existing and future subordinated indebtedness of the guarantor subsidiary, including the Company's existing senior subordinated notes. The notes rank equal in right of payment with all existing and future senior indebtedness of the guarantor subsidiary but are effectively senior to the guarantees of the Company's existing senior unsecured notes and the Company's existing senior secured second lien notes to the extent of the Company's and the guarantor subsidiary's value of the collateral securing the notes. The 6.75% Senior Secured First

Lien Notes, 5.375% Senior Secured First Lien Notes, and 5.0% Senior Secured First Lien Notes are effectively equal in right of payment with each other and the guarantees of the Company's senior secured credit facilities. Each series of notes are effectively subordinated to any obligations secured by liens permitted under the indenture for the particular series of notes and structurally subordinated to any existing and future indebtedness and other liabilities of any subsidiary of a guarantor that is not also a guarantor of the notes.

All senior unsecured notes (i) rank senior in right of payment to all of the Company's existing and future subordinated indebtedness, (ii) rank equally in right of payment to all of the existing and future senior indebtedness, (iii) are effectively subordinated in right of payment to all existing and future secured debt to the extent of the value of the assets securing such debt, and (iv) are structurally subordinated to all obligations of each subsidiary that is not a guarantor of the senior notes.

The notes are similarly guaranteed in accordance with their terms by each of the Company's domestic subsidiaries that guarantee obligations under the Company's senior secured term loan facility described in more detail in note 18 "Supplemental Guarantor Condensed Consolidating Financial Statements" of these consolidated financial statements.

All obligations under the senior secured notes, senior secured second lien notes, and senior unsecured notes also contain a number of covenants similar to those described for the senior secured obligations noted above. The Company is in compliance with all applicable covenants.

Note 3: Goodwill and Other Intangibles

The following table presents changes to goodwill for the years ended December 31, 2014 and 2015:

(in millions)	Global Business Solutions	Global Financial Solutions	Network & Security Solutions	Divested Operations	Totals
Balance as of January 1, 2014					
Goodwill	$ 15,892	$ 2,210	$ 2,205	$ 181	$ 20,488
Accumulated impairment losses	(1,363)	(683)	(1,013)	(181)	(3,240)
	14,529	1,527	1,192	—	17,248
Acquisitions	—	—	33	—	33
Other adjustments (primarily foreign currency)	(180)	(84)	—	—	(264)
Balance as of December 31, 2014					
Goodwill	15,712	2,126	2,238	181	20,257
Accumulated impairment losses	(1,363)	(683)	(1,013)	(181)	(3,240)
	14,349	1,443	1,225	—	17,017
Acquisitions	9	—	46	—	55
Other adjustments (primarily foreign currency)	(154)	(72)	—	—	(226)
Balance as of December 31, 2015					
Goodwill	15,567	2,054	2,284	181	20,086
Accumulated impairment losses	(1,363)	(683)	(1,013)	(181)	(3,240)
	$ 14,204	$ 1,371	$ 1,271	$ —	$ 16,846

The intangible amortization expense associated with customer relationships and other intangibles, including amortization associated with investments in affiliates, was as follows:

Year ended December 31, (in millions)	Amount
2015	$ 843
2014	877
2013	924

The carrying value of the First Data trade name is $604 million as of December 31, 2015 and 2014. Upon consideration of many factors, including the determination that there are no legal, regulatory or contractual provisions that limit the useful life of the First Data trade name, the Company determined that the First Data trade name had an indefinite useful life. The Company also considered the effects of obsolescence, demand, competition, other economic factors, and its ability to maintain and protect the trade name without significant expenditures. The First Data trade name is expected to contribute directly or indirectly to the future cash flows of the Company for an indefinite period. As an indefinite lived asset, the First Data trade name is not amortized but is reviewed annually for impairment until such time as it is determined to have a finite life. The First Data trade name was not impaired as of December 31, 2015 or 2014.

The following table provides the components of other intangibles:

	As of December 31,					
	2015			2014		
(in millions)	Cost	Accumulated Amortization	Net of Accumulated Amortization	Cost	Accumulated Amortization	Net of Accumulated Amortization
Customer relationships	$ 7,435	$ (5,299)	$ 2,136	$ 7,475	$ (4,871)	$ 2,604
Other intangibles:						
Conversion costs	$ 218	$ (102)	$ 116	$ 205	$ (89)	$ 116
Contract costs	280	(123)	157	235	(131)	104
Software	2,019	(1,547)	472	1,856	(1,415)	441
Other, including trade names	1,400	(362)	1,038	1,414	(330)	1,084
Total other intangibles	$ 3,917	$ (2,134)	$ 1,783	$ 3,710	$ (1,965)	$ 1,745

The estimated future aggregate amortization expense for the next five years is as follows:

Year ended December 31, (in millions)	Amount
2016	$ 676
2017	569
2018	496
2019	431
2020	350

The Company tests contract and conversion costs for recoverability on an annual basis by comparing the remaining expected undiscounted cash flows under the contract to the net book value. Any assets that are determined to be unrecoverable are written down to their fair value. In addition to this annual test, these assets and all other long lived assets are tested for impairment upon an indicator of potential impairment.

Note 4: Stock Compensation Plans

The Company provides share-based compensation awards to its employees under the 2015 Omnibus Incentive Plan (stock plan), which the Company adopted in conjunction with its initial public offering (IPO) on October 15, 2015. The total number of shares of Class A common stock that may be issued under the stock plan is 71 million, plus any shares of Class B common stock subject to outstanding awards granted under the Company's 2007 Equity Plan that are forfeited, terminated, canceled, expired unexercised, withheld in payment of the exercise price, or withheld to satisfy tax withholding obligations which automatically converted on a one-for-one basis into shares of Class A common stock. The stock plan allows for the Company to award an equity interest in the Company, or be paid incentive compensation, including incentive compensation measured by reference to the value of the Company's Class A common stock.

Share-based compensation expense for awards that vest based solely on service conditions is recognized over the requisite service period. As discussed in note 1 "Summary of Significant Accounting Policies" of these consolidated financial statements, on October 15, 2015, the Company filed its Prospectus with the Securities and Exchange Commission pursuant to Rule 424(b) and started trading on the New York Stock Exchange, therefore all shares are subject to vesting.

Under certain circumstances, the Company redeemed common stock held by its employees.

Total share-based compensation expense recognized in the "Selling, general, and administrative" and "Cost of services" line items of the consolidated statements of operations resulting from stock options, non-vested restricted stock awards, and non-vested restricted stock units was as follows:

Year ended December 31, (in millions)	Cost of services	Selling, general, and administrative	Total
2015 (a)	$ 130	$ 199	$ 329
2014 (b)	2	49	51
2013 (c)	2	37	39

(a) Approximately $14 million of share-based compensation expense was recognized as a result of the departure of certain executive officers. $254 million was recognized in conjunction with the IPO.
(b) Approximately $37 million of share-based compensation expense was recognized as a result of the departure of certain executive officers.
(c) Approximately $20 million of share-based compensation expense was recognized as a result of granting an executive officer shares of common stock and fully vested restricted stock units.

On September 28, 2015, the Company authorized the grant of restricted stock awards, restricted stock units, and options to certain executives in connection with the consummation of its initial public offering and these awards were valued at approximately $120 million, resulting in incremental unrecognized compensation expense. Two-thirds of these grants are subject to time-based vesting conditions over the next five years and one-third are subject to a market-based vesting condition. Subject to the recipient's continued service with the Company through the applicable vesting event, shares subject to market-based stock options and market-based restricted stock will fully vest on the date immediately following the date on which the closing trading price of a share of Class A common stock on the NYSE or other such primary exchange on which shares of Class A common stock are listed and traded has equaled or exceeded two times the per share price to the public in the offering for ten consecutive trading days.

During the years ended December 31, 2015, 2014, and 2013, the Company's former parent, FDH, paid $4 million, $15 million, and $22 million, respectively, to repurchase shares from employees that terminated employment with the Company.

Stock Options

During the years ended December 31, 2015, 2014, and 2013, time-based options were granted under the stock plan. The time-based options have a contractual term of 10 years. Time-based options vest equally over a three to five year period from the date of issuance. The outstanding time-based options also have certain accelerated vesting provisions that became effective upon the Company's initial public offering.

As of December 31, 2015, there was approximately $124 million of total unrecognized compensation expense related to stock options to be recognized over a weighted-average period of approximately three years.

The fair value of stock options granted for the years ended December 31, 2015, 2014, and 2013 were estimated at the date of grant using a Black-Scholes option pricing model with the following weighted-average assumptions:

	Year ended December 31,		
	2015	2014	2013
Risk-free interest rate	1.87%	2.24%	1.40%
Dividend yield	—	—	—
Expected volatility	55.15%	50.45%	56.61%
Expected term (in years)	7	7	7
Fair value of stock	$ 15.53	$ 12.64	$ 11.06
Fair value of options	$ 8.68	$ 6.76	$ 6.29

Risk-free interest rate—The risk-free rate for stock options granted during the period was determined by using a zero-coupon U.S. Treasury rate for the periods that coincided with the expected terms listed above.

Expected dividend yield—No routine dividends are currently being paid, or are expected to be paid in future periods.

Expected volatility—As the Company does not have sufficient historical data due to its relatively short history of being publicly traded, the expected volatility is based on the historical volatilities of a group of guideline companies.

Expected term—The Company estimated the expected term by utilizing the "simplified method" as allowed by the SEC.

Fair value of stock—The Company determined the fair value based on discounted cash flows and comparison to a group of guideline companies prior to being publicly traded on October 15, 2015 and the Company's closing stock price thereafter.

A summary of stock option activity for the year ended December 31, 2015 is as follows:

(options in millions)	Options	Weighted-Average Exercise Price	Weighted-Average Remaining Contractual Term	Aggregate Intrinsic Value (in millions)
Outstanding as of January 1, 2015	32	$ 10.75		
Granted	11	$ 15.53		
Exercised	(1)	$ 9.86		
Cancelled / Forfeited	(1)	$ 11.25		
Outstanding as of December 31, 2015 (a)	41	$ 11.94	7 years	$ 166
Options exercisable as of December 31, 2015 (a)	19	$ 10.32	5 years	$ 108

(a) Includes 2 million of outstanding options subject to the market conditions described above. There are no exercisable options subject to these market conditions.

The total intrinsic value and amount paid related to stock options exercised during the twelve months ended December 31, 2015, 2014, and 2013 was $4 million, $2 million, and $3 million, respectively.

Restricted Stock Awards and Restricted Stock Units

Restricted stock awards and units were granted under the stock plan during 2015, 2014, and 2013. Grants were made as incentive awards. The restrictions on the awards granted lapsed upon the Company's initial public offering. However, they remain subject to the remaining lock-up period and/or applicable vesting requirements. As of December 31, 2015, there was approximately $248 million of total unrecognized compensation expense related to restricted stock of which approximately $70 million will be recognized in the first quarter of 2016 as the lock-up associated with the filing of the Company's prospectus expires, the remaining $178 million will be recognized over the respective service period, approximately two years.

During 2015, 2014, and 2013, the Company paid $11 million, $5 million, and $6 million, respectively, to repurchase stock awards from employees that terminated employment with the Company.

A summary of restricted stock award and restricted stock unit activity for the year ended December 31, 2015 is as follows:

(awards/units in millions)	Awards/Units	Weighted-Average Grant-Date Fair Value
Non-vested as of January 1, 2015	15	$ 11.98
Granted	19	$ 14.96
Vested	(1)	$ 15.04
Cancelled / Forfeited	(1)	$ 14.02
Non-vested as of December 31, 2015 (a)	32	$ 14.30

(a) Includes 1 million of shares subject to the market conditions described above.

The total fair value of shares vested (measured as of the date of vesting) during the twelve months ended December 31, 2015, 2014, and 2013 was $11 million, $15 million, and $18 million, respectively.

Note 5: Stockholders' Equity and Redeemable Noncontrolling Interest

Dividends

The Company's senior secured revolving credit facility, senior secured term loan facility, and the indentures governing the senior secured notes, senior unsecured notes, and senior subordinated notes limit the Company's ability to pay dividends. The restrictions are subject to numerous qualifications and exceptions, including an exception that allows the Company to pay a dividend to repurchase, under certain circumstances, the equity of the Company's former parent, FDH, held by employees, officers and directors that were obtained in connection with the stock compensation plan. Prior to the Company filing its prospectus with the Securities and Exchange Commission and the merger with FDH, the Company paid cash dividends to FDH totaling $4 million during 2015, $686 million during 2014, and $28 million during 2013.

Other Comprehensive Income

The income tax effects allocated to and the cumulative balance of each component of OCI are as follows:

(in millions)	Beginning Balance	Pretax Gain (Loss) Amount	Tax (Benefit) Expense	Net-of-Tax Amount	Ending Balance
As of December 31, 2015					
Unrealized (losses) gains on securities	$ (5)	$ 3	$ —	$ 3	$ (2)
Foreign currency translation adjustment [a]	(801)	(261)	19	(280)	(1,081)
Pension liability adjustments	(123)	(19)	(6)	(13)	(136)
	$ (929)	$ (277)	$ 13	$ (290)	$ (1,219)
As of December 31, 2014					
Unrealized gains (losses) on securities	$ 2	$ (7)	$ —	$ (7)	$ (5)
Foreign currency translation adjustment [a]	(504)	(298)	(1)	(297)	(801)
Pension liability adjustments	(87)	(35)	1	(36)	(123)
	$ (589)	$ (340)	$ —	$ (340)	$ (929)
As of December 31, 2013					
Unrealized gains on securities	$ 1	$ 2	$ 1	$ 1	$ 2
Foreign currency translation adjustment [a]	(426)	(103)	(25)	(78)	(504)
Pension liability adjustments	(127)	64	24	40	(87)
	$ (552)	$ (37)	$ —	$ (37)	$ (589)

(a) Net-of-tax Foreign currency translation adjustment for the years ended December 31, 2015, 2014, and 2013 is different than the amount presented on the consolidated statements of comprehensive income (loss) by $(10) million, $(11) million, and $1 million, respectively, due to the foreign currency translation adjustment related to noncontrolling interests not included above.

Redeemable Noncontrolling Interest

The following table presents a summary of the redeemable noncontrolling interest activity:

(in millions)	Redeemable Noncontrolling Interest
Balance as of January 1, 2013	$ 68
Distributions	(35)
Share of income	34
Adjustment to redemption value of redeemable noncontrolling interest	2
Balance as of December 31, 2013	69
Distributions	(35)
Share of income	34
Adjustment to redemption value of redeemable noncontrolling interest	2
Balance as of December 31, 2014	70
Distributions	(35)
Share of income	34
Adjustment to redemption value of redeemable noncontrolling interest	8
Balance as of December 31, 2015	$ 77

Note 6: Net Loss Per Share

Upon the HoldCo Merger, all outstanding shares of FDH's Class A Common Stock, Class B Common Stock, and Series A Voting Participating Convertible Preferred Stock (Series A Preferred Stock) automatically converted to identical shares of the Company's stock. Following the filing of the Company's prospectus with the Securities and Exchange Commission, holders of existing Class B Common Stock and Series A Preferred Stock received Class B Common Stock in the Company. Other than voting rights, this common stock has the same rights as the Class A Common Stock and therefore both are treated as the same class of stock for purposes of the net loss per share calculation.

Diluted net loss per share has been computed to give effect to the impact, if any, of shares issuable upon the assumed exercise of the Company's common stock equivalents, which consist of outstanding stock options and unvested restricted stock.

For the year ended December 31, 2015, all outstanding options and unvested restricted stock were excluded from the calculation of diluted shares due to these securities being anti-dilutive because of the Company's net loss attributable to First Data Corporation.

The following table sets forth the computation of the Company's basic and diluted net loss per share:

	Year ended December 31,		
(in millions, except share amounts)	2015	2014	2013
Numerator:			
Net loss used in computing net loss per share, basic and diluted	$ (1,481)	$ (458)	$ (952)
Denominator:			
Shares used in computing net loss per share, basic and diluted (a)	192,263,793	1,000	1,000
Net loss per share, basic and diluted	$ (7.70)	$ (458,000)	$ (952,000)
Anti-dilutive shares excluded from diluted net loss per share	26,752,706	—	—

(a) 2015 weighted-average shares calculated using 1,000 shares outstanding prior to the HoldCo Merger and the filing of the Company's prospectus in October 2015 and the Class A and Class B common stock outstanding after these transactions. 2014 and 2013 weighted-average shares calculated using 1,000 shares outstanding prior to the HoldCo Merger and the filing of the Company's prospectus in October 2015.

Note 7: Segment Information

Operating segments are defined as components of an enterprise about which separate financial information is available that is evaluated regularly by a company's chief operating decision maker (CODM), or decision-making group, in deciding how to allocate resources and in assessing performance. The Company's CODM is its Chief Executive Officer. The Company is organized into three segments: Global Business Solutions, Global Financial Solutions, and Network & Security Solutions.

The business segment measurements provided to and evaluated by the chief operating decision maker are computed in accordance with the principles listed below.

- The accounting policies of the operating segments are the same as those described in the summary of significant accounting policies.
- Intersegment revenues are eliminated in the segment that sells directly to the end market.
- Segment revenue excludes reimbursable PIN debit fees, postage, and other revenue.
- Adjusted EBITDA by segment includes equity earnings in affiliates and excludes depreciation and amortization expense, net income attributable to noncontrolling interests, other operating expenses, and other income (expense). Additionally, adjusted EBITDA is adjusted for items similar to certain of those used in calculating the Company's compliance with debt covenants. The additional items that are adjusted to determine adjusted EBITDA are:
    - share-based compensation and related expense is excluded;
    - debt issuance costs are excluded and represent costs associated with issuing debt and modifying the Company's debt structure; and
    - KKR related items including annual sponsor and other fees for management, consulting, financial, contract termination, and other advisory services are excluded.
- For significant affiliates, segment revenue and adjusted EBITDA are reflected based on the Company's proportionate share of the results of its investments in businesses accounted for under the equity method and consolidated subsidiaries with noncontrolling ownership interests. For other affiliates, the Company includes equity earnings in affiliates, excluding amortization expense, in segment revenue and adjusted EBITDA. In addition, the Company's segment measures reflect revenue-based commission payments to Independent Sales Organizations and sales channels, which are treated as an expense in the consolidated statements of operations, as contra revenue.
- Corporate operations include corporate-wide governance functions such as the Company's executive management team, aviation, tax, treasury, internal audit, corporate strategy, and certain accounting, human resources and legal costs related to supporting the corporate function. Costs incurred by Corporate that are attributable to a segment are allocated to the respective segment.

The following tables present the Company's operating segment results for the years ended December 31, 2015, 2014, and 2013:

	Year ended December 31, 2015				
(in millions)	Global Business Solutions	Global Financial Solutions	Network & Security Solutions	Corporate	Totals
Revenues:					
Transaction and processing service fees	$ 3,209	$ 1,323	$ 1,322	$ —	$ 5,854
Product sales and other	845	172	142	—	1,159
Equity earnings in affiliates	35	—	—	—	35
Total segment revenues	$ 4,089	$ 1,495	$ 1,464	$ —	$ 7,048
Depreciation and amortization	$ 490	$ 393	$ 91	$ 25	$ 999
Adjusted EBITDA	1,681	550	639	(140)	2,730
Other operating expenses and other income (expense) excluding divestitures	26	(16)	(3)	(36)	(29)
Equity earnings in affiliates	239	—	—	—	239

	Year ended December 31, 2014				
(in millions)	Global Business Solutions	Global Financial Solutions	Network & Security Solutions	Corporate	Totals
Revenues:					
Transaction and processing service fees	$ 3,250	$ 1,313	$ 1,277	$ —	$ 5,840
Product sales and other	766	176	92	—	1,034
Equity earnings in affiliates	30	—	—	—	30
Total segment revenues	$ 4,046	$ 1,489	$ 1,369	$ —	$ 6,904
Depreciation and amortization	$ 518	$ 401	$ 90	$ 23	$ 1,032
Adjusted EBITDA	1,687	529	608	(161)	2,663
Other operating expenses and other income (expense) excluding divestitures	38	(3)	96	15	146
Equity earnings in affiliates	216	—	4	—	220

	Year ended December 31, 2013				
(in millions)	Global Business Solutions	Global Financial Solutions	Network & Security Solutions	Corporate	Totals
Revenues:					
Transaction and processing service fees	$ 3,197	$ 1,217	$ 1,284	$ —	$ 5,698
Product sales and other	709	167	78	—	954
Equity earnings in affiliates	32	—	—	—	32
Total segment revenues	$ 3,938	$ 1,384	$ 1,362	$ —	$ 6,684
Depreciation and amortization	$ 543	$ 424	$ 107	$ 17	$ 1,091
Adjusted EBITDA	1,644	404	549	(148)	2,449
Other operating expenses and other income (expense) excluding divestitures	36	(10)	(5)	(118)	(97)
Equity earnings in affiliates	185	—	3	—	188

The following table presents a reconciliation of reportable segment amounts to the Company's consolidated balances for the years ended December 31, 2015, 2014, and 2013:

	Year ended December 31,		
(in millions)	2015	2014	2013
Total segment revenues	$ 7,048	$ 6,904	$ 6,684
Adjustments for non wholly owned entities (a)	74	57	39
ISOs commission expense (b)	642	587	579
Reimbursable debit network fees, postage, and other	3,687	3,604	3,507
Total revenues	$ 11,451	$ 11,152	$ 10,809
Total Adjusted EBITDA	$ 2,730	$ 2,663	$ 2,449
Adjustments to reconcile to Net loss attributable to First Data Corporation:			
Adjustments for non wholly owned entities (a)	26	24	2
Depreciation and amortization	(1,022)	(1,056)	(1,091)
Interest expense, net	(1,537)	(1,728)	(1,856)
Loss on debt extinguishment	(1,068)	(274)	(79)
Other items (c)	(75)	92	(134)
Income tax expense	(101)	(82)	(105)
Share-based compensation	(329)	(50)	(38)
Costs of alliance conversions	(5)	(20)	(68)
KKR related items	(100)	(27)	(32)
Net loss attributable to First Data Corporation	$ (1,481)	$ (458)	$ (952)

(a) Net adjustment to reflect the Company's proportionate share of alliance revenue and adjusted EBITDA and amortization related to equity method investments not included in adjusted EBITDA.
(b) Reported within Selling, general, and administrative expense in the consolidated statements of operations.
(c) Includes adjustments to exclude the official check and money order businesses due to the Company's wind down of these businesses, restructuring, certain retention bonuses, non-normal course litigation and regulatory settlements, and "Other income (expense)" as presented in the consolidated statements of operations, which includes divestitures, impairments, derivative gains and (losses), and non-operating foreign currency gains and (losses).

Total segment assets, capital expenditures, and investment in unconsolidated affiliates are not disclosed as the Company's CODM does not utilize such information when allocating resources to the segment or when assessing the segments' performance.

The following tables presents a reconciliation of reportable segment depreciation and amortization amounts to the Company's consolidated balances in the consolidated statements of cash flows for the years ended December 31, 2015, 2014, and 2013:

	Year ended December 31,		
(in millions)	2015	2014	2013
Segment depreciation and amortization	$ 999	$ 1,032	$ 1,091
Adjustments for non wholly owned entities	83	86	79
Amortization of initial payments for new contracts (a)	51	45	42
Total consolidated depreciation and amortization per consolidated statements of cash flows	1,133	1,163	1,212
Amortization of equity method investment (b)	(60)	(62)	(79)
Amortization of initial payments for new contracts (a)	(51)	(45)	(42)
Total consolidated depreciation and amortization per consolidated statements of operations	$ 1,022	$ 1,056	$ 1,091

(a) Included in "Transaction and processing service fees" as contra-revenue in the Company's consolidated statements of operations.
(b) Included in "Equity earnings in affiliates" in the Company's consolidated statements of operations.

The following tables presents revenues and long-lived assets by principal geographic area for the years ended December 31, 2015, 2014, and 2013:

(in millions)	United States	International	Total
Revenues:			
2015	$ 9,795	$ 1,656	$ 11,451
2014	9,428	1,724	11,152
2013	9,145	1,664	10,809
Long-Lived Assets:			
2015	$ 19,400	$ 2,316	$ 21,716
2014	19,708	2,588	22,296
2013	20,020	2,959	22,979

Note 8: Income Taxes

	Year ended December 31,		
(in millions)	2015	2014	2013
Components of pretax (loss) income:			
Domestic	$ (1,332)	$ (378)	$ (843)
Foreign	165	195	173
	$ (1,167)	$ (183)	$ (670)
Provision for income taxes:			
Federal	$ 7	$ 16	$ 39
State and local	14	22	20
Foreign	80	44	46
Income tax expense	$ 101	$ 82	$ 105
Effective income tax rate	(9)%	(45)%	(16)%

The Company's effective tax rates differ from statutory rates as follows:

	Year ended December 31,		
	2015	2014	2013
Federal statutory rate	35 %	35 %	35 %
State income taxes, net of federal income tax benefit	3	(1)	2
Nontaxable income from noncontrolling interests	6	37	9
Impact of foreign operations (a)	—	(9)	(1)
Tax effects of foreign exchange gains/losses	(1)	(6)	1
Valuation allowances	(54)	(103)	(55)
Liability for unrecognized tax benefits	(2)	12	—
Prior year adjustments	4	(7)	(6)
Nondeductible bad debts	—	(3)	—
Other	—	—	(1)
Effective tax rate	(9)%	(45)%	(16)%

(a) The impact of foreign operations includes the effects of earnings and profits adjustments, foreign losses, and differences between foreign tax expense and foreign taxes eligible for the U.S. foreign tax credit.

The Company's income tax provisions (benefits) consisted of the following components:

	Year ended December 31,		
(in millions)	2015	2014	2013
Current:			
Federal	$ 5	$ —	$ (1)
State and local	23	39	23
Foreign	80	61	52
	108	100	74
Deferred:			
Federal	2	17	40
State and local	(9)	(18)	(3)
Foreign	—	(17)	(6)
	(7)	(18)	31
	$ 101	$ 82	$ 105

Deferred tax assets and liabilities are recognized for the expected tax consequences of temporary differences between the book and tax bases of the Company's assets and liabilities. Valuation allowances are recorded to reduce deferred tax assets when it is more likely than not that a tax benefit will not be realized. Deferred tax assets are included in "Other long-term assets" and deferred tax liabilities are included in "Deferred tax liabilities" in the Company's consolidated balance sheets. As discussed in note 1 "Summary of Significant Accounting Policies" of these consolidated financial statements, the Company adopted new FASB guidance that requires companies to classify all deferred tax assets and liabilities as noncurrent on the balance sheet instead of separating deferred taxes into current and noncurrent amounts. The guidance was retrospectively adopted to 2014, and resulted in a decrease in "Other current assets," "Other long-term assets," "Accounts payable and accrued liabilities," and "Deferred tax liabilities" of $86 million, $6 million, $6 million, and $86 million, respectively, as of December 31, 2014.

The following table outlines the principal components of deferred tax items:

(in millions)	As of December 31, 2015	2014
Deferred tax assets related to:		
Reserves and other accrued expenses	$ 90	$ 266
Pension obligations	6	—
Employee related liabilities	171	84
Deferred revenues	44	30
Net operating losses and tax credit carryforwards	3,116	2,160
U.S. foreign tax credits on undistributed earnings	330	280
Foreign exchange (gain)/loss	32	52
Total deferred tax assets	3,789	2,872
Valuation allowance	(2,694)	(1,694)
Realizable deferred tax assets	1,095	1,178
Deferred tax liabilities related to:		
Property, equipment, and intangibles	(1,019)	(1,083)
Pension obligations	—	(2)
Investment in affiliates and other	(306)	(331)
U.S. tax on foreign undistributed earnings	(192)	(185)
Total deferred tax liabilities	(1,517)	(1,601)
Net deferred tax liabilities	$ (422)	$ (423)

The Company's deferred tax assets and liabilities were included in the consolidated balance sheets as follows:

(in millions)	As of December 31, 2015	2014
Deferred tax assets	$ 9	$ 12
Deferred tax liabilities	(431)	(435)
Net deferred tax liabilities	$ (422)	$ (423)

As of December 31, 2015 and 2014, the Company had recorded valuation allowances of $2.7 billion and $1.7 billion, respectively, against its net deferred tax assets. The increase to the valuation allowance of $1.0 billion in 2015 was primarily due to current year federal, state, and foreign net operating losses which may not be utilized within the statute of limitations. In determining the necessary amount of valuation allowance, the Company has considered a tax planning strategy related to its investments in affiliates. Implementation of this strategy would result in the immediate reversal of temporary differences associated with the excess of book basis over tax basis in the investments. This planning strategy would be implemented only in the event of anticipated expiration of significant net operating losses in the United States federal jurisdiction, which is not expected in the near term.

The following table presents the amounts of federal, state, and foreign net operating loss carryforwards and foreign tax credit, general business credit, and minimum tax credit carryforwards:

(in millions)	As of December 31, 2015
Federal net operating loss carryforwards (a)	$ 5,138
State net operating loss carryforwards (a)	6,014
Foreign net operating loss carryforwards (b)	2,874
Foreign tax credit carryforwards (c)	248
General business credit carryforwards (d)	12
Minimum tax credit carryforwards (e)	2

(a) If not utilized, these carryforwards will expire in years 2016 through 2035.
(b) Foreign net operating loss carryforwards of $64 million, if not utilized, will expire in years 2016 through 2035. The remaining foreign net operating loss carryforwards of $2.8 billion have an indefinite life.
(c) If not utilized, these carryforwards will expire in years 2018 through 2025.
(d) If not utilized, these carryforwards will expire in years 2027 through 2034.
(e) These carryforwards have an indefinite life.

The Company intends to indefinitely invest its net equity in its foreign operations, with the exception of any undistributed foreign earnings. Accordingly, as of December 31, 2015, no provision had been made for U.S. federal and state income taxes on the cumulative amount of temporary differences related to investments in foreign subsidiaries, other than those differences related to the undistributed earnings. Upon sale or liquidation of these investments, the Company would potentially be subject to U.S., state, and foreign income taxes and withholding taxes payable to the various foreign countries. The amount of unrecognized deferred tax liability related to investments in foreign subsidiaries is approximately $204 million as of December 31, 2015.

A reconciliation of the unrecognized tax benefits for the years ended December 31, 2013, 2014, and 2015 is as follows:

(in millions)	Unrecognized Tax Benefits
Balance as of January 1, 2013	$ 286
Increases for tax positions of prior years	3
Decreases for tax positions of prior years	(3)
Increases for tax positions related to the current period	5
Decreases for cash settlements with taxing authorities	(6)
Decreases due to the lapse of the applicable statute of limitations	(6)
Balance as of December 31, 2013	279
Increases for tax positions of prior years	3
Decreases for tax positions of prior years	(29)
Increases for tax positions related to the current period	1
Decreases for cash settlements with taxing authorities	(13)
Decreases due to the lapse of the applicable statute of limitations	(5)
Balance as of December 31, 2014	236
Increases for tax positions of prior years	25
Decreases for tax positions of prior years	(4)
Increases for tax positions related to the current period	1
Decreases for cash settlements with taxing authorities	(3)
Decreases due to the lapse of the applicable statute of limitations	(6)
Balance as of December 31, 2015	$ 249

Most of the unrecognized tax benefits are included in the "Other long-term liabilities" line of the consolidated balance sheets, net of the federal benefit on state income taxes (approximately $22 million as of December 31, 2015). However, those unrecognized tax benefits that affect the federal consolidated tax years ending December 31, 2008 through December 31, 2015 are included in the "Deferred tax liabilities" line of the consolidated balance sheets, as these items reduce the Company's net operating loss and

credit carryforwards from those periods. The unrecognized tax benefits as of December 31, 2015, 2014, and 2013 included approximately $136 million, $126 million, and $161 million, respectively, of tax positions that, if recognized, would affect the effective tax rate.

The Company recognizes interest and penalties related to unrecognized tax benefits in the "Income tax expense" line item of the consolidated statements of operations. Cumulative accrued interest and penalties (net of related tax benefits) are not included in the ending balances of unrecognized tax benefits. Cumulative accrued interest and penalties are included in the "Other long-term liabilities" line of the consolidated balance sheets while the related tax benefits are included in the "Deferred tax liabilities" line of the consolidated balance sheets. The following table presents the approximate amounts associated with accrued interest expense and the cumulative accrued interest and penalties:

	Year ended December 31,		
(in millions)	2015	2014	2013
Current year accrued interest expense (net of related tax benefits)	$ 7	$ 1	$ 5
Cumulative accrued interest and penalties (net of related tax benefits)	45	39	45

As of December 31, 2015, the Company anticipates it is reasonably possible that its liability for unrecognized tax benefits may decrease by approximately $124 million within the next 12 months as a result of the possible closure of federal tax audits, potential settlements with certain states and foreign countries, and the lapse of the statute of limitations in various state and foreign jurisdictions.

The Company or one or more of its subsidiaries file income tax returns in the U.S. federal jurisdiction and various state and foreign jurisdictions. As of December 31, 2015, the Company was no longer subject to income tax examination by the U.S. federal jurisdiction for years before 2005. State and local examinations are substantially complete through 2006. Foreign jurisdictions generally remain subject to examination by their respective authorities from 2008 forward, none of which are considered major jurisdictions.

Under the Tax Allocation Agreement executed at the time of the spin-off of The Western Union Company (Western Union) on September 29, 2006, Western Union is responsible for and must indemnify the Company against all taxes, interest, and penalties that relate to Western Union for periods prior to the spin-off date. If Western Union were to agree to or be finally determined to owe any amounts for such periods but were to default in its indemnification obligation under the Tax Allocation Agreement, the Company as parent of the tax filing group during such periods generally would be required to pay the amounts to the relevant tax authority, resulting in a potentially material adverse effect on the Company's financial position and results of operations. As of December 31, 2015, the Company had approximately $120 million of income taxes payable, including approximately $4 million of uncertain income tax liabilities, recorded related to Western Union for periods prior to the spin-off date. The Company has recorded a corresponding account receivable of equal amount from Western Union, which is included as a long-term account receivable in the "Other long-term assets" line of the Company's consolidated balance sheets, reflecting the indemnification obligation. The uncertain income tax liabilities and corresponding receivable are based on information provided by Western Union regarding its tax contingency reserves for periods prior to the spin-off date. There is no assurance that a Western Union-related issue raised by the IRS or other tax authority will be finally resolved at a cost not in excess of the amount reserved and reflected in the Company's uncertain income tax liabilities and corresponding receivable from Western Union. The Western Union contingent liability is in addition to the Company's liability for unrecognized tax benefits discussed above.

The IRS completed its examination of the U.S. federal consolidated income tax returns of the Company for 2005 through 2007 and issued a 30-Day letter in October 2012. The 30-Day letter claims that the Company and its subsidiaries, which included Western Union during some of the years at issue, owe additional taxes with respect to a variety of adjustments. The Company and Western Union agree with several of the adjustments in the 30-Day letter, such adjustments representing tax due of approximately $40 million. This undisputed tax and associated interest due (pretax) of approximately $21 million through December 31, 2015, have been fully reserved. The undisputed tax for which Western Union would be required to indemnify the Company is greater than the total tax due, such that settlement of the undisputed tax would result in a net refund to the Company. As to the adjustments that are disputed, such issues represent total taxes allegedly due of approximately $59 million, of which $40 million relates to the Company and $19 million relates to Western Union. The Company estimates that total interest due (pretax) on the disputed amounts is approximately $23 million through December 31, 2015, of which $13 million relates to the Company and $10 million relates to Western Union. As to the disputed issues, the Company and Western Union are contesting the asserted deficiencies with the Appeals Office of the IRS. The Company believes that it has adequately reserved for the disputed issues in its liability for

unrecognized tax benefits described above and that final resolution of those issues will not have a material adverse effect on its financial position or results of operations.

Note 9: Related Party Transactions

Merchant Alliances

A substantial portion of the Company's business within the Global Business Solutions segment is conducted through merchant alliances. Merchant alliances are alliances between the Company and financial institutions. If the Company has majority ownership and management control over an alliance, then the alliance's financial statements are consolidated with those of the Company and the related processing fees are treated as an intercompany transaction and eliminated upon consolidation. If the Company does not have a controlling ownership interest in an alliance, it uses the equity method of accounting to account for its investment in the alliance. As a result, the Company's consolidated revenues include processing fees charged to alliances accounted for under the equity method. No directors or officers of the Company have ownership interests in any of the alliances. The formation of each of these alliances generally involves the Company and the bank contributing contractual merchant relationships to the alliance and a cash payment from one owner to the other to achieve the desired ownership percentage for each. The Company and the bank enter into a long-term processing service agreement as part of the negotiation process. This agreement governs the Company's provision of transaction processing services to the alliance. As of December 31, 2015 and 2014, the Company had $50 million and $43 million, respectively, of amounts due from unconsolidated merchant alliances included within "Accounts receivable" in the Company's consolidated balance sheets. As of December 31, 2015 and 2014, the Company had $5 million and $9 million, respectively, of amounts due to unconsolidated merchant alliances included within "Accounts payable and accrued liabilities" in the Company's consolidated balance sheets.

Management Agreement

In connection with the 2007 acquisition of the Company by affiliates of Kohlberg Kravis Roberts & Co. L.P. (KKR), the Company entered into a management agreement with KKR and one of its affiliates (Management Agreement) pursuant to which KKR provided advisory services to the Company and received fees and reimbursements of related out-of-pocket expenses. The Management Agreement was terminated upon the consummation of the Company's initial public offering. Upon termination the Company paid a $78 million termination fee to KKR which was based on the net present value of future payment obligations under the Management Agreement. For the years ended December 31, 2015, 2014, and 2013, the Company, inclusive of the termination fee, paid $98 million, $20 million, and $20 million, respectively, of management fees to KKR.

Relationship with KKR Capital Markets

For the years ended December 31, 2015, 2014, and 2013, KKR Capital Markets LLC, an affiliate of KKR, acted as an arranger and bookrunner for various financing transactions under the existing credit agreements, and as an initial purchaser of certain existing notes issued by the Company, and received underwriter and transaction fees totaling $25 million, $4 million, and $10 million, respectively.

For the years ended December 31, 2015 and 2014, KKR Capital Markets LLC also acted as a placement agent in the Company's initial public offering for placement of the Company's Class A common stock and in the private placement of shares of Holdings' Class B common stock and received $19 million and $41 million, respectively, for such services.

Note 10: Restructuring

During the years ended December 31, 2015, 2014, and 2013, the Company recorded restructuring charges in connection with management's alignment of the business with strategic objectives, cost savings initiatives and the departure of certain executive officers.

On May 4, 2015, the Company announced a strategic expense management initiative to optimize its annualized expense base by mid-2016. Anticipated restructuring costs will be approximately $75 million, mainly cash, and commenced in the second quarter of 2015. The net charge is expected to include costs for severance, retention and transition, asset impairments, professional services fees, and gains/losses on the sale of facilities. The vast majority of the net charge will be related to personnel (severance, retention and transition).

A summary of net pretax benefits (charges), incurred by segment, for each period is as follows:

(in millions)	Year ended December 31, 2015	2014	2013
Global Business Solutions	$ (20)	$ —	$ (14)
Global Financial Solutions	(11)	1	(4)
Network & Security Solutions	(3)	(2)	(6)
Corporate	(19)	(12)	(24)
Restructuring, net	$ (53)	$ (13)	$ (48)

The following table summarizes the Company's utilization of restructuring accruals for the years ended December 31, 2014 and 2015:

(in millions)	Employee Severance	Other
Remaining accrual as of January 1, 2014	$ 21	$ —
Restructuring, net	12	1
Cash payments and other	(21)	—
Remaining accrual as of December 31, 2014	12	1
Restructuring, net	46	7
Cash payments and other	(29)	(7)
Remaining accrual as of December 31, 2015	$ 29	$ 1

Note 11: Settlement Assets and Obligations

Settlement assets and obligations result from the Company's processing services and associated settlement activities, including settlement of payment transactions. Settlement assets are generated principally from merchant services transactions. Certain merchant settlement assets that relate to settlement obligations accrued by the Company are held by partner banks to which the Company does not have legal ownership but has the right to use to satisfy the related settlement obligation. The Company records corresponding settlement obligations for amounts payable to merchants and for payment instruments not yet presented for settlement. The difference in the aggregate amount of such assets and liabilities is due to unrealized net investment gains and losses, which are reported as OCI in equity.

The principal components of the Company's settlement assets and obligations are as follows:

(in millions)	As of December 31, 2015	2014
Settlement assets:		
Cash and cash equivalents	$ 1,426	$ 1,419
Investment securities	1	17
Due from card associations and bank partners	5,816	5,220
Due from merchants	907	899
	8,150	7,555
Long-term settlement assets: (a)		
Investment securities	1	3
	$ 8,151	$ 7,558
Settlement obligations:		
Payment instruments outstanding	$ 34	$ 82
Card settlements due to merchants	8,116	7,475
	$ 8,150	$ 7,557

(a) Long-term settlement assets are included within "Other long-term assets" on the Company's consolidated balance sheets.

The changes in settlement assets and obligations are presented on a net basis within operating activities in the consolidated statements of cash flows. However, because the changes in the settlement assets balance exactly offset changes in settlement obligations, the activity nets to zero.

Note 12: Acquisitions and Dispositions

2015 Acquisitions

On June 9, 2015, the Company acquired Transaction Wireless, Inc. a provider of digital stored value products that offers gift card programs, loyalty incentives, and integrated marketing solutions for retailers, partners, and consumers. The purchase price was approximately $62 million in cash and $3 million in equity. The acquisition is reported in the Company's Network & Security Solutions segment.

In addition to TWI, the Company also completed an acquisition of a webstore builder as well as an acquisition of a wholesale independent sales organization, both of which are reported in the Company's Global Business Solutions segment.

2014 Acquisitions

In August 2014, the Company acquired Gyft, Inc., a leading digital platform that enables consumers to buy, send, manage, and redeem gift cards using mobile devices. The acquisition is reported as part of the Network & Security Solutions segment. Refer to note 14 "Commitments and Contingencies" of these consolidated financial statements for additional information regarding the liability for contingent consideration.

2014 Dispositions

On May 29, 2014, the Company completed the sale of its 30% minority interest in a transportation payments business, Electronic Funds Source LLC (EFS), which was reported as part of the Network & Security Solutions segment. The Company recognized a gain on sale of $98 million recorded in "Other income (expense)" in the consolidated statements of operations, comprised of $264 million in cash reduced by its investment and associated deal costs of $166 million, and recorded an income tax provision of $7 million as a result of the final settlement of the sale.

2013 Acquisitions

In October 2013, the Company acquired Perka Inc., a provider of a mobile marketing and consumer loyalty solution. The acquisition is reported as part of the Global Business Solutions segment.

Note 13: Derivative Financial Instruments

The Company enters into the following types of derivatives:

Interest rate contracts:

- Interest rate swaps: The Company uses interest rate swaps to mitigate the exposure to interest rate fluctuations on interest payments related to variable rate debt. The Company uses these contracts in non-qualifying hedging relationships.
- Fixed to floating interest rate swaps: The Company uses fixed to floating interest rate swaps to maintain a desired ratio of fixed rate and floating rate debt. The Company uses these contracts in non-qualifying hedging relationships.
- Foreign exchange contracts: The Company uses cross-currency swaps to protect the net investment in certain foreign subsidiaries and/or affiliates with respect to changes in foreign currency exchange rates. The Company uses these contracts in both qualifying and non-qualifying hedging relationships.

The Company held the following derivative instruments as of the dates indicated:

	As of December 31,							
	2015				2014			
(in millions)	Notional Currency	Notional Value	Assets (a)	Liabilities (a)	Notional Currency	Notional Value	Assets (a)	Liabilities (a)
Derivatives designated as hedges of net investments in foreign operations:								
Foreign exchange contracts	AUD	260	$ 65	$ —	AUD	260	$ 41	$ —
Foreign exchange contracts (b)	EUR	200	51	—	EUR	200	27	—
Foreign exchange contracts	GBP	250	39	—	GBP	250	18	—
Foreign exchange contracts	CAD	110	24	—	CAD	110	9	—
			179	—			95	—
Derivatives not designated as hedging instruments:								
Interest rate contracts	USD	5,000	—	(56)	USD	5,750	47	(105)
Foreign exchange contracts	EUR	—	—	—	EUR	22	1	—
			—	(56)			48	(105)
			$ 179	$ (56)			$ 143	$ (105)

(a) Of the balances included in the table above, in aggregate, $179 million of assets and $51 million of liabilities, net $128 million, as of December 31, 2015 and $142 million of assets and $96 million of liabilities, net $46 million, as of December 31, 2014 are subject to master netting agreements to the extent that the swaps are with the same counterparty. The terms of those agreements require that the Company net settle the outstanding positions at the option of the counterparty upon certain events of default.

(b) Matured January 18, 2016.

The maximum length of time over which the Company is hedging its exposure to the variability in future cash flows for forecasted transactions excluding those forecasted transactions related to the payment of variable interest on existing financial instruments is through January 2018.

Fair Value Measurement

The carrying amounts for the Company's derivative financial instruments are the estimated fair value of the financial instruments. The Company's derivatives are not exchange listed and therefore the fair value is estimated under an income approach using Bloomberg analytics models that are based on readily observable market inputs. These models reflect the contractual terms of the derivatives, such as notional value and expiration date, as well as market-based observables including interest and foreign currency exchange rates, yield curves, and the credit quality of the counterparties. The models also incorporate the Company's creditworthiness in order to appropriately reflect non-performance risk. Inputs to the derivative pricing models are generally observable and do not contain a high level of subjectivity and, accordingly, the Company's derivatives were classified within Level 2 of the fair value hierarchy. While the Company believes its estimates result in a reasonable reflection of the fair value of these instruments, the estimated values may not be representative of actual values that could have been realized or that will be realized in the near future.

Effect of Derivative Instruments on the Consolidated Statements of Operations

Derivative gains and (losses) were as follows for the periods indicated:

	Year ended December 31,					
	2015		2014		2013	
(in millions, pretax)	Interest Rate Contracts	Foreign Exchange Contracts	Interest Rate Contracts	Foreign Exchange Contracts	Interest Rate Contracts	Foreign Exchange Contracts
Derivatives in net investment hedging relationships:						
Gain recognized in OCI (effective portion)	$ —	$ 79	$ —	$ 80	$ —	$ 14
Derivatives not designated as hedging instruments						
Gain (loss) recognized in Other income (expense) in the consolidated statements of operations	$ (19)	$ 2	$ (4)	$ 4	$ (22)	$ (2)

Accumulated Derivative Gains and Losses

The following table summarizes activity in other comprehensive income for the years ended December 31, 2015, 2014, and 2013 related to derivative instruments classified as a net investment hedge held by the Company:

	Year ended December 31,		
(in millions, after tax)	2015	2014	2013
Accumulated gain (loss) included in other comprehensive income (loss) at beginning of the period	$ 37	$ (12)	$ (21)
Increase in fair value of derivatives that qualify for hedge accounting, net of tax (a)	49	49	9
Accumulated gain (loss) included in other comprehensive income (loss) at end of the period	$ 86	$ 37	$ (12)

(a) Gains and (losses) are included in "Unrealized gains (losses) on securities" and in "Foreign currency translation adjustment" on the consolidated statements of comprehensive income (loss).

Note 14: Commitments and Contingencies

Operating Leases

The Company leases certain of its facilities and equipment under operating lease agreements, substantially all of which contain renewal options and escalation provisions. The Company incurred total rent expense of $78 million, $77 million and $76 million for the years ended December 31, 2015, 2014 and 2013, respectively. Future minimum aggregate rental commitments as of December 31, 2015 under all noncancelable operating leases, net of sublease income are due in the following years:

Year ended December 31, (in millions)	Amount
2016	$ 56
2017	46
2018	39
2019	34
2020	24
Thereafter	110
Total	$ 309

Sublease income is earned from leased space and leased equipment which the Company concurrently subleases to third parties with comparable time periods. As of December 31, 2015, sublease amounts totaled less than $5 million in the Company's obligations. In addition, the Company has certain guarantees imbedded in leases and other agreements wherein the Company is required to relieve the counterparty in the event of changes in the tax code or rates. The Company believes the fair value of such guarantees is insignificant due to the likelihood and extent of the potential changes.

Letters of Credit

The Company has $42 million in outstanding letters of credit as of December 31, 2015, all of which were issued under the Company's senior secured revolving credit facility and expire prior to December 31, 2016 with a 1 year renewal option. The letters of credit are held in connection with lease arrangements, bankcard association agreements, and other security agreements. The Company expects to renew most of the letters of credit prior to expiration.

Legal

The Company is involved in various legal proceedings. Accruals have been made with respect to these matters, where appropriate, which are reflected in the Company's consolidated financial statements. The Company may enter into discussions regarding settlement of these matters, and may enter into settlement agreements, if it believes settlement is in the best interest of the Company. The matters discussed below, if decided adversely to or settled by the Company, individually or in the aggregate, may result in liability material to the Company's financial condition and/or results of operations.

There are asserted claims against the Company where an unfavorable outcome is considered to be reasonably possible. These claims can generally be categorized in the following areas: (1) patent infringement which results from claims that the Company is using technology that has been patented by another party; (2) merchant customer matters often associated with alleged processing errors or disclosure issues and claims that one of the subsidiaries of the Company has violated a federal or state requirement regarding credit reporting or collection in connection with its check verification guarantee, and collection activities; and (3) other matters which may include issues such as employment. The Company's estimates of the possible ranges of losses in excess of any amounts accrued are $0 to $20 million for patent infringement, $0 to $50 million for merchant customer matters, and $0 to $30 million for other matters, resulting in a total estimated range of possible losses of $0 to $100 million for all of the matters described above.

The estimated range of reasonably possible losses is based on information currently available and involves elements of judgment and significant uncertainties. As additional information becomes available and the resolution of the uncertainties becomes more apparent, it is possible that actual losses may exceed even the high end of the estimated range.

Other

In the normal course of business, the Company is subject to claims and litigation, including indemnification obligations to purchasers of former subsidiaries. Management of the Company believes that such matters will not have a material adverse effect on the Company's results of operations, liquidity or financial condition.

Contingent Consideration

Over the past 3 years, the Company completed several acquisitions in which contingent consideration was recorded. The transactions called for cash consideration as well as contingent payments for achievement of certain milestones. As part of the purchase price, the Company recorded a $29 million liability for the contingent consideration, of which $4 million was paid during the year ended December 31, 2015. During the year ended December 31, 2015, the Company evaluated the liability and decreased the fair value of the liability by $10 million, $15 million remained accrued as of December 31, 2015. This fair value measurement represents a Level 3 measurement as it is based on significant inputs not observable in the market. Significant judgment is employed in determining the appropriateness of these assumptions as of the acquisition date. The primary assumption is the estimated number of client locations that will be using the acquired software or technology in the next 3 years.

Note 15: Employee Benefit Plans

Defined Contribution Plans

The Company maintains defined contribution savings plans covering virtually all of the Company's U.S. employees and defined contribution pension plans for international employees primarily in the United Kingdom and Australia. The plans provide tax-deferred amounts for each participant, consisting of employee elective contributions, Company matching and discretionary Company contributions. Effective January 1, 2014, the Company suspended matching contributions for all U.S. participants. As a result, the U.S. Plan is no longer a safe harbor plan.

The following table presents the aggregate amounts charged to expense in connection with these plans:

Year ended December 31, (in millions)	Amount
2015	$ 12
2014	15
2013	46

Defined Benefit Plans

The Company has defined benefit pension plans which are frozen and covers certain full-time employees in the United Kingdom and the U.S. The Company also has separate plans covering certain employees located primarily in Germany, Greece, and Austria.

The Company contributed cash in the amount of $12 million, $15 million, and $37 million to defined benefit plans for the years ended December 31, 2015, 2014, and 2013, respectively.

The Company recognizes the funded status of its defined benefit pension plans, measured as the difference between the fair value of the plan assets and the projected benefit obligation, in the consolidated balance sheets, as follows:

	As of December 31,	
(in millions)	2015	2014
U.K. plan:		
Plan benefit obligations	$ (715)	$ (755)
Fair value of plan assets	783	836
Net pension assets (a)	68	81
U.S. and other foreign plans:		
Plan benefit obligations	(252)	(265)
Fair value of plan assets	154	163
Net pension liabilities (b)	(98)	(102)
Funded status of the plans	$ (30)	$ (21)

(a) Pension assets are included in "Other long-term assets" of the consolidated balance sheets.
(b) Pension liabilities are included in "Other long-term liabilities" of the consolidated balance sheets.

The accumulated benefit obligation for all defined benefit pension plans was $1.0 billion as of December 31, 2015 and 2014.

As of December 31, 2015, Plan assets are comprised of approximately 30% of Level 1 securities, 70% of Level 2 securities, and an immaterial amount of Level 3 securities which comprise less than 1% of total plan assets.

The Plan paid benefits in the amount of $41 million, $33 million, and $31 million to defined benefit plans for the periods ended December 31, 2015, 2014, and 2013, respectively. The estimated future benefit payments, which reflect expected future service, are expected to be as follows:

Year ended December 31, (in millions)	Amount
2016	$ 39
2017	39
2018	42
2019	43
2020	44
2021-2025	241

The Company's post-retirement health care and other insurance benefits for retired employees are limited and immaterial.

Note 16: Supplemental Financial Information

Supplemental Consolidated Statements of Operations Information

The following table details the components of "Other income (expense)" on the consolidated statements of operations:

	Year ended December 31,		
(in millions)	2015	2014	2013
Investment gains and (losses)	$ —	$ 100	$ 2
Derivative financial instruments gains and (losses)	(17)	—	(24)
Divestitures, net	5	2	(5)
Non-operating foreign currency gains and (losses)	41	59	(20)
Other income (expense)	$ 29	$ 161	$ (47)

Supplemental Consolidated Balance Sheet Information

	As of December 31,	
(in millions)	2015	2014
Other current assets:		
Prepaid expenses	$ 139	$ 75
Inventory	128	90
Other	114	38
Total Other current assets	$ 381	$ 203
Property and equipment:		
Land	$ 79	$ 83
Buildings	313	342
Leasehold improvements	79	55
Equipment and furniture	1,379	1,290
Equipment under capital lease	468	393
Property and equipment	2,318	2,163
Less: Accumulated depreciation	(1,367)	(1,233)
Total Property and equipment, net of accumulated depreciation	$ 951	$ 930
Accounts payable and accrued liabilities:		
Accounts payable	$ 238	$ 280
Accrued interest expense	132	443
Other accrued expenses	637	548
Other	632	525
Total Accounts payable and accrued liabilities	$ 1,639	$ 1,796

Note 17: Investment in Affiliates

Segment results include the Company's proportionate share of income from affiliates, which consist of unconsolidated investments accounted for under the equity method of accounting. The most significant of these affiliates are related to the Company's merchant bank alliance program.

A merchant alliance, as it pertains to investments accounted for under the equity method, is an agreement between the Company and a financial institution that combines the processing capabilities and management expertise of the Company with the visibility and distribution channel of the bank. The alliance acquires credit and debit card transactions from merchants. The Company provides processing and other services to the alliance and charges fees to the alliance primarily based on contractual pricing. These fees have been separately identified on the face of the consolidated statements of operations.

As of December 31, 2015, there were nine affiliates accounted for under the equity method of accounting, comprised of five merchant alliances and four strategic investments in companies in related markets.

The Wells Fargo alliance met the Significant Subsidiary test provided in Regulations S-X Rule 1-02 (w) in that the Company's equity earnings of this alliance exceeded 20% of the Company's consolidated income from continuing operations before income taxes for the year ended December 31, 2014.

A summary of financial information for the merchant alliances and other affiliates accounted for under the equity method of accounting is presented below.

	As of December 31,	
(in millions)	2015	2014
Total current assets	$ 3,002	$ 2,812
Total long-term assets	55	53
Total assets	$ 3,057	$ 2,865
Total current liabilities	$ 2,925	$ 2,742
Total long-term liabilities	16	17
Total liabilities	$ 2,941	$ 2,759

The primary components of assets and liabilities are settlement-related accounts similar to those described in note 11 "Settlement Assets and Obligations" of these consolidated financial statements.

	Year ended December 31,		
(in millions)	2015	2014	2013
Net operating revenues	$ 1,424	$ 1,357	$ 1,369
Operating expenses	666	638	675
Operating income	$ 758	$ 719	$ 694
Net income	$ 744	$ 696	$ 664
FDC equity earnings	239	220	188

The formation of a merchant alliance accounted for under the equity method of accounting generally involves the Company and/or a financial institution contributing merchant contracts to the alliance and a cash payment from one owner to the other to achieve the desired ownership percentages. The asset amounts reflected above are owned by the alliances and other equity method investees and do not include any of such payments made by the Company. The amount by which the total of the Company's investments in affiliates exceeded its proportionate share of the investees' net assets was approximately $1.0 billion and $1.1 billion as of December 31, 2015 and 2014, respectively.

The non-goodwill portion of this amount is considered an identifiable intangible asset that is amortized. The estimated future amortization expense for these intangible assets as of December 31, 2015 is as follows:

Year ended December 31, (in millions)	Amount
2016	$ 50
2017	44
2018	29
2019	4
2020	—
Thereafter	—

These amounts assume that these alliances continue as they currently exist. Much of the difference between the Company's proportionate share of the investees' net income and the Company's equity earnings noted above relates to this amortization.

Note 18: Supplemental Guarantor Condensed Consolidating Financial Statements

As described in note 2 "Borrowings" of these consolidated financial statements, FDC's 7.0% senior notes are guaranteed by most of the existing and future, direct and indirect, wholly owned, domestic subsidiaries of FDC (Guarantors). The Guarantors guarantee the senior secured revolving credit facility, senior secured term loan facility, the 5.0% senior secured notes, the 5.375% senior secured notes and the 6.75% senior secured notes, which rank senior in right of payment to all existing and future unsecured and second lien indebtedness of FDC's guarantor subsidiaries to the extent of the value of the collateral. The Guarantors guarantee the 8.75% and the 5.750% senior second lien notes which rank senior in right of payment to all existing and future unsecured indebtedness of FDC's guarantor subsidiaries to the extent of the value of the collateral. The 7.0% senior note guarantee is unsecured and ranks equally in right of payment with all existing and future senior indebtedness of the guarantor subsidiaries but senior in right of payment to all existing and future subordinated indebtedness of FDC's guarantor subsidiaries.

All of the above guarantees are full, unconditional, and joint and several and each of the Guarantors is 100% owned, directly or indirectly, by FDC. None of the other subsidiaries of FDC, either direct or indirect, guarantee the notes (Non-Guarantors). The Guarantors are subject to release under certain circumstances as described below.

The credit agreement governing the guarantees of the senior secured revolving credit facility and senior secured term loan facility provide for a Guarantor to be automatically and unconditionally released and discharged from its guarantee obligations in certain circumstances, including under the following circumstances:

- the Guarantor ceases to be a "restricted subsidiary" for purpose of the agreement because FDC no longer directly or indirectly owns 50% of the equity or, if a corporation, stock having voting power to elect a majority of the board of directors of the Guarantor; or
- the Guarantor is designated as an "unrestricted subsidiary" for purposes of the agreement covenants; or
- the Guarantor is no longer wholly owned by FDC subject to the value of all Guarantors released under this provision does not exceed (x) 10% of FDC's Covenant EBITDA plus (y) the amount of investments permitted under the agreement in respect of non-guarantors.

The indentures governing all of the other guarantees described above provide for a Guarantor to be automatically and unconditionally released and discharged from its guarantee obligations in certain circumstances, including upon the earliest to occur of:

- the sale, exchange or transfer of the subsidiary's capital stock or all or substantially all of its assets;
- designation of the Guarantor as an "unrestricted subsidiary" for purposes of the indenture covenants;
- release or discharge of the Guarantor's guarantee of certain other indebtedness; or
- legal defeasance or covenant defeasance of the indenture obligations when provision has been made for them to be fully satisfied.

The following tables present the results of operations, financial position, and cash flows of FDC (FDC Parent Company), the Guarantor subsidiaries, the Non-Guarantor subsidiaries and consolidation adjustments for the years ended December 31, 2015, 2014, and 2013 and as of December 31, 2015 and 2014 to arrive at the information for FDC on a consolidated basis.

	Year ended December 31, 2015				
(in millions)	FDC Parent Company	Guarantor Subsidiaries	Non-Guarantor Subsidiaries	Consolidation Adjustments	Consolidated
Revenues:					
Transaction and processing service fees	$ —	$ 3,906	$ 2,999	$ (308)	$ 6,597
Product sales and other	—	741	503	(77)	1,167
Total revenues (excluding reimbursable items)	—	4,647	3,502	(385)	7,764
Reimbursable PIN debit fees, postage, and other	—	2,521	1,166	—	3,687
Total revenues	—	7,168	4,668	(385)	11,451
Expenses:					
Cost of services (exclusive of items shown below)	—	1,576	1,473	(178)	2,871
Cost of products sold	—	260	173	(77)	356
Selling, general, and administrative	476	1,143	803	(130)	2,292
Depreciation and amortization	12	620	390	—	1,022
Other operating expenses	8	24	21	—	53
Total expenses (excluding reimbursable items)	496	3,623	2,860	(385)	6,594
Reimbursable PIN debit fees, postage, and other	—	2,521	1,166	—	3,687
Total expenses	496	6,144	4,026	(385)	10,281
Operating (loss) profit	(496)	1,024	642	—	1,170
Interest expense, net	(1,527)	(10)	—	—	(1,537)
Loss on debt extinguishment	(1,068)	—	—	—	(1,068)
Interest income (expense) from intercompany notes	288	(289)	1	—	—
Equity earnings from consolidated subsidiaries	810	304	—	(1,114)	—
Other income (expense)	55	3	(29)	—	29
(Loss) income before income taxes and equity earnings in affiliates	(1,938)	1,032	614	(1,114)	(1,406)
Income tax (benefit) expense	(457)	422	136	—	101
Equity earnings in affiliates	—	213	26	—	239
Net (loss) income	(1,481)	823	504	(1,114)	(1,268)
Less: Net income attributable to noncontrolling interests and redeemable noncontrolling interest	—	—	66	147	213
Net (loss) income attributable to First Data Corporation	$ (1,481)	$ 823	$ 438	$ (1,261)	$ (1,481)
Comprehensive (loss) income	$ (1,771)	$ 760	$ 158	$ (715)	$ (1,568)
Less: Comprehensive income attributable to noncontrolling interests and redeemable noncontrolling interest	—	—	56	147	203
Comprehensive (loss) income attributable to First Data Corporation	$ (1,771)	$ 760	$ 102	$ (862)	$ (1,771)

	Year ended December 31, 2014				
(in millions)	FDC Parent Company	Guarantor Subsidiaries	Non-Guarantor Subsidiaries	Consolidation Adjustments	Consolidated
Revenues:					
Transaction and processing service fees	$ —	$ 3,712	$ 3,056	$ (258)	$ 6,510
Product sales and other	—	625	473	(60)	1,038
Total revenues (excluding reimbursable items)	—	4,337	3,529	(318)	7,548
Reimbursable PIN debit fees, postage, and other	—	2,510	1,094	—	3,604
Total revenues	—	6,847	4,623	(318)	11,152
Expenses:					
Cost of services (exclusive of items shown below)	—	1,403	1,523	(258)	2,668
Cost of products sold	—	223	167	(60)	330
Selling, general, and administrative	131	1,125	787	—	2,043
Depreciation and amortization	10	607	439	—	1,056
Other operating expenses	10	3	—	—	13
Total expenses (excluding reimbursable items)	151	3,361	2,916	(318)	6,110
Reimbursable PIN debit fees, postage, and other	—	2,510	1,094	—	3,604
Total expenses	151	5,871	4,010	(318)	9,714
Operating (loss) profit	(151)	976	613	—	1,438
Interest expense, net	(1,724)	(9)	5	—	(1,728)
Loss on debt extinguishment	(274)	—	—	—	(274)
Interest income (expense) from intercompany notes	316	(305)	(11)	—	—
Equity earnings from consolidated subsidiaries	833	294	—	(1,127)	—
Other income (expense)	81	100	(20)	—	161
(Loss) income before income taxes and equity earnings in affiliates	(919)	1,056	587	(1,127)	(403)
Income tax (benefit) expense	(461)	377	166	—	82
Equity earnings in affiliates	—	202	18	—	220
Net (loss) income	(458)	881	439	(1,127)	(265)
Less: Net income attributable to noncontrolling interests and redeemable noncontrolling interest	—	—	66	127	193
Net (loss) income attributable to First Data Corporation	$ (458)	$ 881	$ 373	$ (1,254)	$ (458)
Comprehensive (loss) income	$ (798)	$ 709	$ 187	$ (714)	$ (616)
Less: Comprehensive income attributable to noncontrolling interests and redeemable noncontrolling interest	—	—	55	127	182
Comprehensive (loss) income attributable to First Data Corporation	$ (798)	$ 709	$ 132	$ (841)	$ (798)

	Year ended December 31, 2013				
(in millions)	FDC Parent Company	Guarantor Subsidiaries	Non-Guarantor Subsidiaries	Consolidation Adjustments	Consolidated
Revenues:					
Transaction and processing service fees	$ —	$ 3,585	$ 2,987	$ (227)	$ 6,345
Product sales and other	—	570	447	(60)	957
Total revenues (excluding reimbursable items)	—	4,155	3,434	(287)	7,302
Reimbursable PIN debit fees, postage, and other	—	2,510	997	—	3,507
Total revenues	—	6,665	4,431	(287)	10,809
Expenses:					
Cost of services (exclusive of items shown below)	—	1,508	1,442	(227)	2,723
Cost of products sold	—	217	171	(60)	328
Selling, general, and administrative	115	1,136	729	—	1,980
Depreciation and amortization	7	623	461	—	1,091
Other operating expenses	26	25	5	—	56
Total expenses (excluding reimbursable items)	148	3,509	2,808	(287)	6,178
Reimbursable PIN debit fees, postage, and other	—	2,510	997	—	3,507
Total expenses	148	6,019	3,805	(287)	9,685
Operating (loss) profit	(148)	646	626	—	1,124
Interest expense, net	(1,850)	(10)	4	—	(1,856)
Loss on debt extinguishment	(79)	—	—	—	(79)
Interest income (expense) from intercompany notes	315	(276)	(39)	—	—
Equity earnings from consolidated subsidiaries	579	207	—	(786)	—
Other income (expense)	(53)	(3)	9	—	(47)
(Loss) income before income taxes and equity earnings in affiliates	(1,236)	564	600	(786)	(858)
Income tax (benefit) expense	(284)	250	139	—	105
Equity earnings in affiliates	—	169	19	—	188
Net (loss) income	(952)	483	480	(786)	(775)
Less: Net income attributable to noncontrolling interests and redeemable noncontrolling interest	—	—	56	121	177
Net (loss) income attributable to First Data Corporation	$ (952)	$ 483	$ 424	$ (907)	$ (952)
Comprehensive (loss) income	$ (989)	$ 453	$ 388	$ (663)	$ (811)
Less: Comprehensive income attributable to noncontrolling interests and redeemable noncontrolling interest	—	—	57	121	178
Comprehensive (loss) income attributable to First Data Corporation	$ (989)	$ 453	$ 331	$ (784)	$ (989)

	As of December 31, 2015				
(in millions)	FDC Parent Company	Guarantor Subsidiaries	Non-Guarantor Subsidiaries	Consolidation Adjustments	Consolidated
ASSETS					
Current assets:					
Cash and cash equivalents	$ 105	$ 16	$ 308	$ —	$ 429
Accounts receivable, net of allowance for doubtful accounts	—	826	1,000	—	1,826
Settlement assets (a)	—	4,273	3,877	—	8,150
Intercompany notes receivable	436	86	10	(532)	—
Other current assets	98	188	95	—	381
Total current assets	639	5,389	5,290	(532)	10,786
Property and equipment, net of accumulated depreciation	37	640	274	—	951
Goodwill	—	9,139	7,707	—	16,846
Customer relationships, net of accumulated amortization	—	1,235	901	—	2,136
Other intangibles, net of accumulated amortization	604	703	476	—	1,783
Investment in affiliates	5	900	143	—	1,048
Long-term intercompany receivables	8,523	15,192	6,321	(30,036)	—
Long-term intercompany notes receivable	3,415	236	9	(3,660)	—
Deferred tax assets	524	—	—	(524)	—
Other long-term assets	259	358	265	(70)	812
Investment in consolidated subsidiaries	25,692	5,588	—	(31,280)	—
Total assets	$ 39,698	$ 39,380	$ 21,386	$ (66,102)	$ 34,362
LIABILITIES AND EQUITY					
Current liabilities:					
Accounts payable and accrued liabilities	$ 283	$ 792	$ 564	$ —	$ 1,639
Short-term and current portion of long-term borrowings	740	70	46	—	856
Settlement obligations (a)	—	4,273	3,877	—	8,150
Intercompany notes payable	96	408	28	(532)	—
Total current liabilities	1,119	5,543	4,515	(532)	10,645
Long-term borrowings	18,616	119	2	—	18,737
Deferred tax liabilities	—	875	80	(524)	431
Long-term intercompany payables	18,583	6,874	4,579	(30,036)	—
Long-term intercompany notes payable	245	3,353	62	(3,660)	—
Other long-term liabilities	467	288	127	(70)	812
Total liabilities	39,030	17,052	9,365	(34,822)	30,625
Redeemable equity interest	—	—	77	(77)	—
Redeemable noncontrolling interest	—	—	—	77	77
First Data Corporation stockholders' equity (deficit)	668	22,328	5,933	(28,261)	668
Noncontrolling interests	—	—	88	2,904	2,992
Equity of consolidated alliance	—	—	5,923	(5,923)	—
Total equity	668	22,328	11,944	(31,280)	3,660
Total liabilities and equity	$ 39,698	$ 39,380	$ 21,386	$ (66,102)	$ 34,362

(a) The majority of the Guarantor settlement assets relate to FDC's merchant acquiring business. FDC believes the settlement assets are not available to satisfy any claims other than those related to the settlement liabilities.

	As of December 31, 2014				
(in millions)	FDC Parent Company	Guarantor Subsidiaries	Non-Guarantor Subsidiaries	Consolidation Adjustments	Consolidated
ASSETS					
Current assets:					
Cash and cash equivalents	$ —	$ 23	$ 335	$ —	$ 358
Accounts receivable, net of allowance for doubtful accounts	8	729	1,004	—	1,741
Settlement assets (a)	—	3,849	3,706	—	7,555
Intercompany notes receivable	3,375	307	—	(3,682)	—
Other current assets	5	96	102	—	203
Total current assets	3,388	5,004	5,147	(3,682)	9,857
Property and equipment, net of accumulated depreciation	33	619	278	—	930
Goodwill	—	9,085	7,932	—	17,017
Customer relationships, net of accumulated amortization	—	1,469	1,135	—	2,604
Other intangibles, net of accumulated amortization	603	623	519	—	1,745
Investment in affiliates	—	948	153	—	1,101
Long-term intercompany receivables	6,064	14,442	5,135	(25,641)	—
Long-term intercompany notes receivable	320	1	9	(330)	—
Deferred tax assets	710	—	—	(710)	—
Other long-term assets	265	317	295	(97)	780
Investment in consolidated subsidiaries	24,474	5,331	—	(29,805)	—
Total assets	$ 35,857	$ 37,839	$ 20,603	$ (60,265)	$ 34,034
LIABILITIES AND EQUITY					
Current liabilities:					
Accounts payable and accrued liabilities	$ 592	$ 699	$ 505	$ —	$ 1,796
Short-term and current portion of long-term borrowings	20	64	77	—	161
Settlement obligations (a)	—	3,849	3,708	—	7,557
Intercompany notes payable	309	3,346	27	(3,682)	—
Total current liabilities	921	7,958	4,317	(3,682)	9,514
Long-term borrowings	20,564	131	2	—	20,697
Deferred tax liabilities	—	1,001	144	(710)	435
Long-term intercompany payables	14,397	7,804	3,440	(25,641)	—
Long-term intercompany notes payable	9	260	61	(330)	—
Other long-term liabilities	536	225	124	(97)	788
Total liabilities	36,427	17,379	8,088	(30,460)	31,434
Redeemable equity interest	—	—	70	(70)	—
Redeemable noncontrolling interest	—	—	—	70	70
First Data Corporation stockholders' (deficit) equity	(570)	20,460	6,241	(26,701)	(570)
Noncontrolling interests	—	—	101	2,999	3,100
Equity of consolidated alliance	—	—	6,103	(6,103)	—
Total equity	(570)	20,460	12,445	(29,805)	2,530
Total liabilities and equity	$ 35,857	$ 37,839	$ 20,603	$ (60,265)	$ 34,034

(a) The majority of the Guarantor settlement assets relate to FDC's merchant acquiring business. FDC believes the settlement assets are not available to satisfy any claims other than those related to the settlement liabilities.

	Year ended December 31, 2015				
(in millions)	FDC Parent Company	Guarantor Subsidiaries	Non-Guarantor Subsidiaries	Consolidation Adjustments	Consolidated
CASH FLOWS FROM OPERATING ACTIVITIES					
Net (loss) income	$ (1,481)	$ 823	$ 504	$ (1,114)	$ (1,268)
Adjustments to reconcile to net cash (used in) provided by operating activities:					
Depreciation and amortization (including amortization netted against equity earnings in affiliates and revenues)	12	701	420	—	1,133
(Gains) charges related to other operating expenses and other income (expense)	(47)	21	50	—	24
Loss on debt extinguishment	1,068	—	—	—	1,068
Share-based compensation expense	329	—	—	—	329
Other non-cash and non-operating items, net	(762)	(306)	(14)	1,114	32
(Decrease) increase in cash, excluding the effects of acquisitions and dispositions, resulting from changes in operating assets and liabilities	(1,028)	431	74	—	(523)
Net cash (used in) provided by operating activities	(1,909)	1,670	1,034	—	795
CASH FLOWS FROM INVESTING ACTIVITIES					
Proceeds from dispositions, net of expenses paid	—	4	—	—	4
Additions to property and equipment	(9)	(107)	(166)	—	(282)
Payments to secure customer service contracts, including outlays for conversion, and capitalized systems development costs	—	(264)	(56)	—	(320)
Acquisitions, net of cash acquired	(70)	(19)	—	—	(89)
Proceeds from sale of property and equipment	—	17	—	—	17
Purchase of investments	(17)	—	—	—	(17)
Other investing activities	2	—	—	—	2
Distributions and dividends from subsidiaries	149	254	—	(403)	—
Net cash provided by (used in) investing activities	55	(115)	(222)	(403)	(685)
CASH FLOWS FROM FINANCING ACTIVITIES					
Short-term borrowings, net	(10)	—	(21)	—	(31)
Proceeds from issuance of long-term debt	10,258	—	—	—	10,258
Payment of call premiums and debt issuance cost	(1,062)	—	—	—	(1,062)
Principal payments on long-term debt	(11,472)	(87)	(9)	—	(11,568)
Proceeds from issuance of common stock	2,718	—	—	—	2,718
Distributions and dividends paid to noncontrolling interests and redeemable noncontrolling interest	—	—	(69)	(243)	(312)
Distributions paid to equity holders	—	—	(497)	497	—
Capital transactions, net	(19)	—	(149)	149	(19)
Intercompany	1,546	(1,477)	(69)	—	—
Net cash provided by (used in) financing activities	1,959	(1,564)	(814)	403	(16)
Effect of exchange rate changes on cash and cash equivalents	—	2	(25)	—	(23)
Change in cash and cash equivalents	105	(7)	(27)	—	71
Cash and cash equivalents at beginning of period	—	23	335	—	358
Cash and cash equivalents at end of period	$ 105	$ 16	$ 308	$ —	$ 429

	Year ended December 31, 2014				
(in millions)	FDC Parent Company	Guarantor Subsidiaries	Non-Guarantor Subsidiaries	Consolidation Adjustments	Consolidated
CASH FLOWS FROM OPERATING ACTIVITIES					
Net (loss) income	$ (458)	$ 881	$ 439	$ (1,127)	$ (265)
Adjustments to reconcile to net cash (used in) provided by operating activities:					
Depreciation and amortization (including amortization netted against equity earnings in affiliates and revenues)	10	683	470	—	1,163
(Gains) charges related to other operating expenses and other income (expense)	(71)	(97)	20	—	(148)
Loss on debt extinguishment	274	—	—	—	274
Share-based compensation expense	51	—	—	—	51
Other non-cash and non-operating items, net	(788)	(306)	—	1,127	33
(Decrease) increase in cash resulting from changes in operating assets and liabilities, excluding the effects of acquisitions and dispositions	(694)	571	50	—	(73)
Net cash (used in) provided by operating activities	(1,676)	1,732	979	—	1,035
CASH FLOWS FROM INVESTING ACTIVITIES					
Proceeds from dispositions, net of expenses paid and cash disposed	—	270	—	—	270
Additions to property and equipment	(8)	(124)	(176)	—	(308)
Payments to secure customer service contracts, including outlays for conversion, and capitalized systems development costs	—	(183)	(76)	—	(259)
Acquisitions, net of cash acquired	—	(31)	—	—	(31)
Proceeds from sale of property and equipment	—	2	1	—	3
Other investing activities	—	—	(4)	—	(4)
Distributions and dividends from subsidiaries	75	232	—	(307)	—
Net cash provided by (used in) investing activities	67	166	(255)	(307)	(329)
CASH FLOWS FROM FINANCING ACTIVITIES					
Short-term borrowings, net	10	—	2	—	12
Proceeds from issuance of long-term debt	1,830	—	—	—	1,830
Payment of call premiums and debt issuance cost	(355)	—	—	—	(355)
Principal payments on long-term debt	(3,673)	(73)	(5)	—	(3,751)
Distributions and dividends paid to noncontrolling interests and redeemable noncontrolling interest	—	—	(45)	(221)	(266)
Distributions paid to equity holders	—	—	(453)	453	—
Purchase of noncontrolling interest	—	—	(1)	—	(1)
Capital transactions, net	1,788	—	(75)	75	1,788
Intercompany	1,973	(1,840)	(133)	—	—
Net cash provided by (used in) financing activities	1,573	(1,913)	(710)	307	(743)
Effect of exchange rate changes on cash and cash equivalents	—	5	(35)	—	(30)
Change in cash and cash equivalents	(36)	(10)	(21)	—	(67)
Cash and cash equivalents at beginning of period	36	33	356	—	425
Cash and cash equivalents at end of period	$ —	$ 23	$ 335	$ —	$ 358

(in millions)	Year ended December 31, 2013				
	FDC Parent Company	Guarantor Subsidiaries	Non-Guarantor Subsidiaries	Consolidation Adjustments	Consolidated
CASH FLOWS FROM OPERATING ACTIVITIES					
Net (loss) income	$ (952)	$ 483	$ 480	$ (786)	$ (775)
Adjustments to reconcile to net cash (used in) provided by operating activities:					
Depreciation and amortization (including amortization netted against equity earnings in affiliates and revenues)	7	715	490	—	1,212
Charges (gains) related to other operating expenses and other income (expense)	79	28	(4)	—	103
Loss on debt extinguishment	79	—	—	—	79
Share-based compensation expense	39	—	—	—	39
Other non-cash and non-operating items, net	(537)	(214)	(9)	786	26
(Decrease) increase in cash resulting from changes in operating assets and liabilities, excluding the effects of acquisitions and dispositions	(406)	321	116	—	31
Net cash (used in) provided by operating activities	(1,691)	1,333	1,073	—	715
CASH FLOWS FROM INVESTING ACTIVITIES					
Proceeds from dispositions, net of expenses paid	—	10	8	—	18
Additions to property and equipment	—	(68)	(126)	—	(194)
Payments to secure customer service contracts, including outlays for conversion, and capitalized systems development costs	(1)	(124)	(60)	—	(185)
Acquisitions, net of cash acquired	(12)	—	—	—	(12)
Proceeds from sale of property and equipment	—	5	7	—	12
Other investing activities	—	7	1	—	8
Distributions and dividends from subsidiaries	178	190	—	(368)	—
Net cash provided by (used in) investing activities	165	20	(170)	(368)	(353)
CASH FLOWS FROM FINANCING ACTIVITIES					
Short-term borrowings, net	—	—	(109)	—	(109)
Proceeds from issuance of long-term debt	4,472	—	—	—	4,472
Payment of call premiums and debt issuance cost	(111)	—	—	—	(111)
Principal payments on long-term debt	(4,429)	(67)	(10)	—	(4,506)
Distributions and dividends paid to noncontrolling interests and redeemable noncontrolling interest	—	—	(41)	(183)	(224)
Distributions paid to equity holders	—	—	(373)	373	—
Purchase of noncontrolling interest	—	—	(24)	—	(24)
Capital transactions, net	(30)	—	(178)	178	(30)
Intercompany	1,433	(1,274)	(159)	—	—
Net cash provided by (used in) financing activities	1,335	(1,341)	(894)	368	(532)
Effect of exchange rate changes on cash and cash equivalents	—	(2)	(11)	—	(13)
Change in cash and cash equivalents	(191)	10	(2)	—	(183)
Cash and cash equivalents at beginning of period	227	23	358	—	608
Cash and cash equivalents at end of period	$ 36	$ 33	$ 356	$ —	$ 425

Note 19: Quarterly Financial Results (Unaudited)

Summarized quarterly results for the two years ended December 31, 2015 and 2014, respectively, are as follows:

	2015			
(in millions, except per share amounts)	**First**	**Second**	**Third**	**Fourth**
Revenues	$ 2,695	$ 2,872	$ 2,920	$ 2,964
Expenses	2,435	2,463	2,518	2,865
Operating profit	$ 260	$ 409	$ 402	$ 99
Net (loss) income	$ (63)	$ 33	$ (75)	$ (1,163)
Net loss attributable to First Data Corporation	(112)	(26)	(126)	(1,217)
Net loss per share, basic and diluted (a)	(112,000)	(26,000)	(126,000)	(1.60)

	2014			
(in millions, except per share amounts)	**First**	**Second**	**Third**	**Fourth**
Revenues	$ 2,640	$ 2,837	$ 2,792	$ 2,883
Expenses	2,355	2,455	2,439	2,465
Operating profit	$ 285	$ 382	$ 353	$ 418
Net (loss) income	$ (165)	$ 23	$ (188)	$ 65
Net (loss) income attributable to First Data Corporation	(201)	(34)	(235)	12
Net (loss) income per share, basic and diluted (a)	(201,000)	(34,000)	(235,000)	12,000

(a) As a result of the prospective treatment of the HoldCo Merger, as discussed within note 1 "Summary of Significant Accounting Policies", net loss per share was computed using 1,000 shares outstanding for the first, second, and third quarters of 2015 and 763 million for the fourth quarter of 2015.

FIRST DATA CORPORATION
SCHEDULE II—Valuation and Qualifying Accounts

Description	Balance at Beginning of Period	Additions		Deductions	Balance at End of Period
		Charged to Costs and Expenses	Reclassifications from Other Accounts (a)	Write-offs Against Assets	
Year ended December 31, 2015 deducted from receivables	$ 72	$ 79	$ 3	$ 71	$ 83
Year ended December 31, 2014 deducted from receivables	43	99	11	81	72
Year ended December 31, 2013 deducted from receivables	46	93	—	96	43

(a) Amounts related to reclassifications from "Accounts payable and accrued liabilities" to "Allowance for doubtful accounts" in the Company's consolidated balance sheets.

ITEM 9. CHANGES IN AND DISAGREEMENTS WITH ACCOUNTANTS ON ACCOUNTING AND FINANCIAL DISCLOSURE

None.

ITEM 9A. CONTROLS AND PROCEDURES

Evaluation of Disclosure Controls and Procedures

We have evaluated, under the supervision of our Chief Executive Officer and our Chief Financial Officer, the effectiveness of disclosure controls and procedures as of December 31, 2015. This is done in order to ensure that information we are required to disclose in reports that are filed or submitted under the Securities Exchange Act of 1934 is recorded, processed, summarized, and reported within the time periods specified in SEC rules and forms.

Management's Report on Internal Control over Financial Reporting

Report of Management

Our management is responsible for establishing and maintaining adequate internal control over financial reporting as defined in Rules 13a-15(f) and 15d-15(f) under the Securities Exchange Act of 1934. Our internal control over financial reporting is designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles.

Internal Control over Financial Reporting

Management is also responsible for establishing and maintaining effective internal control over financial reporting. Internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with U.S. generally accepted accounting principles. The Company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the Company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with U.S. generally accepted accounting principles, and that receipts and expenditures of the Company are being made only in accordance with authorizations of management and directors of the Company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the Company's assets that could have a material effect on the financial statements. Management recognizes that there are inherent limitations in the effectiveness of any internal control over financial reporting, including the possibility of human error and the circumvention or overriding of internal control. Accordingly, even effective internal control over financial reporting can provide only reasonable assurance with respect to financial statement preparation. Further, because of changes in conditions, the effectiveness of internal control over financial reporting may vary over time.

In order to ensure that the Company's internal control over financial reporting is effective, management regularly assesses such controls and did so most recently as of December 31, 2015. This assessment was based on criteria for effective internal control over financial reporting described in Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework). Based on this assessment, management believes the Company maintained effective internal control over financial reporting as of December 31, 2015.

Ernst & Young LLP, an independent registered public accounting firm, has issued an attestation report on our internal control over financial reporting which is contained herein.

Changes in Internal Control over Financial Reporting

During the third quarter of 2015, we commenced the migration of certain activities in connection with our strategic expense management initiative. This migration presents transitional risks to maintaining adequate internal controls over financial reporting.

There were no changes in our internal control over financial reporting identified in connection with the above evaluation that occurred during the last fiscal quarter that has materially affected, or is reasonably likely to materially affect, our internal control over financial reporting.

Report of Independent Registered Public Accounting Firm

The Board of Directors and Stockholders of First Data Corporation

We have audited First Data Corporation's internal control over financial reporting as of December 31, 2015, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework) (the COSO criteria). First Data Corporation's management is responsible for maintaining effective internal control over financial reporting, and for its assessment of the effectiveness of internal control over financial reporting included in the accompanying Management's Report on Internal Control over Financial Reporting. Our responsibility is to express an opinion on the company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, First Data Corporation maintained, in all material respects, effective internal control over financial reporting as of December 31, 2015, based on the COSO criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the consolidated balance sheets of First Data Corporation as of December 31, 2015 and 2014, and the related consolidated statements of operations, comprehensive income (loss), cash flows and equity for each of the three years in the period ended December 31, 2015 of First Data Corporation and our report dated February 25, 2016 expressed an unqualified opinion thereon.

/s/ Ernst & Young LLP

Atlanta, Georgia
February 25, 2016

ITEM 9B. OTHER INFORMATION

None.

PART III

ITEM 10. DIRECTORS, EXECUTIVE OFFICERS, AND CORPORATE GOVERNANCE

All information required by this Item is incorporated by reference to our Proxy Statement for the 2016 Annual Meeting of Shareholders to be filed with the U.S. Securities and Exchange Commission within 120 days after December 31, 2015.

ITEM 11. EXECUTIVE COMPENSATION

The information required by this Item is incorporated by reference to our Proxy Statement for the 2016 Annual Meeting of Shareholders to be filed with the SEC within 120 days after December 31, 2015 and is incorporated herein by reference.

ITEM 12. SECURITY OWNERSHIP OF CERTAIN BENEFICIAL OWNERS AND MANAGEMENT AND RELATED STOCKHOLDER MATTERS

The information required by this Item is incorporated by reference to our Proxy Statement for the 2016 Annual Meeting of Shareholders to be filed with the SEC within 120 days after December 31, 2015 and is incorporated herein by reference.

ITEM 13. CERTAIN RELATIONSHIPS AND RELATED TRANSACTIONS, AND DIRECTOR INDEPENDENCE

The information required by this Item is incorporated by reference to our Proxy Statement for the 2016 Annual Meeting of Shareholders to be filed with the SEC within 120 days after December 31, 2015 and is incorporated herein by reference.

ITEM 14. PRINCIPAL ACCOUNTANT FEES AND SERVICES

The information required by this Item is incorporated by reference to our Proxy Statement for the 2016 Annual Meeting of Shareholders to be filed with the SEC within 120 days after December 31, 2015 and is incorporated herein by reference.

PART IV

ITEM 15. EXHIBITS, FINANCIAL STATEMENT SCHEDULES

(a) The following documents are filed as part of this report:

(1) Financial Statements

See Index to Financial Statements on page 56.

(2) Financial Statement Schedules

See Index to Financial Statements on page 56.

(3) Those exhibits required by Item 601 of Regulation S-K and by paragraph (b) below.

(b) The following exhibits are filed as part of this Annual Report or, where indicated, were filed and are incorporated by reference:

		Incorporated by Reference			
Exhibit Number	**Exhibit Description**	**Form**	**File Number**	**Exhibit Number**	**Filing Date**
3(i)	Ninth Amended and Restated Certificate of Incorporation	8-K	1-11073	3.1	10/19/2015
3(ii)	Amended and Restated By-laws	S-1/A	1-11073	3.2	10/1/2015
4.1	Indenture, dated as August 16, 2012, by and among First Data Corporation, the guarantors named therein and Wells Fargo Bank, National Association, as trustee, governing the 6.750% Senior Secured Notes due 2020	8-K	1-11073	10.2	8/20/2012
4.2	First Supplemental Indenture, dated as September 27, 2012, by and among First Data Corporation, the guarantors named therein and Wells Fargo Bank, National Association, as trustee, governing the additional 6.750% Senior Secured Notes due 2020	8-K	1-11073	10.2	10/2/2012
4.3	Indenture, dated as of February 13, 2013, by and among First Data Corporation, the guarantors named therein and Wells Fargo Bank, National Association, as trustee, governing the 11.25% Senior Notes due 2021	8-K	1-11073	4.1	2/13/2013
4.4	Indenture, dated as of August 11, 2015, among First Data Corporation, the subsidiary guarantors named therein and Wells Fargo Bank, National Association, as trustee, governing the 5.375% Senior Secured Notes Due 2023	8-K	1-11073	4.1	8/13/2015
4.5	Indenture, dated as November 18, 2015, by and among the Company, the guarantors named therein and Wells Fargo Bank, National Association, as trustee, governing the 7.000% Senior Notes due 2023	8-K	1-11073	4.1	11/20/2015
4.6	Indenture, dated as November 25, 2015, by and among the Company, the guarantors named therein and Wells Fargo Bank, National Association, as trustee, governing the 5.000% Senior Secured Notes due 2024	8-K	1-11073	4.1	12/1/2015

4.7	Indenture, dated as November 25, 2015, by and among the Company, the guarantors named therein and Wells Fargo Bank, National Association, as trustee, governing the 5.750% Senior Secured Second Lien Notes due 2024	8-K	1-11073	4.4	12/1/2015
4.8	Credit Agreement, dated as of September 24, 2007, as amended and restated as of September 28, 2007 among First Data Corporation, the several lenders from time to time parties thereto, Credit Suisse, Cayman Islands Branch, as administrative agent, swingline lender and letter of credit issuer, Citibank, N.A., as syndication agent, and Credit Suisse Securities (USA) LLC, Citigroup Global Markets, Inc., Deutsche Bank Securities Inc., Goldman Sachs Credit Partners L.P., HSBC Securities (USA) Inc., Lehman Brothers Inc. and Merrill Lynch, Pierce, Fenner & Smith Incorporated, as joint lead arrangers and bookrunners	10-K	1-11073	10.1	3/13/2008
4.9	Guarantee Agreement, dated September 24, 2007, among First Data Corporation, the subsidiaries of First Data Corporation identified therein and Credit Suisse, Cayman Islands Branch, as Collateral Agent	10-Q	1-11073	10.11	11/14/2007
4.10	Pledge Agreement, dated September 24, 2007, among First Data Corporation, the subsidiaries of First Data Corporation identified therein, and Credit Suisse, Cayman Islands Branch, as Collateral Agent	10-Q	1-11073	10.12	11/14/2007
4.11	Security Agreement, dated September 24, 2007, among First Data Corporation, the subsidiaries of First Data Corporation identified therein, and Credit Suisse, Cayman Islands Branch, as Collateral Agent	10-Q	1-11073	10.13	11/14/2007
4.12	2015 June Joinder Agreement, dated as of July 10, 2015, among the Company, certain of its subsidiaries, the lender party thereto, and Credit Suisse AG, Cayman Islands Branch, as administrative agent and collateral agent Exhibit B-Marked Pages of the Conformed Credit Agreement	8-K	1-11073	4.1	7/15/2015
4.13	Amended and Restated Pledge Agreement, dated as of August 11, 2015, among First Data Corporation, the other pledgors named therein and Wells Fargo Bank, National Association, as collateral agent	8-K	1-11073	4.3	8/13/2015
4.14	Amended and Restated Security Agreement, dated as of August 11, 2015, among First Data Corporation, the other grantors named therein and Wells Fargo Bank, National Association, as collateral agent	8-K	1-11073	4.2	8/13/2015
4.15	2015 November Joinder Agreement, dated as of November 24, 2015, among the Company, certain of its subsidiaries, the lender party thereto, and Credit Suisse AG, Cayman Islands Branch, as administrative agent and collateral agent Exhibit B - Marked Pages of the Conformed Credit Agreement	8-K	1-11073	4.7	12/1/2015

4.16	Amended and Restated Security Agreement, dated as of November 25, 2015, among the Company, the other grantors named therein and Wells Fargo Bank, National Association, as collateral agent	8-K	1-11073	4.5	12/1/2015
4.17	Amended and Restated Pledge Agreement, dated as of November 25, 2015, among the Company, the other pledgors named therein and Wells Fargo Bank, National Association, as collateral agent	8-K	1-11073	4.6	12/1/2015
4.18	Registration Rights Agreement, dated as of September 24, 2007 with New Omaha Holdings L.P. and other Investors party thereto	S-1/A	1-11073	4.22	8/25/2015
10.1	Management Agreement, dated September 24, 2007, among First Data Corporation, Kohlberg Kravis Roberts & Co. L.P. and New Omaha Holdings L.P.	10-Q	1-11073	10.10	11/14/2007
10.2	Stockholders Agreement, dated as of July 11, 2014 with New Omaha Holdings L.P. and other Holders party thereto	S-1/A	1-11073	10.15	8/25/2015
10.3	Form of Sale Participation Agreement	10-Q	1-11073	10.8	11/14/2007
10.4 *	Form of Management Stockholder's Agreement for Executive Committee Members (as amended)	10-K	1-11073	10.16	3/19/2013
10.5 *	Form of Management Stockholder's Agreement	S-1	1-11073	10.18	7/20/2015
10.6 *	First Data Corporation Senior Executive Incentive Plan as amended and restated effective January 1, 2014	10-K	1-11073	10.21	3/10/2014
10.7 *	2007 Stock Incentive Plan for Key Employees of First Data Corporation and its Affiliates, as amended	10-K	1-11073	10.10	2/27/2015
10.8 *	Form of Stock Option Agreement for Executive Committee Members	10-Q	1-11073	10.6	11/14/2007
10.9 *	Form of Stock Option Agreement	8-K	1-11073	10.3	5/25/2010
10.10 *	Form of Stock Option Agreement for U.S. Employees effective for grants in or after January 2014	S-1	1-11073	10.16	7/20/2015
10.11 *	Form of Restricted Stock Agreement for Management Committee effective for grants in or after January 2014	S-1	1-11073	10.17	7/20/2015
10.12 *	Form of Restricted Stock Award Agreement	8-K	1-11073	10.2	5/25/2010
10.13 *	First Data Corporation 2015 Omnibus Incentive Plan	8-K	1-11073	10.1	10/19/2015
10.14 *	Form of Option Grant Notice and Option Grant Agreement under the 2015 Omnibus Incentive Plan	S-1/A	1-11073	10.21	10/1/2015
10.15 *	Form of Restricted Stock Grant Notice and Restricted Stock Grant Agreement under the 2015 Omnibus Incentive Plan	S-1/A	1-11073	10.22	10/1/2015
10.16 * (1)	Form of Option Agreement under the 2015 Omnibus Incentive Plan for Management Committee and Directors				

10.17 * (1)	Form of Restricted Stock Award Agreement under the 2015 Omnibus Incentive Plan for Management Committee and Directors				
10.18 *	Form of IPO Cash Bonus Letter Agreement	S-1/A	1-11073	10.23	10/1/2015
10.19 *	First Data Corporation Severance / Change in Control Policy (Management Committee Level), as amended and restated effective January 1, 2015	10-K	1-11073	10.11	2/27/2015
10.20 * (1)	Description of Compensation of Directors				
10.21 *	2008 Non-Employee Director Deferred Compensation Plan	S-4	1-11073	10.25	8/13/2008
10.22 *	Employment Agreement with Frank J. Bisignano effective September 18, 2015	8-K	1-11073	10.1	9/24/2015
10.23	Receivables Financing Agreement dated December 31, 2015 between First Data Corporation, First Data Receivables, LLC, PNC Bank, National Association, and the persons from time to time party thereto as Lenders and Group Agents	8-K	1-11073	10.1	1/7/2016
10.24	Transfer and Contribution Agreement dated December 31, 2015 between First Data Corporation, First Data Receivables, LLC, First Data Resources, LLC, Remitco LLC, TeleCheck Services, Inc., Star Networks, Inc., Star Processing, Inc., Instant Cash Services, LLC, TASQ Technology, Inc., First Data Government Solutions, Inc., and First Data Government Solutions, LP	8-K	1-11073	10.2	1/7/2016
21 (1)	Subsidiaries of First Data Corporation				
23.1 (1)	Consent of Ernst & Young LLP, Independent Registered Public Accounting Firm				
23.2 (1)	Consent of KPMG LLP, Independent Registered Public Accounting Firm				
31.1 (1)	Certification of CEO pursuant to rule 13a-14(a) or 15d-14(a) of the Exchange Act, as adopted pursuant to Section 302 of the Sarbanes-Oxley Act of 2002				
31.2 (1)	Certification of CFO pursuant to rule 13a-14(a) or 15d-14(a) of the Exchange Act, as adopted pursuant to Section 302 of the Sarbanes-Oxley Act of 2002				
32.1 (1)	Certification of CEO pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002				
32.2 (1)	Certification of CFO pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002				
101.INS (1)	XBRL Instance Document				
101.SCH (1)	XBRL Taxonomy Extension Schema Document				
101.CAL (1)	XBRL Taxonomy Extension Calculation Linkbase Document				

101.DEF (1)	XBRL Taxonomy Extension Definitions Linkbase Document
101.LAB (1)	XBRL Taxonomy Extension Label Linkbase Document
101.PRE (1)	XBRL Taxonomy Extension Presentation Linkbase Document

(1) Filed herewith

* Management contracts and compensatory plans and arrangements required to be filed as exhibits pursuant to Item 15(b) of this report.

(c) The following financial statements are included in this annual report pursuant to Regulations S-X Rule 3-09:

(1) Wells Fargo Merchant Services, LLC
(A Joint Venture)
Financial Statements
December 31, 2015 and 2014
(With Independent Auditors' Report Thereon)

WELLS FARGO MERCHANT SERVICES, LLC

(A Joint Venture)

Financial Statements

December 31, 2015 and 2014

(With Independent Auditors' Report Thereon)

WELLS FARGO MERCHANT SERVICES, LLC
(A Joint Venture)
Financial Statements
December 31, 2015 and 2014

Table of Contents

	Page
Independent Auditors' Report	119
Balance Sheets	121
Statements of Revenues and Expenses	122
Statements of Members' Equity	123
Statements of Cash Flows	124
Notes to Financial Statements	125

KPMG LLP
Suite 1400
55 Second Street
San Francisco, CA 94105

Independent Auditors' Report

The Members and Board of Directors of
Wells Fargo Merchant Services, LLC:

We have audited the accompanying financial statements of Wells Fargo Merchant Services, LLC (the Company), which comprise the balance sheets as of December 31, 2015 and 2014, and the related statements of revenues and expenses, members' equity, and cash flows for the years then ended, and the related notes to the financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with U.S. generally accepted accounting principles; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

KPMG LLP is a Delaware limited liability partnership,
the U.S. member firm of KPMG International Cooperative
("KPMG International"), a Swiss entity.

Opinion

In our opinion, the financial statements referred to above present fairly in all material respects, the financial position of Wells Fargo Merchant Services, LLC, as of December 31, 2015 and 2014, and the results of its operations and its cash flows for the years then ended in accordance with U.S. generally accepted accounting principles.

KPMG LLP

San Francisco, California February 19, 2016

WELLS FARGO MERCHANT SERVICES, LLC
(A Joint Venture)
Balance Sheets
December 31, 2015 and 2014
(Dollars in thousands)

Assets	2015	2014
Cash and cash equivalents	$ 52,089	$ 64,403
Settlement assets	1,258,031	1,045,533
Accounts receivable, net of reserve for merchant credit losses of $5.2 million in 2015 and $4.5 million 2014	400,827	316,446
Intangibles	457	479
Other assets	144	12
Total assets	$ 1,711,548	$ 1,426,873
Liabilities and Members' Equity		
Settlement liabilities	$ 1,171,815	$ 977,144
Accounts payable and accrued expenses	43,952	30,465
Interchange payable to Wells Fargo Bank, N.A.	340,437	280,982
Related party payable to First Data Merchant Services Corporation	23,200	13,664
Distribution payable to Wells Fargo Bank, N.A.	76,532	72,016
Distribution payable to First Data Merchant Services Corporation	51,021	48,011
Total liabilities	1,706,957	1,422,282
Members' equity	4,591	4,591
Total liabilities and members' equity	$ 1,711,548	$ 1,426,873

See accompanying notes to financial statements.

WELLS FARGO MERCHANT SERVICES, LLC
(A Joint Venture)
Statements of Revenues and Expenses
December 31, 2015 and 2014

(Dollars in thousands)

	2015	2,014
Revenues:		
Card services revenue, net of $4.3 billion and $3.5 billion in interchange and assessments in 2015 and 2014, respectively	$ 762,608	$ 704,972
Product sales revenue	70,635	54,593
Other revenue	60,777	53,612
Net revenue	894,020	813,177
Expenses:		
Cost of card services	202,769	186,955
Cost of product sold	21,464	16,141
Selling, general and administrative	145,197	132,520
Other expenses	11,160	8,734
Total expenses	380,590	344,350
Net operating income	513,430	468,827
Interest income	695	1,338
Net income	$ 514,125	$ 470,165

See accompanying notes to financial statements.

WELLS FARGO MERCHANT SERVICES, LLC
(A Joint Venture)
Statements of Members' Equity
December 31, 2015 and 2014
(Dollars in thousands)

	Wells Fargo Bank, N.A.	First Data Merchant Services Corporation	Total
Members' equity at December 31, 2013	$ 2,755	$ 1,836	$ 4,591
Net income	282,099	188,066	470,165
Distributions to members	(282,099)	(188,066)	(470,165)
Members' equity at December 31, 2014	2,755	1,836	4,591
Net income	308,475	205,650	514,125
Distributions to members	(308,475)	(205,650)	(514,125)
Members' equity at December 31, 2015	$ 2,755	$ 1,836	$ 4,591

See accompanying notes to financial statements.

WELLS FARGO MERCHANT SERVICES, LLC
(A Joint Venture)
Statements of Cash Flows
December 31, 2015 and 2014
(Dollars in thousands)

	2015	2014
Cash flows from operating activities:		
Net income	$ 514,125	$ 470,165
Adjustments to reconcile net income to net cash provided by operating activities:		
Amortization of intangibles	318	298
Provisions for merchant credit losses	13,108	10,375
Changes in operating assets and liabilities:		
Settlement assets	(212,497)	(172,676)
Accounts receivable, net of reserve for merchant credit losses	(97,490)	(54,891)
Settlement liabilities	194,672	163,911
Accounts payable and accrued expenses	13,487	5,091
Payable to Wells Fargo Bank, N.A.	59,455	47,815
Payable to First Data Merchant Services Corporation	9,536	(8,847)
Other assets	(132)	—
Net cash provided by operating activities	494,582	461,241
Cash flows from investing activities:		
Contract acquisition costs	(296)	(339)
Net cash used in investing activities	(296)	(339)
Cash flows from financing activities:		
Distributions to members	(506,600)	(460,576)
Net cash used in financing activities	(506,600)	(460,576)
(Decrease)/Increase in cash and cash equivalents	(12,314)	326
Cash and cash equivalents at beginning of year	64,403	64,077
Cash and cash equivalents at end of year	$ 52,089	$ 64,403

See accompanying notes to financial statements.

WELLS FARGO MERCHANT SERVICES, LLC
(A Joint Venture)
Financial Statements
December 31, 2015 and 2014

(Dollars in thousands, unless otherwise noted)

(1) Business Description

Wells Fargo Merchant Services, LLC (the "Company") is a joint venture between First Data Merchant Services Corporation ("FDMS") and Wells Fargo Bank, N.A. ("Wells Fargo"). FDMS is a fully owned subsidiary of First Data Corporation. The Company was established pursuant to the terms of an alliance agreement (the "Membership Agreement") dated November 1, 1993, as amended and a Limited Liability Company Agreement dated September 1, 1997, as amended. The Membership Agreement will terminate on December 31, 2019. FDMS and Wells Fargo are here-in-after referred to, individually, as a "Member" or, collectively, as "Members".

The Company is engaged in processing and funds transfer related to the authorization, processing, and settlement of credit and debit card transactions for merchants. A majority of its revenue is based on the dollar amount of transactions processed. The Company provides services to merchant customers within all 50 states, with a significant concentration in California. The Company is operationally dependent on both FDMS and Wells Fargo. The Company's primary operations are conducted through FDMS. The Company's funding and settlement are primarily conducted through Wells Fargo. The majority of the bank accounts used for daily operations are with Wells Fargo.

(2) Summary of Significant Accounting Policies

(a) Use of Estimates

The preparation of consolidated financial statements in conformity with U.S. generally accepted accounting principles requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities and disclosures of contingent assets and liabilities at the date of the financial statements and the reported amounts of revenues and expenses during the reporting period. Actual results could differ from the estimates. Items subject to such estimates and assumptions include the reserve for merchant credit and fee losses.

(b) Settlement Assets and Liabilities

1) The Company has a fiduciary responsibility to its merchant customers as it relates to the transfer of funds from a cardholder's issuing bank, via the VISA, MasterCard, American Express or Discover card companies (the "Card Associations") and the Accel, AFFN, Alaska Option, Credit Union 24, Interlink, Jeanie, Maestro, NYCE, Pulse, NETS, Shazam, and Star Debit Networks (the "Debit Networks"). The Company records such amounts due from the issuing banks, Card Associations and Debit Networks within the balance sheet caption settlement assets while the related liability, settlement liabilities, represents amounts due to merchants. Pursuant to the Card Associations' and Debit Networks' rules, such fiduciary funds are not available to support the operations of the Company.

2) When a cardholder or a credit issuing institution disputes a transaction, within the Card Association guidelines, the Company's merchant customers have a liability for the disputed charges. However, in the case of merchant fraud, insolvency or bankruptcy, the Company may also be liable. Fee receivables that are ultimately deemed as uncollectable are charged-off against the merchant credit and fee loss reserve.

The Company's determination of the level of the reserve is calculated based on the level of sales volumes multiplied by loss factors taking into consideration charge-offs, recoveries and merchant collateral and rests upon various judgments and assumptions, including the review of historical data and a specific analysis of receivables due from merchants. Our charge-off policy is to fully charge down the balance when the receivable is 60 days past due. The Company requires cash deposits, guarantees, letters of credit or other types of collateral by certain merchants to minimize its credit risk. Included in the balance sheet's settlement assets is $109.2 million and $53.7 million in Merchant collateral, as of December 31, 2015 and 2014, respectively. Merchant collateral represents restricted cash held by the Company in a Wells Fargo bank account. The reserve for merchant credit losses is a valuation allowance for probable losses inherent as of the balance sheet date. The Company considers the reserve for merchant credit losses adequate to cover losses inherent in the portfolio as of December 31, 2015 and 2014.

(c) Cash and Cash Equivalents

The Company considers all highly liquid investments with a maturity of three months or less when purchased to be cash equivalents. At December 31, 2015 and 2014, the majority of the Company's cash and cash equivalents were held in Wells Fargo accounts and are FDIC insured.

(d) Intangibles

The Company capitalizes initial payments for new contracts, contract renewals and conversion costs associated with customer processing relationships to the extent recoverable through future operations, contractual minimums and/or penalties in the case of early termination. The Company's accounting policy is to limit the amount of capitalized costs for a given contract to the lesser of the estimated ongoing future cash flows from the contract or the termination fees the Company would receive in the event of early termination of the contract by the customer. The company amortizes intangibles over the period of the contract.

(e) Accounts Payable and Accrued Expenses

The Company accrues for certain expenses that have been received and that are billed one month in arrears. These estimates are classified within accounts payable and accrued expenses in the balance sheet.

(f) Income Taxes

No provision is made in the accounts of the Company for federal or state income taxes because all items of income and expense and other items affecting taxable income are allocated to the Members for inclusion in their income tax returns.

In accounting for income taxes, the Company follows the guidance in FASB ASC 740 (formerly FASB Interpretation No. 48), as amended by ASU 2009-06, *Accounting for Uncertainty in Income Taxes.* ASC 740 requires the Company to determine whether a tax position of the Company is more likely than not to be sustained upon examination by the applicable taxing authority, including resolution of any related appeals or ligation processes, based on the technical merits of the position. The tax benefit to be recognized is measured as the largest amount of benefit that is greater than fifty percent likely of being realized upon ultimate settlement which could result in the Company recording a tax liability that would reduce net assets. ASC 740 also provides guidance on thresholds, measurement, de-recognition, classification, interest and penalties, accounting in interim periods, disclosure, and transition that is intended to provide better financial statement comparability among different entities. As an LLC and pass-through entity, the Company does not incur tax expense and is not required to record a tax provision related to uncertain tax positions, in accordance with the recognition, measurement, classification, and disclosure requirements of ASC 740-10. The U.S. is the major tax jurisdiction for the Company. The tax returns of the Company can be examined by the relevant taxing authorities until the applicable statute of limitations has expired, which is generally three to four years from the date the return is initially filed, depending on the specific jurisdiction. Based on analysis by the Company, there were no material positions identified which did not meet the "more likely than not" standard as of and for the years ended December 31, 2015 and 2014.

(g) Members' Equity

An equity account is maintained for each Member. In certain instances, the Members may be required to make additional contributions to the Company. Such contributions will be determined on a pro-rata basis in accordance with each Member's Membership Interest at the time of the request and will be added to the Member's equity account. Membership Interest is defined as the ownership percentage of the Company by each member.

(h) Revenue Recognition

The Company recognizes card services revenues from its transaction processing and authorization services as such services are performed. The revenues from transaction processing and authorization services are included in card services revenue in the statement of revenue and expenses. The Company recognizes revenue when the price is fixed or determinable, persuasive evidence of an arrangement exists, the service is performed and collectability of the resulting receivable is reasonably assured. Certain revenues are recorded net of certain costs not controlled by the Company, including interchange and assessment fees charged by the Card Associations. Such costs totaled $4.3 billion and $3.5 billion for the years ended December 31, 2015 and 2014. The Company recognizes product revenue from merchant referred leases, rentals and sales as such services are performed. The Company records expense associated with the corresponding charge from affiliates of FDMS.

Debit revenues are recorded gross and are included within card services revenue in the statement of revenues and expenses. Debit Network fees are recorded within cost of card services in the statement of revenues and expenses. Debit revenues are recognized as such services are performed. Debit Network fees totaled $105.2 million and $101.6 million for the years ended December 31, 2015 and 2014.

In addition to the above, the Company recognizes other fees for services as such services are performed. The other revenue caption on the statement of revenues and expenses includes relevant items such as monthly fees, new account fees, income from cash advances, chargeback fees, supply fees and early termination fees.

(i) Comprehensive Income

For the year ended December 31, 2015 and 2014 net income equals comprehensive income.

(3) Intangibles

Following is a summary of the Company's intangibles for the years ended December 31, 2015 and 2014:

	Intangible Assets, Gross of Accumulated Amortization	Accumulated Amortization	Intangible Assets, Net of Accumulated Amortization
Beginning balance as of January 1, 2015	$ 2,309	$ (1,830)	$ 479
Additions	296	—	296
Retirements	(339)	339	—
Amortization	—	(318)	(318)
Ending balance as of December 31, 2015	$ 2,266	$ (1,809)	$ 457
Beginning balance as of January 1, 2014	$ 2,370	$ (1,933)	$ 437
Additions	340	—	340
Retirements	(401)	401	—
Amortization	—	(298)	(298)
Ending balance as of December 31, 2014	$ 2,309	$ (1,830)	$ 479

For the years ended December 31, 2015 and 2014, amortization expense of $318 and $298, respectively, is included in other expenses in the statement of revenues and expenses.

(4) Related Party Transactions

The Company's primary operations are conducted through FDMS. FDMS charges the Company fees for services provided pursuant to an operating agreement (the "Operating Agreement") dated January 31, 2000, as amended and restated. The Members also agreed to perform certain additional management functions (the "Additional Services") of the Company, for which they will be reimbursed by the Company. These fees are included in cost of card services, cost of product sold and selling, general and administrative expenses within the statement of revenue and expense. The financial statements may not necessarily be indicative of the financial position that would have existed, or the results of operations or cash flows that would have occurred had the Company operated as an independent enterprise. During the years ended December 31, 2015 and 2014, the Company reimbursed FDMS and Wells Fargo for performing the Additional Services as follows:

(Dollars in thousands, unless otherwise noted)

	2015	
	First Data Merchant Services, Corporation	Wells Fargo Bank, NA
Cost of card services	$ 76,686	$ —
Cost of product sold	21,464	—
Selling, general and administrative	14,324	130,873
Total	$ 112,474	$ 130,873

	2014	
	First Data Merchant Services, Corporation	Wells Fargo Bank, NA
Cost of card services	$ 66,980	$ —
Cost of product sold	16,141	—
Selling, general and administrative	12,206	120,314
Total	$ 95,327	$ 120,314

Included in the balance sheets at December 31, 2015 and 2014 is a payable to FDMS of $23,200 and $13,644, respectively. These balances primarily consist of selling, general and administrative costs, cost of card services and cost of product sold owed to FDMS which are partially offset by net revenue owed to WFMS for the contributed portfolio. These balances are settled monthly, one month in arrears.

Included in the balance sheets at December 31, 2015 and 2014 is a payable to Wells Fargo of $340,437 and $280,982, respectively, which is primarily attributable to non-interest bearing advances, made by Wells Fargo to the Company. These payable amounts are settled monthly, one month in arrears.

(5) Allocation and Distribution of Income to Members

Profits and losses of the Company are allocated in accordance with each Member's Interest. Distributions of allocated income to the Members are made on a quarterly basis, subject to consent of the Members. Income distributed shall equal 100% of the distributable funds, as defined in the Membership Agreement, unless a smaller percentage is agreed to by the Members.

(6) Termination of Company

The Company can be terminated in the event of certain termination events, set forth in the Membership Agreement with an effective date of January 1, 2014. These include merger or acquisition of either of the Members, and various other performance criteria. If the Company is terminated prior to December 31, 2019, based on who initiates the termination, an early termination fee may apply in accordance with the provisions and criteria of the agreement.

(7) Limited Liability of Members

The Members of a Delaware limited liability company are generally not liable for the acts and omissions of the Company, much in the same manner as the shareholders, officers and directors of a corporation are generally not liable for the acts and omissions of the corporation. Such liability is generally limited by the provisions of the Delaware Limited Liability Company Act and by applicable case law.

(8) Fair Value of Financial Instruments

FASB ASC 825, *Financial Instruments*, requires the disclosure of the fair value of financial instruments, including assets and liabilities recognized in the balance sheets. Management estimates that the aggregate fair value of financial instruments recognized in the balance sheets (including receivables, payables and merchant collateral) approximates their carrying value; as such financial instruments are short-term in nature or carry floating rates of interest.

(9) Guarantees and Reserve for Merchant Credit Losses

Under the card companies' rules, when a merchant processor acquires card transactions, it has certain liabilities for the transactions. This liability arises from disputes between cardholders and merchants due to the cardholders' dissatisfaction with merchandise quality or the merchants' service, which are not resolved with the merchant. In such cases, the transactions are "charged back" to the respective merchants and the related purchase amounts are refunded to the cardholders by the card issuer. If the merchant does not fund the refund due to insolvency, bankruptcy or other extraneous reasons, the Company, in certain circumstances is liable for the full amount of the transaction. This liability is considered a guarantee under FASB ASC 460, *Guarantees*.

The Company's legal obligation under these rules is to settle any individual chargeback for which an individual merchant fails to fulfill as noted above. Contractually, the maximum exposure for this obligation is the total amount of transactions processed for the preceding four months period, or from the date of delivery of the goods and services by the merchant, if longer than four months for all merchants, which in the case of the Company is in the billions of dollars. It should be noted that the Company has not experienced material chargeback loss activity as a result of merchant processing activities and advises that caution should be used when assessing the maximum exposure described above. The Company records a provision for this estimated obligation based upon a number of factors which include historical losses, credit risk of specific customers and other relevant factors. As shown below, for the years ended December 2015 and 2014, the Company incurred aggregate merchant credit losses of $12,430 and $9,229, net of recoveries, on total processed volumes. The Company calculates its provision and evaluates the appropriateness of its reserves on a monthly basis.

(Dollars in thousands, unless otherwise noted)

The following is the activity related to the reserve for merchant credit losses for the years ended December 31, 2015 and 2014:

Beginning balance as of January 1, 2015	$	4,507
Provisions for credit loss		13,108
Charge-offs, net of recoveries of $696		(12,430)
Ending balance as of December 31, 2015	$	5,185
Beginning balance as of January 1, 2014	$	3,361
Provisions for credit loss		10,375
Charge-offs, net of recoveries of $387		(9,229)
Ending balance as of December 31, 2014	$	4,507

(10) Subsequent Events

The Company has evaluated the subsequent events from the balance sheet date through February 19, 2016, the date at which the financial statements were available to be issued, and determined that there are no other items to disclose.

Pursuant to the requirements of Section 13 or 15(d) of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized.

FIRST DATA CORPORATION
(Registrant)

By: /S/ FRANK BISIGNANO
Frank Bisignano
Chief Executive Officer

Date: February 25, 2016

Pursuant to the requirements of the Securities Exchange Act of 1934, this report has been signed below by the following persons on behalf of the registrant and in the capacities and on the dates indicated:

Name	Title	Date
/S/ FRANK BISIGNANO **Frank Bisignano**	Chief Executive Officer and Director (principal executive officer)	February 25, 2016
/S/ HIMANSHU A. PATEL **Himanshu A. Patel**	Executive Vice President, Chief Financial Officer (principal financial officer)	February 25, 2016
/S/ MATTHEW CAGWIN **Matthew Cagwin**	Senior Vice President, Corporate Controller and Chief Accounting Officer (principal accounting officer)	February 25, 2016
/S/ JOE W. FOREHAND **Joe W. Forehand**	Director	February 25, 2016
/S/ HENRY R. KRAVIS **Henry R. Kravis**	Director	February 25, 2016
/S/ HEIDI G. MILLER **Heidi G. Miller**	Director	February 25, 2016
/S/ JAMES E. NEVELS **James E. Nevels**	Director	February 25, 2016
/S/ SCOTT C. NUTTALL **Scott C. Nuttall**	Director	February 25, 2016
/S/ TAGAR C. OLSON **Tagar C. Olson**	Director	February 25, 2016
/S/ JOSEPH J. PLUMERI **Joseph J. Plumeri**	Director	February 25, 2016

Exhibit 10.16

OPTION AGREEMENT

FIRST DATA CORPORATION

2015 OMNIBUS INCENTIVE PLAN

Subject to the terms of the First Data Corporation 2015 Omnibus Incentive Plan (Plan), First Data Corporation (First Data) and the Participant (you) agree as follows:

1. **Definitions**. Whenever the following terms are used in this Option Agreement (Agreement), they have the meanings below. Capitalized terms that are not defined in this Agreement have the meanings defined in the Plan.

1.1 **Exercise Price**. The term Exercise Price means the exercise price on your Grant Notice.

1.2 **Grant Date**. The term Grant Date means the date on your Grant Notice.

1.3 **Option Period**. The term "Option Period" means the period beginning on the Grant Date and ending on the 10th anniversary of the Grant Date.

1.4 **Grant Notice**. The term "Grant Notice" means the document attached as Exhibit A to this Agreement.

2. **Grant of Options**. First Data grants to you the right and option to purchase all or any part of the aggregate number of shares of Common Stock subject to the options on your Grant Notice (the Options, with each Option representing the right to purchase one share of Common Stock), at an Exercise Price per share on your Grant Notice.

3. **Vesting**. The Options will vest as follows:

3.1 **Continuous Employment**. As long as you have not experienced a Termination before each applicable vesting date, one-third of the Options will vest and become exercisable on the first anniversary of the Grant Date, one-third of the Options will vest and become exercisable on the second anniversary of the Grant Date and the remaining one-third of the Options will vest and become exercisable on the third anniversary of the Grant Date (each anniversary, a Vesting Date). Upon vesting, the Options will be rounded down to the nearest whole Option.

3.2 **Termination**. In the event of your Termination before the last Vesting Date, you will forfeit any unvested Options for no consideration.

4. **Exercise of Options after Termination**. The terms of Section 7(c)(2) of the Plan are incorporated into this Agreement by this reference and made a part of this Agreement.

5. **Method of Exercising Options**. You may exercise all or any portion of the vested Options by delivering notice of the number of shares that are being exercised together with full payment of the Exercise Price for the portion of the Options being exercised. The notice must be in writing to either First Data or a third-party administrator engaged by First Data. Payment of the Exercise Price may be made using the methods described in Section 7(d)(1) or Section 7(d)(2)(C) of the Plan.

6. **Issuance of Shares**. Following the exercise of all or any portion of the Options, as promptly as practical after receipt of full payment of the Exercise Price and any required taxes, First Data will issue or transfer to you the number of shares of Common Stock for which the Option has been exercised, and either (1) deliver to you a certificate or certificates for the shares registered in your name, (2) cause the shares to be registered in book-entry form on First Data's stock register, or (3) cause the shares to be credited to your account at a third-party administrator.

7. **Non-Transferability**. You may not transfer the Options except as permitted under Section 14(b) of the Plan.

8. **Confidential Information; Non-Compete; Non-Solicit; Clawback/Forfeiture.**

8.1 In consideration of First Data granting you the Options, you agree that you will not directly or indirectly:

8.1.1 at any time during or after your Termination, use, disclose or disseminate any Confidential Information or Trade Secrets about the business of First Data or any Affiliate. These obligations do not apply to any Confidential Information or Trade Secret that has become generally known to competitors of First Data or any Affiliate through no act or omission of yours. Nothing in this Agreement prohibits or impedes you from communicating, cooperating or filing a complaint with any U.S. federal, state or local governmental or law enforcement branch, agency or entity (collectively, a Governmental Entity) concerning possible violations of any U.S. federal, state or local law or regulation, or otherwise making disclosures to any Governmental Entity, in each case, that are protected under the whistleblower provisions of any such law or regulation, as long as in each case the communications and disclosures are consistent with applicable law. You are not authorized to disclose any information covered by First Data's or any Affiliate's attorney-client privilege or attorney work product or Trade Secrets without the written consent of the Board or its designee;

8.1.2 at any time during your service with First Data or any Affiliate and for a period of two years following Termination, act as a proprietor, investor, director, officer, employee, stockholder, consultant or partner in any business that directly or indirectly competes, at the relevant determination date, with First Data's business or any Affiliate's business in any geographic area where First Data or any Affiliate manufactures, produces, sells, leases, rents, licenses or otherwise provides products or services. This section does not restrict you from investing in publicly-available mutual funds or exchange-traded funds; and

8.1.3 at any time during your service with First Data or any Affiliate and for a period of two years following Termination, (A) solicit customers or clients of First Data or any Affiliate to terminate their relationship with First Data or any Affiliate or solicit those customers or clients to compete with any business of First Data or any Affiliate or (B) solicit or offer employment to any person who is, or has been at any time during the 12 months before the Termination, employed by First Data or any Affiliate.

8.2 If you are bound by any other agreement with First Data or any Affiliate regarding the use, dissemination or disclosure of Confidential Information or Trade Secrets, the terms of this Agreement will be read in such a way as to further restrict and not to permit any more extensive use, dissemination or disclosure of Confidential Information or Trade Secrets.

8.3 If a court holds that the restrictions stated in Section 8 are unreasonable or otherwise unenforceable, the maximum period, scope or geographic area determined to be reasonable by the court will be substituted for the stated period, scope or area. Because your services are unique and because you have had access to Confidential Information and/or Trade Secrets, money damages will be an inadequate remedy for any breach of this Agreement. In the event of a breach or threatened breach of this Agreement, First Data may, in addition to other rights and remedies existing in its favor, apply to any court of competent jurisdiction for specific performance and/or injunctive relief in order to enforce or prevent any violations of this Agreement.

8.4 If you have engaged in or engage in any Detrimental Activity, then the Committee may take any action permitted under the Plan, including: (1) canceling the Options; or (2) requiring that you forfeit any gain realized on the exercise of the Options or the sale of any shares received upon exercise of the Options and repay that gain to First Data. In addition, if you receive any amount greater than what you should have received under the terms of this Agreement for any reason, then you must repay any excess amount to First Data. The Options will be subject to reduction, cancellation, forfeiture or recoupment to the extent necessary to comply with applicable law.

9. **No Rights as Stockholder**. Neither you nor any Permitted Transferee of the Options will have any rights as a stockholder with respect to any share of Common Stock underlying an Option until you have become the holder of record or the beneficial owner of the share. Further, no adjustment will be made for dividends or distributions or other rights for any share of Common Stock for which the record date is before the date that you become the holder of record or the beneficial owner of the share.

10. **Tax Withholding**. This Award will be subject to all applicable taxes as provided in Section 14(d) of the Plan.

11. **Notice**. Every notice or other communication relating to this Agreement between First Data and you must be in writing. All notices and communications between you and any third-party plan administrator must be mailed, delivered, transmitted or sent according to that third-party plan administrator's procedures.

12. **Binding Effect**. This Agreement will be binding upon and inure to the benefit of the heirs, executors, administrators and successors of the parties to this Agreement.

13. **Waiver and Amendments**. The Committee may waive any conditions or rights under, amend any terms of, or alter, suspend, discontinue, cancel or terminate, this Agreement, prospectively or retroactively, except that your consent will be required for any waiver, amendment, alteration, suspension, discontinuance, cancellation or termination that would materially and adversely affect your rights. No waiver by either of the parties to this Agreement of their rights will constitute a waiver of any subsequent occurrences or transactions unless the waiver specifically states that it is to be construed as a continuing waiver. The Committee's rights under this Section 13 may be subject to stockholder approval as required under Section 13(b) of the Plan.

14. **Governing Law; Forum**. This Agreement will be construed and interpreted under the State of Delaware, without regard to the principles of conflicts of law. If any controversy among the parties arises out of, or relates to, this Agreement, you and First Data agree and consent to the exclusive jurisdiction and venue of the state and federal courts of New Castle County in the State of Delaware.

15. **Plan**. The terms of the Plan are incorporated into this Agreement and made a part of this Agreement. In the event of a conflict or inconsistency between the terms of the Plan and this Agreement, the Plan will control. You acknowledge that a copy of the Plan (which is publicly-filed) has been made available to you, as well as a prospectus describing the terms of the Plan.

16. **Imposition of Other Requirements**. First Data may impose any other requirements on your participation in the Plan, on the Options granted under this Agreement and on any shares acquired under the Plan, if First Data determines it is necessary or advisable for legal or administrative reasons. First Data may also require you to sign any additional agreements that may be necessary to accomplish the foregoing.

17. **Entire Agreement**. The information on your Grant Notice, this Agreement and the Plan constitute the entire understanding between you and First Data regarding the Options granted under this Agreement.

EXHIBIT A - GRANT NOTICE
FOR OPTION AGREEMENT

Name: **[Name] (you)**
ID: **[Employment ID]**
Grant Date: [Date]
Number of Options: [Amount]
Exercise Price: [Price]

Acknowledgement and Acceptance

By signing below, you acknowledge that the Award reflected in this Grant Notice is governed by the Plan and the Option Agreement terms and conditions, which you have received with this notice. You also accept the grant of the above award under its terms and conditions.

ACCEPTED BY:

_____
Signature

_____
Date

Exhibit 10.17

RESTRICTED STOCK AWARD AGREEMENT

FIRST DATA CORPORATION

2015 OMNIBUS INCENTIVE PLAN

Subject to the terms of the First Data Corporation 2015 Omnibus Incentive Plan (Plan), First Data Corporation (First Data) and the Participant (you) agree as follows:

1. **Definitions**. The term "Grant Date" means the date on specified in the grant notice attached as Exhibit A (Grant Notice). Other capitalized terms that are not defined in this Agreement have the meanings defined in the Plan.

2. **Grant of Restricted Shares**. First Data grants to you the number of shares of Restricted Stock included on your Grant Notice (Restricted Shares).

3. **Vesting**. The Restricted Period for the Restricted Shares will lapse and the Restricted Shares will vest as follows:

3.1 **Continuous Employment**. As long as you have not experienced a Termination before each applicable vesting date, 20% of the Restricted Shares will vest on the first anniversary of the Grant Date, 40% of the Restricted Shares will vest on the second anniversary of the Grant Date, and the remaining 40% of the Restricted Shares will vest on the third anniversary of the Grant Date (each anniversary, a Vesting Date). Upon vesting, the Restricted Shares will be rounded down to the nearest whole share of Common Stock.

3.2 **Termination**. In the event of your Termination before the last Vesting Date, you will forfeit any unvested Restricted Shares for no consideration.

4. **Non-Transferability**. You may not transfer the Restricted Shares except as permitted under Section 14(b) of the Plan.

5. **Confidential Information; Non-Compete; Non-Solicit; Clawback/Forfeiture**.

5.1 In consideration of First Data granting you the Restricted Shares, you agree that you will not directly or indirectly:

5.1.1 at any time use, disclose, or disseminate any Confidential Information or Trade Secrets about the business of First Data or any Affiliate. These obligations do not apply to Confidential Information or Trade Secrets that have become generally known to competitors of First Data or any Affiliate through no act or omission of yours. Nothing in this Agreement prohibits or impedes you from communicating, cooperating, or filing a complaint with any U.S. federal, state, or local governmental or law enforcement branch, agency, or entity (collectively, a Governmental Entity) concerning possible violations of any U.S. federal, state, or local law or regulation, or otherwise making disclosures to any Governmental Entity, in each case, that are protected under the whistleblower provisions of any such law or regulation, as long as in each case the communications and disclosures are consistent with applicable law. You are not authorized to disclose any information covered by First Data's or its Affiliates' attorney-client privilege or attorney work product or Trade Secrets without the written consent of the Board or its designee;

5.1.2 at any time during your service with First Data or any Affiliate and for a period of two years following Termination, act as a proprietor, investor, director, officer, employee, stockholder, consultant, or partner in any business that directly or indirectly competes, at the relevant determination date, with First Data's business or any Affiliate's business in any geographic area where First Data or any Affiliate manufactures, produces, sells, leases, rents, licenses, or otherwise provides products or services, except that this section does not restrict you from investing in publicly-available mutual funds or exchange-traded funds; or

5.1.3 at any time during your service with First Data or any Affiliate and for a period of two years following Termination, (1) solicit customers or clients of First Data or any Affiliate to terminate their relationship with First Data or any Affiliate or solicit those customers or clients to compete with any business of First Data or any Affiliate or (2)

solicit or offer employment to any person who is, or has been at any time during the 12 months before your Termination, employed by First Data or any Affiliate.

5.2 If you are bound by any other agreement with First Data or any Affiliate covering the use, dissemination, or disclosure of Confidential Information or Trade Secrets, the terms of this Agreement will be read in a way to further restrict and not to permit any more extensive use, dissemination, or disclosure of Confidential Information or Trade Secrets.

5.3 If a court holds that the restrictions stated in this Section 5 are unreasonable or otherwise unenforceable, the maximum period, scope, or geographic area determined to be reasonable by the court will be substituted for the stated period, scope, or area. Because your services are unique and because you have had access to Confidential Information and/or Trade Secrets, money damages will be an inadequate remedy for any breach of this Agreement. In the event of a breach or threatened breach of this Agreement, First Data may, in addition to other rights and remedies existing in its favor, apply to any court of competent jurisdiction for specific performance and/or injunctive relief in order to enforce or prevent any violations of this Agreement.

5.4 If you have engaged in or engage in any Detrimental Activity, then the Committee may take any action permitted under the Plan, including: (1) canceling the Restricted Shares; or (2) requiring you to forfeit any gain realized on the vesting and/or sale of the Restricted Shares and repay that gain to First Data. In addition, if you receive any amount greater than what you should have received under this Agreement, then you must repay any excess amount to First Data. The Restricted Shares will be subject to reduction, cancellation, forfeiture, or recoupment to the extent necessary to comply with applicable law.

6. **Stockholder Rights**. Subject to the restrictions set forth in Section 9 of the Plan, you generally will have the rights and privileges of a First Data stockholder as to the Restricted Shares on the Grant Date, including the right to vote the Restricted Shares. However, any dividends payable on the Restricted Shares will be held by First Data and delivered to you (without interest) within 15 days after the applicable Restricted Shares vest. You will forfeit the right to any accumulated dividends if you forfeit the Restricted Shares to which the dividends relate. To the extent you forfeit the Restricted Shares, any stock certificates issued to you evidencing the shares must be returned to First Data, and all of your rights to those shares and as a stockholder with respect to those shares will terminate without further obligation on First Data's part.

7. **Tax Withholding**. This Award will be subject to all applicable taxes as provided in Section 14(d) of the Plan.

8. **Notice**. Every notice or other communication relating to this Agreement between First Data and you must be in writing. All notices and communications between you and any third-party Plan administrator must be mailed, delivered, transmitted, or sent according to that administrator's procedures.

9. **Binding Effect**. This Agreement will be binding upon and inure to the benefit of the heirs, executors, administrators, and successors of the parties to this Agreement.

10. **Waiver and Amendments**. The Committee may waive any conditions or rights under, amend any terms of, or alter, suspend, discontinue, cancel, or terminate this Agreement, prospectively or retroactively, except that your consent will be required for any waiver, amendment, alteration, suspension, discontinuance, cancellation, or termination that would materially and adversely affect your rights. No waiver by either of the parties to this Agreement of their rights will constitute a waiver of any subsequent occurrences or transactions unless the waiver specifically states that it is to be construed as a continuing waiver. The Committee's authority under this Section 11 may be subject to stockholder approval as required under Section 13(b) of the Plan.

11. **Governing Law; Forum**. This Agreement will be construed and interpreted under the laws of the State of Delaware, without regard to the principles of conflicts of law. If any controversy among the parties arises out of, or relates to, this Agreement, you and First Data agree and consent to the exclusive jurisdiction and venue of the state and federal courts of New Castle County in the State of Delaware.

12. **Plan**. The terms of the Plan are incorporated into this Agreement. In the event of a conflict or inconsistency between the terms of the Plan and this Agreement, the Plan will control. You acknowledge that a copy of the Plan (which is publicly-filed) has been made available to you, as well as a prospectus describing the terms of the Plan.

13. **Imposition of Other Requirements**. First Data may impose any other requirements on your participation in the Plan, on the Restricted Shares, and on any shares acquired under the Plan if First Data determines it is necessary or

advisable for legal or administrative reasons. First Data may also require you to sign any additional agreements that may be necessary to accomplish the foregoing.

14. **Entire Agreement**. The information on your Grant Notice, this Agreement, and the Plan constitute the entire understanding between you and First Data regarding the Restricted Shares.

EXHIBIT A - GRANT NOTICE
FOR RESTRICTED STOCK AWARD AGREEMENT

Name: **[Name] (you)**
ID: **[Employment ID]**
Grant Date: [Date]
Number of Shares of Restricted Stock: [Amount]

Acknowledgement and Acceptance

By signing below, you acknowledge that the Award reflected in this Grant Notice is governed by the Plan and the Restricted Stock Award Agreement terms and conditions, which you have received with this notice. You also accept the grant of the above award under its terms and conditions.

ACCEPTED BY:

_____
Signature

_____
Date

Exhibit 10.20

Description of Compensation of Directors

Each Director not employed by First Data or affiliates of Kohlberg Kravis Roberts & Co. (KKR) receives the following:

- At the time of their appointment, a one-time grant of 158,182 options to purchase shares of Class A common stock of First Data pursuant to the First Data Corporation 2015 Omnibus Incentive Plan (2015 Plan) with a strike price equal to the Fair Market Value at the time of grant to vest in equal annual installments on the first three anniversaries of the grant date.

- Annual grant of restricted stock of First Data equivalent in value to $125,000, both at the time of their appointment and during the first quarter of each subsequent calendar year during which they continue to serve pursuant to the 2015 Plan and on the following terms:

    - 20% vesting one year from the grant date;
    - 40% vesting two years from the grant date;
    - 40% vesting three years from the grant date;
    - Forfeiture of unvested awards upon termination of Board service for any reason other than Death or Disability; and
    - In the event of Death or Disability, First Data shall exercise call rights and pay 100% of the fair market value for unvested awards.

- Annual cash retainer of $75,000 to be paid in quarterly installments on the first day of each calendar quarter.

Each non-employee Director associated with KKR receives an annual cash retainer of $40,000, payable in semi-annual installments.

All cash compensation may be deferred under the First Data 2008 Non-Employee Director Deferred Compensation Plan based upon the election made prior to each calendar year by each director. All amounts deferred will accrue earnings based on the performance of Class A common stock and are paid to the director upon termination of the director's service, subject to acceleration of the payout under certain circumstances.

Exhibit 21

LIST OF FIRST DATA CORPORATION SUBSIDIARIES

Name of Subsidiary	Jurisdiction of Incorporation
Administradora de Tarjetas S.R.L.	Argentina
BA Merchant Services, LLC	Ohio
Banc of America Merchant Services, LLC	Delaware
Bank of America Merchant Services Canada Corp.	Canada
Bankcard Investigative Group Inc.	Delaware
BOFA Merrill Lynch Merchant Services (Europe) Limited	United Kingdom
BUYPASS Inco Corporation	Delaware
BWA Merchant Services Pty Ltd	Australia
Call Interactive Holdings LLC	Delaware
Cash Axcess Corporation (Proprietary) Limited	South Africa
Cashcard Australia Limited	Australia
CESI Holdings, LLC	Delaware
Clover MarketPlace, LLC	Delaware
Clover Network, Inc.	Delaware
Concord Computing Corporation	Delaware
Concord Corporate Services, Inc.	Delaware
Concord EFS Financial Services, Inc.	Delaware
Concord EFS, Inc.	Delaware
Concord Emerging Technologies, Inc.	Arizona
Concord Financial Technologies, Inc.	Delaware
Concord One, LLC	Delaware
Concord Payment Services, Inc.	Georgia
Concord Processing, Inc.	Delaware
Concord Transaction Services, LLC	Colorado
CTS Holdings, LLC	Colorado
CTS, Inc.	Tennessee
D.Man Debtors Notification Company S.A.	Greece
DW Holdings Canada ULC	Canada
Eastern States Bankcard Association Inc.	New York not-for-profit
Eastern States Monetary Services Inc.	New York not-for-profit
Electronic Banking Solutions Limited	Australia
EPSF Corporation	Delaware
European Merchant Services B.V.	Netherlands
FD do Brasil Soluções de Pagamento Ltda.	Brazil
FDFS Holdings, LLC	Delaware
FDGS Group, LLC	Delaware
FDGS Partner, LLC	Delaware
FDR (First Data Resources) Europe B.V.	Netherlands
FDR Ireland Limited	Delaware
FDR Limited	Delaware
FDR Missouri Inc.	Delaware
FDR U.K. Limited	United Kingdom
FDS Holdings, Inc.	Delaware
Federated Union Systems, Limited	Ireland
Federated Union Systems Europe, Ltd.	Ireland

First Data Asia Pte Ltd.	Singapore
First Data Austria GmbH	Austria
First Data Austria Holdings GmbH	Austria
First Data Canada Ltd.	Canada
First Data Capital, Inc.	Delaware
First Data Card Solutions, Inc.	Maryland
First Data (China) Co., Ltd.	China
First Data Chile Limitada	Chile
First Data CIS	Russia
First Data Colombia Ltda.	Colombia
First Data Commercial Services Limited	Ireland
First Data Communications Corporation	Delaware
First Data Cono Sur SRL	Argentina
First Data Corporation Australia (Holdings) Pty Limited	Australia
First Data Czech Republic	Czech Republic
First Data Deutschland GmbH	Germany
First Data Development Pvt Ltd	India
First Data EC, LLC	Delaware
First Data EESTI OU	Estonia
First Data Europe Limited	United Kingdom
First Data Egypt LLC	Egypt
First Data Government Solutions, Inc.	Delaware
First Data Government Solutions, LP	Delaware
First Data Global Services Limited	Ireland
First Data GmbH	Germany
First Data (Greece) US Holding Corp.	Delaware
First Data Hellas Processing Services and Holdings SA	Greece
First Data Holding I (Netherlands) BV	Netherlands
First Data Hong Kong Limited	Hong Kong
First Data Magyarorszag Kereskedelmi es Szolgaltato Kft	Hungary
First Data (India) Private Limited	India
First Data International d.o.o.	Croatia
First Data International LLC	Delaware
First Data International (Italia) Srl	Italy
First Data International Luxembourg II SARL	Luxembourg
First Data International Luxembourg III SARL	Luxembourg
First Data International Luxembourg IV SARL	Luxembourg
First Data International Luxembourg VI SARL	Luxembourg
First Data International Luxembourg VII SARL	Luxembourg
First Data Korea Limited	Korea
First Data Latin America Inc.	Delaware
First Data Latvia	Latvia
First Data Lietuva	Lithuania
First Data (Mauritius) Holding Company	Mauritius
First Data Merchant Services LLC	Florida
First Data Merchant Services México, S. de R.L. de C.V.	Mexico
First Data Merchant Services Northeast, LLC	Delaware
First Data Merchant Services Southeast, L.L.C.	Delaware
First Data Merchant Solutions (B) Sdn Bhd	Brunei
First Data Merchant Solutions (Hellas) Ltd	Greece

First Data Merchant Solutions (Hong Kong) Private Limited	Hong Kong
First Data Merchant Solutions (Malaysia) Sdn. Bhd.	Malaysia
First Data Merchant Solutions Private Limited (Singapore)	Singapore
First Data Middle East FZ-LLC	UAE
First Data Mobile Holdings, Inc.	Delaware
First Data Mobile (Bermuda) Holdings, Ltd.	Bermuda
First Data Mobile Holdings Limited	Ireland
First Data Mobile Payments Limited	Ireland
First Data Mobile Solutions GmbH	Germany
First Data Mobile Solutions Limited	Ireland
First Data (Norway) Holding AS	Norway
First Data Operations (Austria) GmbH	Austria
First Data Payment Services, LLC	Delaware
First Data Polska S.A.	Poland
First Data Procurements México, S. de R.L. de C.V.	Mexico
First Data Puerto Rico, LLC	Puerto Rico
First Data Real Estate Holdings L.L.C.	Delaware
First Data Receivables, LLC	Delaware
First Data Reporting Services LLC	Delaware
First Data Resources Australia Limited	Australia
First Data Resources Investments Pty Limited	Australia
First Data Resources, LLC	Delaware
First Data Resources South Africa (Proprietary) Limited	South Africa
First Data Retail ATM Services L.P.	Texas
First Data Romania SRL	Romania
First Data Serbia and Montenegro d.o.o.	Serbia
First Data Services LLC	Delaware
First Data (Singapore) Pte. Ltd.	Singapore
First Data Slovakia, s.r.o.	Slovakia
First Data Solutions Inc.	Washington
First Data Spain Holdings, S.L.	Spain
First Data Technologies, Inc.	Delaware
First Data Transportation Services Inc.	Tennessee
First Data Trust Company, LLC	Colorado
First Data Uruguay SA	Uruguay
First Data Voice Services	Delaware general partnership
First Merchant Processing (Ireland) Limited	Ireland
FSM Services Inc.	Delaware
FTS (NSW) Pty. Limited	Australia
Funds & Assets Management LLC	New York
FundsXpress, Inc.	Delaware
FundsXpress Financial Network, Inc.	Texas
GoEasy LLC	Delaware
GYFT, Inc.	Delaware
Gyft Mobile, Inc.	Delaware
Huntington Merchant Services, L.L.C.	Delaware
ICICI Merchant Services Private Limited	India
Ignite Payments, LLC	California
Instant Cash Services, LLC	Delaware

Integrated Payment Systems Canada Inc.	Canada
Integrated Payment Systems Inc.	Delaware
Inverland Jasper SL	Spain
IRS Intelligent Risk Management Solutions GmbH	Germany
Linkpoint International, Inc.	Nevada
Marketplace Merchant Solutions Limited	Ireland
MAS Inco Corporation	Delaware
MAS Ohio Corporation	Delaware
Merchant Solutions Private Limited	Bangladesh
Merchant Solutions Private Limited	Sri Lanka
Merchant Solutions Pte (Macau) Limited	Macau
Money Network Financial, LLC	Delaware
National Payment Systems Inc.	New York
New Payment Services, Inc.	Georgia
Omnipay Limited	Ireland
PayPoint Electronic Payment Systems, LLC	Delaware
PaySys de Costa Rica, S.A.	Costa Rica
PaySys Europe, B.V.	Netherlands
PaySys International, Inc.	Florida
PaySys International Limited	Ireland
PaySys International Pty. Ltd.	Australia
Pegaso Argentina S.R.L.	Argentina
Perka, Inc.	Delaware
Perka Limited	Ireland
Posnet SRL	Argentina
Processing Center, S.A.	Panama
Publicdatasystems, Inc.	Delaware
REMITCO LLC	Delaware
Research Park Association, Inc.	Florida not-for-profit
Sagebrush Holdings LLC	Delaware
Scotia Cardpoint Merchant Services	Puerto Rico
Size Technologies, Inc.	California
Spree Commerce Inc.	Delaware
Star Networks, Inc.	Delaware
Star Processing, Inc.	Delaware
Star Systems Assets, Inc.	Delaware
Star Systems, Inc.	Delaware
Star Systems, LLC	Delaware
Strategic Investment Alternatives LLC	Delaware
SunTrust Merchant Services, LLC	Delaware
TASQ LLC	Delaware
TASQ Technology, Inc.	California
TeleCash GmbH & Co. KG	Germany
TeleCash Management GmbH	Germany
TeleCheck International, Inc.	Georgia
TeleCheck Payment Systems Limited	New Zealand
TeleCheck Services Canada, Inc.	Canada
TeleCheck Services, Inc.	Delaware
TeleCheck Services of Puerto Rico, Inc.	Georgia
Tissington Limited	Ireland

Transaction Solutions, LLC	Delaware
Transaction Wireless, Inc.	Delaware
TRS Recovery Services, Inc.	Colorado
TWI MOR Holding, LLC	Delaware
Unified Merchant Services	Georgia General Partnership
ValueLink, LLC	Delaware
Zolter Services Limited	Ireland

Exhibit 23.1

Consent of Independent Registered Public Accounting Firm

We consent to the incorporation by reference in the Registration Statement (Form S-8 No. 333-207439) pertaining to the 2007 Stock Incentive Plan for Employees of First Data Corporation and its Affiliates, the First Data Corporation 2015 Omnibus Incentive Plan and the First Data Corporation 2015 Employee Stock Purchase Plan of our reports dated February 25, 2016, with respect to the consolidated financial statements and schedule of First Data Corporation, and the effectiveness of internal control over financial reporting of First Data Corporation, included in this Annual Report (Form 10-K) for the year ended December 31, 2015.

/s/ Ernst & Young LLP

Atlanta, Georgia
February 25, 2016

Exhibit 23.2

KPMG LLP
Suite 1400
55 Second Street
San Francisco, CA 94105

Consent of Independent Registered Public Accounting Firm

The Members
Wells Fargo Bank, N.A.
First Data Merchant Services Corporation; and

The Board of Directors
Wells Fargo Merchant Services, LLC:

We consent to the incorporation by reference in the following registration statements:

(1) Form S-1 No. 333-205750 of First Data Corporation; and

(2) Form S-8 No. 333-207439 of First Data Corporation

of our report dated February 19, 2016, with respect to the balance sheets of Wells Fargo Merchant Services, LLC as of December 31, 2015 and 2014, and the related statements of revenues and expenses, members' equity, and cash flows for each of the years in the two-year period ended December 31, 2015, included in the Form 10-K of First Data Corporation dated February 25, 2016.

KPMG LLP

San Francisco, California
February 25, 2016

Exhibit 31.1

CERTIFICATION OF CHIEF EXECUTIVE OFFICER

I, Frank Bisignano, Chief Executive Officer of First Data Corporation, certify that:

1. I have reviewed this Annual Report on Form 10-K of First Data Corporation;

2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4. The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

   (a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

   (b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

   (c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

   (d) Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

5. The registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

   (a) All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

   (b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: February 25, 2016

/s/ FRANK BISIGNANO

Frank Bisignano
Chief Executive Officer

Exhibit 31.2

CERTIFICATION OF CHIEF FINANCIAL OFFICER

I, Himanshu Patel, Executive Vice President, Chief Financial Officer (principal financial officer) of First Data Corporation, certify that:

1. I have reviewed this Annual Report on Form 10-K of First Data Corporation;

2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4. The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

   (a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

   (b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

   (c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

   (d) Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

5. The registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

   (a) All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

   (b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: February 25, 2016

/s/ HIMANSHU A. PATEL

Himanshu A. Patel
Executive Vice President, Chief Financial Officer
(principal financial officer)

Exhibit 32.1

CERTIFICATION OF CHIEF EXECUTIVE OFFICER

The certification set forth below is being submitted in connection with the Annual Report of First Data Corporation on Form 10-K for the period ended December 31, 2015 (the "Report") for the purpose of complying with Rule 13a-14(b) or Rule 15d-14(b) of the Securities Exchange Act of 1934 (the "Exchange Act") and Section 1350 of Chapter 63 of Title 18 of the United States Code.

Frank Bisignano, the Chief Executive Officer of First Data Corporation, certifies that, to the best of his knowledge:

1. The Report fully complies with the requirements of Section 13(a) or 15(d) of the Exchange Act; and

2. The information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of First Data Corporation.

Date: February 25, 2016

/s/ FRANK BISIGNANO

Frank Bisignano
Chief Executive Officer

Exhibit 32.2

CERTIFICATION OF CHIEF FINANCIAL OFFICER

The certification set forth below is being submitted in connection with the Annual Report of First Data Corporation on Form 10-K for the period ended December 31, 2015 (the "Report") for the purpose of complying with Rule 13a-14(b) or Rule 15d-14(b) of the Securities Exchange Act of 1934 (the "Exchange Act") and Section 1350 of Chapter 63 of Title 18 of the United States Code.

Himanshu Patel, Executive Vice President, Chief Financial Officer (principal financial officer) of First Data Corporation, certifies that, to the best of his knowledge:

1. The Report fully complies with the requirements of Section 13(a) or 15(d) of the Exchange Act; and

2. The information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of First Data Corporation.

Date: February 25, 2016

/s/ HIMANSHU A. PATEL

Himanshu A. Patel
Executive Vice President, Chief Financial Officer
(principal financial officer)

Appendix 2

Kelly Tinsley

Executive Oversight

Professional Experience

Ms. Tinsley is a skilled manager who specializes in organizing and managing resources to successfully achieve strategic project goals and objectives for human services clients using web-based CRM, e-commerce and ERP solutions. She is an experienced manager offering 17 years' progressive expertise in leadership and problem solving for social services, public sector, not-for-profit, pharmaceutical, automotive, education and financial industries. Ms. Tinsley is a business strategist with experience planning and managing multimillion-dollar projects, and aligning business goals with technology solutions to drive process improvements. Ms. Tinsley effectively manages large project teams and is known for high-quality deliverables that meet or exceed timeline and budgetary targets.

Relevant Experience

Company Name	First Data
Project Name	Various
Timeline	2015 – Present
Position Title	Director, Professional Services Midwest Region

Ms. Tinsley is currently providing Executive Oversight for several key large Indiana accounts, including the Indiana Eligibility Determination Services System (IEDSS) - IV&V, Indiana Medicaid Management Information System (MMIS) OV&V/UAT, and Indiana ICES OV&V. She also provides Executive Oversight for human services projects in other states.

Company Name	Johnson & Johnson, LifeScan, Inc.
Project Name	Various
Timeline	2013 – 2015
Position Title	Contract Project Manager, Data Governance Strategy and Implementation, Digital Marketing

Ms. Tinsley led the design, development, implementation, and support of business solutions for consumer data management. She managed data applications through complete lifecycle, as well as managed cross cultural and cross domain teams, and led team for Data Cleansing and standard processes. She led and facilitated cross functional teams to develop organizational design and data governance initiatives, and established direction to define and document business processes. She identified root causes and risks and developed and recommended solutions for customers.

Company Name	International Business Machines
Project Name	Various
Timeline	2009 – 2013

Position Title	Associate Partner, Social Services – Project Assurance, Sales and Delivery

Ms. Tinsley provided project oversight, business development and delivery for IBM Social Services offerings, including Cúram Software, case management and CRM solutions. She delivered oversight for multiple states, localities and not-for-profits for social services case management, HIE, integrated eligibility and unemployment insurance. Ms. Tinsley was responsible for revenue, profit, sales, pipeline generation and client relationships for consulting services in strategic states. She developed client strategies and business cases. She also managed proposal development for SLE case management, health insurance exchange, Medicaid eligibility, integrated eligibility and unemployment insurance.

Company Name	International Business Machines
Project Name	Various
Timeline	2003 – 2009
Position Title	Project Manager, Social Services Delivery

Ms. Tinsley planned, executed, and finalized projects within triple constraints of delivering on time, within budget and scope objectives, including acquiring resources and coordinating efforts of team members in order to deliver projects according to plan. She identified, effectively communicated, and resolved project issues and risks. She coached, mentored, and motivated team members, influencing them to take positive action and accountability for assigned work. Ms. Tinsley managed project portfolios ranging from $5M to $20M. Her scope of responsibilities included implementing stakeholder requirements for system design, development and implementation. She performed extensive delivery risk reviews for prospective projects, gathering details utilized for pricing services, evaluating project and contract risks and providing actionable plans to achieve profitability.

Company Name	International Business Machines
Project Name	Various
Timeline	1998 – 2003
Position Title	Project Manager, Public Sector Delivery

Ms. Tinsley was the Project Manager for IBM Public Sector offerings. She was handpicked as preferred project manager for multiple troubled project recovery efforts, selection determined by key branch office delivery managers and customer teams. She demonstrated outstanding leadership and superb project management skills. Ms. Tinsley stepped in, turned around, and saved a $5.5M project, successfully restoring client confidence for a two-year, at-risk project by building and deepening customer relationships for the express purpose of surpassing client expectations and advancing project status. She pioneered innovative team building and cross-functional project management techniques to expedite workflow, simplify processes, and reduce operating costs.

Company Name	International Business Machines
Project Name	Various

Timeline	1996 –1998
Position Title	Senior Business Analyst, Industrial and Public Sector Delivery

Ms. Tinsley was the Business Analyst and Process Consultant for Industrial and Public Sector clients. She led multi-person teams in Requirement Analysis, JAD sessions, Business and Systems reviews and working sessions to understand the requirements and system design for both COTS and custom developed applications. Ms. Tinsley implemented a Package Enabled Business Transformation discipline surrounding requirements/change management, impact analysis, gap analysis, development testing, and training.

Education

Degree	• BS, Japanese and French, Georgetown University • Candidate MBA/MA, University of Michigan Finance / Asian Studies (two courses remaining)
Professional Development	• Project Management Professional (PMP) (I), CIPM (I) • Contract and Deliverables Management (IBM), Detailed Estimation (IBM), Project Financials (IBM), Delivery Excellence & Leadership – FFP Management, Start it Right, Improving Project Profitability (IBM)

References

Company Name	California Department of Industrial Relations
Contact Name	James Culbeaux, CIO
Address	Reference prefers phone or email contact
Phone Number	415-703-4454
Email Address	jculbeaux@dir.ca.gov

Company Name	California Department of Industrial Relations
Contact Name	Mark Fudem, Judge
Address	Reference prefers phone or email contact
Phone Number	707-480-9722
Email Address	mfudem@dir.ca.gov

Company Name	Deliotte, LLP
Contact Name	Shelley Mills-Brinkley, Director
Address	Reference prefers phone or email contact
Phone Number	203-915-0038
Email Address	Shelley.mills-brinkley@deloitte.com

Alan F. Ashurst
EES Project Manager

Professional Experience

Mr. Ashurst is an information technology professional with extensive management and leadership expertise in the health care, government, technology, transportation, and beverage industries. He applies passion and high ethical values to bring team leadership, people and project management, process implementation, and strategic planning skills to enable organizational success.

Relevant Experience

Company Name	First Data Government Solutions, LP
Project Name	Nebraska Department of Health and Human Services, Division of Medicaid and Long-Term Care
Timeline	February 2014 - Present
Position Title	Project Manager

Mr. Ashurst manages day-to-day activities of the IV&V team and maintains the project schedule. Duties include creation and presentation of Monthly Management and Briefing reports, risk/issue management, and development of the overall IV&V Project Management Plan. Mr. Ashurst leads verification and validation of project's product and processes, contributes to Deliverable Review Reports and is the primary customer/SI liaison for IV&V.

Project Name	Connecticut Department of Social Services (DSS) Modernization Planning and Procurement
Timeline	August 2013 – January 2014
Position Title	Analyst

Mr. Ashurst is an integral member of First Data's team advising the State on resource capacity planning, process and technology improvements related to Human Services eligibility system modernization. This project includes a technical assessment as well as a Cost Benefit Analysis (CBA) to provide both technical standards for the modernization effort and cost justification for the project objectives.

Project Name	South Dakota Eligibility Planning
Timeline	June 2013 - August 2013
Position Title	Analyst

Mr. Ashurst provided expert analysis on First Data's team to aid the State in planning for an eligibility and enrollment system replacement. South Dakota requested this analysis to modernize their legacy eligibility system, improve the delivery of services with innovative best practices and state-of-the-art technologies, and to implement federal and state

compliancy standards while leveraging enhanced Federal Financial Participation match dollars.

Company Name	Sandata Technologies, LLC
Project Name	Various
Timeline	July 2012 – May 2013
Position Title	Implementation Director

Mr. Ashurst was responsible for the overall direction, coordination, execution, control and completion of specific implementations of home health care agency management and monitoring solutions; ensuring consistency with company strategy, commitments and goals.

Company Name	Policy Studies/Maximus
Project Name	Various
Timeline	January 2012 – July 2012
Position Title	Solution Architect

Mr. Ashurst developed capture strategies including business solution, potential customers, competitive assessments, teaming suppliers, and price to win for Health Insurance Exchange, Medicaid/CHIP Enrollment Broker, and specialized HHS Call Center opportunities.

Company Name	HP Enterprise Services
Project Name	Various
Timeline	October 2010 – January 2012
Position Title	Healthcare Eligibility Product Manager

Mr. Ashurst is defining the vision for public Health Benefits eligibility products to align with US health care reform as specified by the Patient Protection and Affordable Care Act . He was responsible for product planning and execution from inception through the product lifecycle, including gathering and prioritizing product requirements, defining the product vision, and working closely with Product Development, Sales, and Delivery units to ensure revenue and customer satisfaction goals are met.

Company Name	State of Colorado, Department of Health Care Policy & Financing
Project Name	Various
Timeline	August 2009 – September 2010
Position Title	Claims Systems Section Manager

The Department of Health Care Policy and Financing administers the Medicaid and Child Health Plan Plus programs as well as a variety of other programs for Colorado's low-income families, the elderly, and persons with disabilities. Mr. Ashurst's specific duties included the following:

- Provided the operational interface between State policy/program staff and the fiscal agent who manages the Medicaid Management Information System (MMIS).
- Managed department staff to provide user acceptance testing of fiscal agent changes
- Worked with program/policy staff to obtain knowledge of program policy/rules and ensure that the MMIS enforces and supports those rules operationally and systematically.

Education

Degrees	• M. S. - Organizational Leadership and Executive Project Management, Regis University, 2016 • B.S., Business Administration (Management), Regis University, Denver, 2004, Magna Cum Laude
Certifications	• ITIL Foundations, Six Sigma Green Belt, Leadership Development Program, Center for Creative Leadership

References

Company Name	State of Colorado
Contact Name	Jennifer Okes, Director of Public School Finance
Address	201 E. Colfax Ave, Denver, CO 80203
Phone Number	(303)866-2996
Email Address	okes_j@cde.state.co.us

Company Name	State of Colorado
Contact Name	Guy Mellor, State Human Resources Director (ret.)
Address	31758 Chalet Drive, Conifer, CO 80433
Phone Number	(303) 921-4341
Email Address	guymellor@wispertel.net

Company Name	State of Colorado, Health Care Policy & Financing
Contact Name	Sandra Salus, Manager of Fee for Service Unit
Address	1570 Grant St. Denver, CO 80203
Phone Number	(303)866-3513
Email Address	Sandra.salus@state.co.us

Willard Starlard

EES Business Analyst

Professional Experience

Mr. Starlard brings over thirty years of information technology experience in state government, military and public utilities with comprehensive involvement in the complete system development lifecycle at both project management and technical levels including analysis, design, development, conversion, testing, and implementation. He has extensive experience in team leadership, independent verification and validation, business analysis, and Business requirements documentation. He has broad application experience in design, development and implementation in eligibility, child welfare, inventory management and other state services.

Relevant Experience

Company Name	First Data Government Solutions
Project Name	Arkansas Department of Human Services-Eligibility & Enrollment Framework
Timeline	July 2013 – December 2015
Position Title	IV&V Technical Manager / Project Lead

Mr. Starlard evaluated project plans and development adherence. He also evaluated development quality of deliverables. He provided detailed recommendations for development and testing improvement, risk mitigation and contingency options. Mr. Starlard worked directly with the client and vendors to gather and communicate pertinent information and coordinate with the First Data Team's comprehensive status reports. He executed specific client related evaluations with documentation on findings.

Company Name	Ciber
Project Name	Mississippi, Department of Human Services-National Accuracy Clearinghouse Pilot Project
Timeline	August 2012 – July 2013
Position Title	Project Lead

The National Accuracy Clearinghouse Pilot Project was a federal project created to reduce and/or eliminate dual participation within the SNAP and D-SNAP programs between participating states. Mr. Starlard was responsible for evaluating proposals submitted for the development and evaluator vendor. He coordinated the 5 pilot states (AL, FL, GA, LA and MS) involved in the project. He also tracked the established project budget ($2.5 million). Mr. Starlard managed the development and evaluator vendors to confirm project work plan tasks were met and deliverables were accepted and approved through the collaborative efforts of the governance council.

Company Name	Northrup Grumman / TRW
Project Name	Arkansas, Department of Human Services, Decision Support System (Child Care Data Warehousing) Project & DoD Supplemental Nutrition Assistance Program
Timeline	July 2003 – March 2012
Position Title	Business & Technical Analyst

Mr. Starlard was responsible for gathering of user requirements through JADs, and documentation of those requirements for the Decision Support System (Child Care Data Warehousing Project) and the DoD Supplemental Nutrition Assistance Program (SNAP) Project. He interacted with Departmental heads and upper management levels regularly. He developed specialized training scripts, as well as management reports and scorecards.

Company Name	SCB Computer Technology, Inc.
Project Name	Various
Timeline	October 1995 – July 2003
Position Title	Various

Mr. Starlard supported the following projects:

- **State of Arkansas, Department of Human Services, CHRIS Project** - The Children's Reporting and Information System (CHRIS) was developed to meet the needs of our family service workers. The system reduces paperwork, provides tools to track the children and families to assure that information being collected is correct. Mr. Starlard filled several roles on this project as follows:
  - ✓ Project Manager - Responsible for the overall management of the CHRIS project at a contractor level. Managed eight developers, two DBAs, one Senior Systems Analyst, two Technical Analysts and one UNIX Administrator. Responsible for the coordination of development and deployment of enhancement / maintenance releases for CHRIS.
  - ✓ Technical Manager - Responsible for the coordination of development and deployment of enhancement / maintenance releases for CHRIS.
  - ✓ PB Technical Analyst - Responsible for leading the analysis of applications development for the CHRIS system.
  - ✓ Lead Developer - Lead the development team of eight programmers to develop and enhance the CHRIS application.
- **State of Alabama, Department of Public Health** - Mr. Starlard was the Powerbuilder Mentor on the Business Analysis team helping to develop initial requirements for the set-up of a client/server development team with special emphasis on POWERBUILDER application development.

Company Name	Digital Equipment Corporation
Project Name	Various
Timeline	November 1994 – October 1995

Position Title	Lead Analyst

Mr. Starlard was responsible for RAD development of a major requisition application. He performed business analysis and data analysis, and provided high level to detailed specifications.

Company Name	Greyhound Lines, Inc.
Project Name	Various
Timeline	June 1992 – November 1994
Position Title	Programmer / Lead Analyst

Mr. Starlard was responsible for leading design efforts by developing detailed project plans and allocating resource requirements. He designed interfaces with multiple platform projects he was involved in, and improved the planning department's ability to perform decision support analysis to plan transportation capabilities for a nationwide bus network.

Education

Degree	• B.S. in Computer Science, Southern University

References

Company Name	Datapath
Contact Name	Ken Benson
Address	46 Emerald Drive Maumelle, AR 72113
Phone Number	501-247-1839
Email Address	Benson7@sbcglobal.net

Company Name	Mississippi Department of Human Services
Contact Name	Valeria O'Neal
Address	750 North State Street Jackson, MS 39202
Phone Number	601-359-4640
Email Address	valeria.o'neal@mdhs.ms.gov

Company Name	Arkansas Department of Information Systems
Contact Name	Kimberly Gardner
Address	One Capital Mall, Suite 3 Little Rock, AR 72201
Phone Number	501-231-8612
Email Address	kim.gardner@arkansas.gov

David Sullivan, PMP

EES Business Analyst

Professional Experience

Mr. Sullivan is a certified Project Management Professional and Certified Scrum Master with expertise in project management, quality assurance, independent verification and validation, development, and training services to government health and human services agencies. For the past 20 years, he has managed teams of IT professionals in the areas of analysis, design and development of new technology solutions, project management and oversight, cost-benefit analysis, and system design.

Relevant Experience

Company Name	First Data Government Solutions, LP
Project Name	Nebraska Department of Health and Human Services Eligibility and Enrollment Solution (EES)
Timeline	April 2015 – Present
Position Title	Senior Business Consultant

Mr. Sullivan serves as a Senior Business Consultant leading assessments of plans, processes, and creation of IV&V deliverables. He conducts in-depth analysis of the vendor's deliverables to ensure that they complied with stated requirements and analyzes users' needs to ensure the solution provides the desired functionality. He is responsible for leading IV&V risk assessments and for producing risk assessment reports. He also establishes and monitors project performance metrics and reporting.

Company Name	Catholic Health Initiatives, EPMO – Physician and Clinical Services
Project Name	Various
Timeline	April 2013 – April 2015
Position Title	Senior Project Manager / Program Manager

Mr. Sullivan served as the Enterprise Project Management Office Program / Project Manager, and led the effort to implement a CHI strategic initiative to replace traditional infusion pumps with computerized medication safety and infuser managed IV pumps across all (39) CHI facilities ($37- million). He also led the effort to implement a cardiovascular review and reporting solution that integrates with Dragon speaking naturally dictation solution and interfaces with the electronic health record system and the archive system

Company Name	First Data Government Solutions, LP
Project Name	Louisiana Department of Children and Family Services Transformation Project
Timeline	July 2012 – April 2013

Position Title	PMO UAT Lead

Mr. Sullivan acted as the Project Management Office UAT Lead for a project that encompassed three projects: common Access Front End, Document Imaging and Content Management, and Customer Service Center. He assisted State staff by providing project management support, UAT management support, mentoring of State staff and issue and risk management. He established and monitored UAT defect tracking, reporting and resolutions. Mr. Sullivan reviewed deliverables to verify that deliverables matched requirements and provided the desired functionality. He also participated in deliverable reviews to confirm that all of the requirements across the three projects were met and met the expectations for a streamlined and integrated solution.

Company Name	Software Engineering Services (SES)
Project Name	Various
Timeline	December 2005 – July 2012
Position Title	Senior Project Manager/Project Consultant

Mr. Sullivan supported the following projects during his employment:

- **Veterans Administration Central Iowa Healthcare System (VA CIHCS)** - Mr. Sullivan coordinated a facility wide assessment covering the current policies, procedures, and actual practices to produce reports. He led the effort to develop a single reporting solution that saved an estimated 3,000 hours and allowed for automated report generation.
- **Florida Department of Revenue Independent Verification and Validation (FL IVV)** - Mr. Sullivan conducted in-depth analysis of the vendor's deliverables to ensure that the deliverable complied with contract, stated requirements, and user's needs. He observed system and integration testing of the vendor's code to ensure that the deliverable complied with contract, stated requirements, and user's needs.
- **Douglas Omaha Technology Commission (DOT.Comm)** - Mr. Sullivan coordinated the security assessment covering policies, procedures, actual practices, and network. He assisted with business cases to secure funding to act on the recommendations proved.
- **Texas Health and Human Services Commission** - Mr. Sullivan managed the IV&V team assisting with Medicaid development including expanding the team role into other facets of the Medicaid development effort. He worked with the Client and the Development Vendor to develop and document the submittal, review, and approval processes including redefining the scope of work to better meet the Client's needs. He also assisted in collecting and analyzing cost estimates to the actual invoiced amounts.
- **Blue Cross Blue Shield of Nebraska** - Mr. Sullivan managed the upgrade of enterprise imaging system including porting to new technology. He managed the multi-phase (year) design and development of a national data warehouse. Mr. Sullivan participated in project management process development, and contributed to change management process development.
- **SES Corporate PMO** - Mr. Sullivan served as the Senior PMP and SCM in the PMO. He led the new software development for automating project management office using the capability maturity model as a framework. He recommended and participated in

project management training, coordinated and conducted PMP exam prep classes for the staff, including assisting with preparing the application.

Company Name	Mutual of Omaha
Project Name	Various
Timeline	May 2000 – December 2005
Position Title	Lead Analyst / Project Manager

Mr. Sullivan managed new technology projects, including implementing the data warehouses used at the home office for the Group Health Division. He developed and implemented new processes for managing rapid development projects. He also developed a process for managing and reporting on related repeatable short duration activities and projects.

Education

Certification	• Project Management Professional (PMP) certification • Certified Scrum Master

References

Company Name	Chief, Enterprise and Solutions Architecture Branch, US Strat-Com
Contact Name	John Kuklinski
Address	901 SAC Bl #BH5 Offutt AFB, NE 68113
Phone Number	Available on request
Email Address	Available on request

Company Name	Information Services Manager, Mutual of Omaha
Contact Name	David Kern
Address	3301 Dodge St, Omaha, NE 68131
Phone Number	Available on request
Email Address	Available on request

Company Name	EPMO Program Director, Catholic Health Initiatives
Contact Name	Carrie Lousberg
Address	198 Inverness Dr W, Englewood, CO 80112
Phone Number	Available on request
Email Address	Available on request

Terry Honke

EES Technical Analyst

Professional Experience

Mr. Honke has more than 20 years of experience in technical support and management of large-scale projects. He has supported projects in Nebraska for 10 years, including serving as the Technical Lead on the current Nebraska DHHS eligibility and enrollment system project. Mr. Honke is a certified Scrum Master. He has directed teams in enterprise architecture, quality control, and application development.

Relevant Experience

Company Name	First Data Government Solutions
Project Name	Nebraska DHHS Modernization Medicaid Eligibility & Enrollment System
Timeline	January 2014 – Present
Position Title	Technical Lead

As an integral member of First Data's team, Mr. Honke advises the State on technical planning, requirements, architecture, design, development, and implementation topics related to the eligibility and enrollment systems. He uses his professional knowledge and experience to promote innovative best practice discussions. The project has allowed him to work closely with State business analysts to create and deliver attestation letters required for each round of testing associated with CMS Payment Error Rate Measurement (PERM) project. Each round of testing requires IV&V to attest to the quality control and quality assurance measures executed by the State prior to the submission process.

Company Name	IBM / Kenexa Corporation
Project Name	Various
Timeline	April 2011 – February 2013
Position Title	Director of Software Development

Mr. Honke reported to the Vice President of Operation and functioned in a Scrum Master role. He directed and managed Scrum teams in Lincoln, Nebraska and India and directed quality control and infrastructure teams. He provided governance and guidance on SOA web and mobile platforms, and was a member of the roadmap committee providing enterprise architectural oversight. He assisted with establishing product lifecycle management approaches and reduced post-deployment defects by instituting root cause analysis. He also replicated the application platform to the new European data center and implemented Agile methodology and Scrum processes.

Company Name	Ameritas Life Insurance Corporation
Project Name	Various
Timeline	January 2009 – April 2011

Position Title	Manager of Group IT Shared Services Development Team

Mr. Honke functioned as Scrum Master, establishing and managing the Shared Service Application Development team implementing elements of Agile/SCRUM development, and resource procurement. He established a Service Oriented Architecture (SOA) platform. He captured business requirements, defined solution architecture, managed BI warehouse reporting, EDI and operational support teams. He also facilitated change control board meetings and business planning sessions. Mr. Honke was the EDI and MAR compliance point of contact. He completed enterprise architecture center of excellence certification training and deployed the first Websphere portal and SOA applications. He also formalized test and release methodology for Websphere portal projects.

Company Name	National Research Corporation
Project Name	Various
Timeline	July 2005 – January 2009
Position Title	Director of Application Development

Mr. Honke directed application development teams and handled resource procurement. He restructured individual developers into a comprehensive application development entity and implemented Agile/SCRUM software development methodology. He gathered executive business requirements to create an enterprise solution and architecture, and managed BI and database support, quality control, and operational support teams. Mr. Honke was the SOX Development Officer and a member of the Internal Standards Committee. He established the corporate change board and holistic solution planning sessions, formalized the testing and release methodology within the organization and implemented Microsoft SharePoint devices within operational and business teams.

Company Name	Blue Cross Blue Shield Nebraska
Project Name	Various
Timeline	November 1998 – July 2005
Position Title	Director of Product Development

Mr. Honke executed the project charter and converted DOS claim processing system into Windows/Internet EDI HIPAA based applications for both professional and institutional lines of business. He directed EDI product development involving joint venture between Blue Cross Blue Shield Nebraska and Blue Cross Blue Shield Kansas. Mr. Honke established Standard Operating Procedures (SOP) for product development to guarantee Federal compliance with HIPAA and PHI mandates, and delivered 4 software products in 5-year period on time and within budget. He institutionalized Rational Unified Process / Iterative and formalized the UML project model along with the supporting Artifacts. He established a comprehensive product development team, and started holistic solution planning sessions based around solution architecture.

Education

Degree	• Associate Of Applied Science/Computer Technology, Southeast

	Community College, 1981 • Bachelor Of Science/Business Administration (Computer Science), University Of Nebraska-Lincoln, 1979
Certifications	• Scrum Master (Scrum Alliance Certified/Jean Tabaka) • Agile Methodology (ASCIT/Sally Elatta) • Corporate Balanced Scorecard (Blue Cross Blue Shield) • Enterprise Architect (John Zachman) • Enterprise Architecture Center of Excellence Certification (Sam Holcman) • HIPAA certified (Ameritas Life Insurance, Blue Cross Blue Shield, National Research) • IBM Functional Tester, Websphere Portal Certification (IBM) • Management and Leadership (Gallup University) • Mercer Performance Management (Blue Cross Blue Shield) • Microsoft Solution Framework (Blue Cross Blue Shield) • Rational Business Requirements, UML, and Unified Process

References

Company Name	IBM / Kenexa
Contact Name	Jon Zvolanek, Vice President of Operations
Address	Lincoln, NE
Phone Number	Available by Request
Email Address	Available by Request

Company Name	IBM / Kenexa
Contact Name	Sandy Deets, Director of Survey Systems
Address	Crete, NE
Phone Number	Available by Request
Email Address	Available by Request

Company Name	James Fairchild
Contact Name	Ameritas Life Insurance Corporation, Web Lead Developer
Address	Lincoln, NE
Phone Number	Available by Request
Email Address	Available by Request

Marianne Kennedy, PMP

DMA Project Manager

Professional Experience

Ms. Kennedy has more than 30 years of experience in technology business leadership, in the areas of consulting, enterprise, and IT strategic planning. She has spent over 10 years supporting efforts in enterprise architecture and technology strategic planning. She also brings more than 4 years of healthcare experience, supporting health information technology, data analytics, MITA, HIPAA, and ACA. Ms. Kennedy is skilled in agile and software development management, as well as technical operations.

Relevant Experience

Company Name	First Data Government Solutions, LP
Project Name	New Mexico HSD PMO – MMIS-R and CSES-R PMO
Timeline	July 2015 – March 2016
Position Title	Project Director

Ms. Kennedy led the New Mexico Medicaid PMO during the planning, requirements and early procurement phases of their MMIS replacement project and the Child Support Enforcement System replacement project. As Project Director over both projects, she worked with the client on project priorities, resources for PMO and staff augmentation, development of the procurement strategy to support the HSD 2020 Vision, development of Enterprise Architecture components, MMIS migration approach, and requirements development and delivery for both MMISR and CSESR.

Company Name	Xerox Government Health Services
Project Name	California MediCal Program (CAMMIS)
Timeline	February 2014 – July 2015
Position Title	Enterprise Integration Officer

Ms. Kennedy worked with the California Health and Human Services Agency, the Department of Health Care Services (DHCS) Director of the CAMMIS program and Xerox Executive team in the role of Enterprise Integration Officer. She provided leadership in cross organizational coordination of CAMMIS Business Operations, Legacy Systems Group, Technical Operations and System Replacement Delivery. As Enterprise Integration Officer working with the DHCS leadership, led business process and organization change management to support the transition from the Legacy systems and operations to the replacement MMIS including business process re-engineering, organizational skills requirements, and integration of legacy and replacement operations. As a subject matter expert, provided Enterprise Architecture and roadmap analysis with recommendations for risk mitigation, and developed the Scope Definition Document as a primary deliverable in the Scaled Agile Methodology for SCRUM teams vision and scope alignment.

Company Name	Kennedy Consulting
Project Name	Health Information Exchange Architecture and Roadmap
Timeline	September 2013 – February 2014
Position Title	Enterprise Architect Consultant

Ms. Kennedy worked with the California Health and Human Services Agency, the Department of Health Care Services (DHCS) Director of Enterprise Architecture and CalOHII's Chief Medical Information Officer to develop the Health Information Exchange Architecture and Roadmap. She developed a roadmap with initiatives including MDM, IdAM, SOA and ESB, Member and Provider Portals, Big Data Analytics for population analysis and fraud detection, Technical Services re-use strategy, and Enterprise Roadmap and Portfolio Management Process development.

Company Name	Natoma Technologies, Inc.
Project Name	Various
Timeline	October 2009 – April 2012
Position Title	Program Manager/Senior Project Manager

Ms. Kennedy implemented program management for major technology initiatives, and mentored PMO staff. She supported the following agencies:

- California Department of Insurance – provided PMO program management support for a large technology project.
- California Office of Statewide Hospital Planning and Development – supported full business process reengineering and implementation of Accela COTS product for the facilities development division.
- California Health Benefit Exchange – supported proposal development for CalHEERS project; provided input on overall architecture, design, MITA requirements, and system integration to meet federal funding timelines.

Company Name	Kennedy Consulting
Project Name	Various
Timeline	April 2009 – October 2009; October 2002 – June 2004
Position Title	Principal/Consultant

Ms. Kennedy provided consulting services to start-up and small businesses in the areas of business plan development, business valuation and capitalization strategies. She supported efforts in business process reengineering to streamline operations and reduce costs. She led implementations of technology to increase revenue opportunities and operating efficiency.

Company Name	Amdocs Ltd/DST Innovis
Project Name	Various
Timeline	May 2004 – February 2009

Position Title	Project Manager/Manager of Product Management

As project manager, Ms. Kennedy worked with development teams around the world, and was responsible for PMO oversight of 8 project teams in the development of new software products supporting a rapidly changing market. She led product planning, scope development, cross-organization change management processes, product requirements traceability for a $100M program. She also was responsible for the release management process for synchronized integration testing across 8 concurrent development streams using an Agile methodology.

Education

Degree	• M.S. in Systems Management, University of Southern California • B.A. in Business/Economics, UCLA
Certification	• Project Management Professional (PMP) • Certified Enterprise Architect Professional (PEAF Pragmatic Enterprise Architecture Framework) • Certified SCRUM Master • Certified SCRUM Product Owner

References

Company Name	California Department of Health Care Services
Contact Name	Phil Heinrich, Chief Office of HIPPA Compliance
Address	P.O. Box 997413, MS 4722, Sacramento, CA 95819-7413
Phone Number	916-552-9050
Email Address	Philip.Heinrich@dhcs.ca.gov

Company Name	Medix Consulting, LLC
Contact Name	Belinda Ramirez, General Manager
Address	1024 Iron Point, Folsom CA 95630
Phone Number	916-496-3071
Email Address	Belinda.Ramirez@MedixConsulting.com

Company Name	RMS
Contact Name	Cynthia Izuno-Levin, Director Program Management
Address	7575 Gateway Blvd., Newark CA 94560
Phone Number	408-242-5477
Email Address	Cynthia.l.levin@gmail.com

Michael Lawson

DMA Business Analyst

Professional Experience

Mr. Lawson is an experienced consultant, analyst, and subject matter expert in the healthcare industry who brings over 10 years of Medicaid expertise including fiscal agent operations, Medicaid Management Information Systems (MMIS), Independent Verification & Validation (IV&V) and Project Management Office (PMO) experience. His background has included User Acceptance Testing management and coordination, training development, requirements gathering and analysis, schedule management, technical analysis, and development of Request for Proposal (RFP) requirements.

Relevant Experience

Company Name	First Data Government Solutions, LP
Project Name	Center of Excellence
Timeline	January 2016 – Present
Position Title	Government Consultant

Mr. Lawson is supporting the internal Center of Excellence, lending his MMIS Subject Matter expertise to the development, review, and enhancement of templates, tools, and methodologies. The continuous improvement within this community provides a greater maturity level that corresponds directly to the staff efficiencies and effectiveness on all of our related projects. The artifacts maintained as part of our methodologies and processes are available to our staff at all times and part of our Day One solution.

Company Name	CSG Government Solutions
Project Name	Wisconsin Division of Health Services ICD-10 Transition, MITA 3.0 Assessment, MMIS Strategy & Procurement
Timeline	May 2013 – December 2015
Position Title	Senior Consultant / SME / UAT Manager

Mr. Lawson has supported Wisconsin's Division of Health Services on multiple initiatives:

- **MITA 3.0 Assessment, MMIS Strategy and Procurement Approach** - provided the CSG team with subject matter expertise on the Wisconsin Medicaid technical environment; documented requirements during the MITA SS-A workshops; coordinated high level and detailed requirements development
- **ICD-10 Transition** - provided User Acceptance Testing Management services; assisted in the development of business requirements; facilitated sessions to review and revise functional/non-functional requirements with DHCAA subject matter experts; maintained ICD-10 project plan, coordinated ICD-10 training development

Company Name	Xerox

Project Name	Various
Timeline	October 2005 – April 2013
Position Title	Various

Mr. Lawson held the following positions during his employment with Xerox:

- **New Mexico Medicaid, Claims and Third Party Liability Manager** - Mr. Lawson managed Medicaid claims processing and TPL Helpdesk. He was a subject matter expert (SME) for multiple Joint Application Design (JAD) sessions for gathering and defining requirements. He implemented Business Process Management (BPM) workflow processes for all operational areas. He implemented a change control process for BPM/Workflow. He also verified and validated testing. Mr. Lawson was the MS System Contact for New Mexico Medicaid Electronic Document Management System (EDMS). He supported proposal writing and review for Claims and EDMS sections of a successful New Mexico rebid. He also functioned as a first point of contact and liaison for SAS70 audit. He managed multiple vendors providing systems administration and support, and developed forms to improve operational efficiency.
- **Claims, Third Party Liability and Provider Enrollment Manager** - Mr. Lawson managed all functions of mailroom, scanning, data entry, claims resolution, TPL, and provider enrollment. He supported proposal writing and review for the TPL section of a successful Hawaii rebid. He functioned as a first point of contact and liaison for SAS70 audit. Mr. Lawson served as a SME for Medicaid Information Technology Architecture (MITA) assessment, ICD-10 assessment, and HIPAA 5010 assessment.
- **Continuous Quality Improvement Manager** - Mr. Lawson managed processes and procedures for quality assurance and training. He validated all operational procedures. He served as the first point of contact and liaison for SAS70 audit. He increased quality awareness within the account, and increased knowledge base of quality associates. He developed error trend tracking and analysis processes. Mr. Lawson implemented piece rate compensation program for quality assurance department. He tracked performance indicators for an operational report card. He also facilitated Medicaid and MMIS training.
- **Business Analyst** - Mr. Lawson tested and tracked defect issues and system enhancements. He served as an interface between developers and users to translate business requirements into technical specifications. He reviewed and approved DLAs and DLEs. He also developed test plans, performed testing, and verified test results.
- **Claims Support and Third Party Liability Supervisor** - Mr. Lawson supervised claims resolution and third party liability processes and teams. He implemented piece rate compensation program for TPL department, and managed multiple enhancements to OCR.
- **Claims Support Supervisor** - Mr. Lawson was responsible for overseeing and improving claims resolution and adjustment functions. He implemented piece rate compensation program for the claims support department. He developed, wrote, revised and/or validated all department manuals including procedures, training material and supporting documentation. He also assisted with optical character recognition implementation.

Education

Degree	• A.A. in Business Administration, Central New Mexico Community College

References

Company Name	State of Wisconsin, Department of Human Services
Contact Name	David Ebert
Address	Available on request
Phone Number	(608) 577-6235
Email Address	Davida.ebert@dhs.wisconsin.gov

Company Name	State of Texas, Department of Aging and Disability Services
Contact Name	Ammar Bhaisaheb
Address	Available on request
Phone Number	(512) 438-4451
Email Address	Ammar.bhaisaheb@dads.state.tx.us

Company Name	CDMS, Inc.
Contact Name	Perry Kurlander
Address	Available on request
Phone Number	(717) 540-1301
Email Address	Perry.kurlander@cdmspa.com

Wayne Walton

DMA Business Analyst

Professional Experience

Mr. Walton is an information systems consultant with experience in project management and SDLC methodologies. He is experienced in requirements gathering and analysis and documentation. He brings subject matter expertise in CMS healthcare policy. Mr. Walton has supported several state government agencies in health and human services efforts.

Relevant Experience

Company Name	Ciber, Inc.
Project Name	WellCare Managed Care Organization
Timeline	July 2015 – December 2015
Position Title	Principal Consultant

Mr. Walton served as a consultant and healthcare subject matter expert on new state managed care organization projects, including Iowa and Georgia. Mr. Walton analyzed and aligned WellCare's Managed Care Program requirements with the CMS MITA processes.

Company Name	CSG Government Solutions
Project Name	Various
Timeline	November 2012 – March 2015
Position Title	Senior Consultant/Business Architecture Lead

Mr. Walton provided broad experience and consulting skills as a business analyst, project manager, and subject matter expert on a variety of government related projects involving: IV&V, MITA, MMIS, Business Technology and Architecture Framework.

Company Name	GeBBS Technology Solutions
Project Name	Multichannel Enrollment Project, NASCO
Timeline	June 2011 – October 2012
Position Title	Product Designer

Mr. Walton provided subject matter expertise in an Agile SDLC by supporting software engineering, QA, and product management within the commercial, Medicaid Health Insurance Exchange space, focusing on ASC X12 Standards for EDI. Mr. Walton provided Medicaid expertise to NASCO Government Services while assisting in creating, analyzing, and proposing a new line of business that included processing health claims for various State Medicaid programs.

Company Name	Axiom Systems
Project Name	South Carolina HIPAA 5010

Timeline	April 2011 – May 2011
Position Title	Business Analyst

Mr. Walton provided expertise in assisting the Department of Health and Human Services (SCDHHS) in meeting federally mandated compliance for Medicaid health care claim processing using the HIPAA 5010 transaction sets. He performed an analysis of existing processes used in providing Medicaid business services for the State's Provider, Member, Contractor communities in mapping the HIPAA 837 transaction set from 4010 to 5010.

Company Name	SLI Global Solutions
Project Name	Washington MITA SSA
Timeline	June 2010 – March 2011
Position Title	Lead Business Analyst

Mr. Walton provided expertise in leading the State of Washington's Medicaid Purchasing Administration through an enterprise wide federally mandated assessment of the processes the state utilizes to conduct Medicaid business services. He assessed current processes, initiatives, and goals in alignment with Federal guidelines for MITA.

Company Name	Diversified Services Network, Inc.
Project Name	Missouri Medicaid Web Portal Enhancement Project
Timeline	June 2009 – March 2010
Position Title	Senior IV&V Consultant

Mr. Walton provided IV&V of multiple enhancements for a 400 million dollar state wide systems reengineering implementation. As a consulting subject matter expert, he provided input and direction on client deliverables, oversight for the implementation of the Missouri Medicaid Web Portal Enhancement project, assisting with use case creation, UAT, and validating and verifying contractor submitted deliverables.

Company Name	Xerox
Project Name	Alaska MMIS Project
Timeline	February 2008 – June 2009
Position Title	Senior Systems Analyst

Mr. Walton supported daily and ongoing requirements identification, clarification, and validation for development of Alaska's new MMIS. Mr. Walton created scope diagrams and use cases for requirements analysis for technical and functional specifications. He established technical and design context for provider re-enrollment approach document.

Company Name	Modis and First Consulting Group
Project Name	Various
Timeline	October 2007 – January 2008
Position Title	Project Manager/Business Analyst

Mr. Walton delivered special projects for government healthcare solutions at CIGNA Healthcare (Nashville, TN) and UNITED Healthcare (Basking Ridge, NJ). He analyzed data models and created flow diagrams for projected implementations. He also conducted end user meetings to cull requirements and provide technical feedback.

Company Name	Symphony Corporation
Project Name	Tennessee Department of Health EHR Requirements and RFP Project
Timeline	September 2006 – September 2007
Position Title	Project Manager/Senior Business Analyst

Mr. Walton served as deputy project manager and technical consultant during the requirements gathering phase for State of Tennessee's Department of Health system replacement project. Mr. Walton led and facilitated joint application development sessions with client's business users to clearly define and document business needs. He developed Use Cases and Test Scenarios for the State client to introduce to the vendor.

Education

Degree	• B.B.A. in Computer Information Systems, Middle Tennessee State University

References

Company Name	Missouri MMIS IV&V
Contact Name	Mike Sizemore
Address	By Request
Phone Number	217-725-2482
Email Address	mike.sizemore@comcast.net

Company Name	Tennessee EMR
Contact Name	John A. Roberts
Address	By Request
Phone Number	615-741-3702
Email Address	John.A.Roberts@state.tn.us

Company Name	BCBS Medicaid/Medicare Claims Processing
Contact Name	Leon D. Adams
Address	By Request
Phone Number	336-643-4160
Email Address	lee.adams @nasco.com

Mark DeMaskey

DMA Technical Analyst

Professional Experience

Mr. DeMaskey has more than 15 years of experience in support of Medicaid and health and human service agency efforts. Mr. DeMaskey has contributed to MMIS DDI efforts across several states serving in many varied roles and brings extensive experience and leadership in the implementation of MMIS systems. Mr. DeMaskey brings considerable analytical and business intelligence experience and expertise. His healthcare career started in commercial health insurance and evolved to business intelligence development for the Medicare Services, Surveillance Utilization Review system.

Relevant Experience

Company Name	Blue Tack Consulting
Project Name	MMIS Procurement Projects – New Mexico and California
Timeline	August 2015 – Present
Position Title	MMIS Subject Matter Expert

Mr. DeMaskey serves as an MMIS SME and proposal writer for a major Medicaid procurement project. This includes the development of the architecture framework and business rules model.

Company Name	United Health Group – Optum
Project Name	MMIS DSS/DW projects – Alaska, New Hampshire, Arkansas
Timeline	July 2014 – May 2015
Position Title	MMIS Subject Matter Expert

Mr. DeMaskey served as a SME in a data analytics support role for Optum decision support systems/ data warehouses across several MMIS implementations. This involved Informatica ETL rules, Oracle, EDW, SQL, source-to-target mappings, business analytics, CMS reports, ACA, Medicaid Expansion Assessment, and enhancements for T-MSIS.

Company Name	Signature Consulting - Centers for Medicare and Medicaid Services
Project Name	MMIS T-MSIS – New Hampshire, Montana, West Virginia
Timeline	March 2014 – August 2014
Position Title	MMIS Subject Matter Expert/Technical Analyst

Mr. DeMaskey provided MMIS SME/guidance and technical assistance to several states for T-MSIS specifications and data analytics.

Company Name	Xerox
Project Name	Washington DC MMIS Project

Timeline	December 2013 – April 2014
Position Title	Systems Analyst

Mr. DeMaskey served in a developer role for the Affordable Care Act (ACA) eligibility and process integration design and development across Claims (FFS and Managed Care), Reference, DRAMS, and Financial Reporting.

Company Name	RLT Group
Project Name	South Carolina Dept of HHS MMIS Replacement Project
Timeline	February 2013 – November 2013
Position Title	Technical Director

Mr. DeMaskey was responsible for overall FFS claim and encounter integration, provider management, analytics, accounting, and case management. He confirmed that replacement MMIS projects were compliant with HIPAA, ACA, Federal and State regulations, and NIST security requirements.

Company Name	CSG
Project Name	Florida Agency for Health Care Administration MMIS - PMO ICD-10
Timeline	September 2012 – January 2013
Position Title	MMIS Consultant

Mr. DeMaskey provided technical analysis and program assessment guidance for ICD-10 remediation planning to the State project management office. CSG required a Medicaid technical SME familiar with the HP interchange MMIS.

Company Name	PCG
Project Name	Iowa Department of Human Services PMO / IV&V
Timeline	June 2012 – September 2012
Position Title	MMIS Subject Matter Expert

Mr. DeMaskey served in an enterprise business and technical support role to the State PMO data center. He managed the start-up phases for the MIDAS project IV&V.

Company Name	RLT Group
Project Name	CMS Innovation Center Health Care PMO
Timeline	March 2011 – June 2012
Position Title	MMIS Subject Matter Expert

Mr. DeMaskey provided strategic business and technical goals and architecture for a comprehensive service delivery model with supporting evidence to meet the CMS three-part aim of better health, better health care, and lower costs through improvement.

Company Name	Xerox
Project Name	Vermont Health Enterprise MMIS Solution

Timeline	January 2011 – March 2011
Position Title	MMIS Subject Matter Expert

Mr. DeMaskey provided proposal support for program management, member management, ICD-10 strategy, and MITA business area for a new Medicaid Enterprise Solution.

Company Name	Gabriel Systems
Project Name	Georgia Dept of Community Health PMO – MMIS Replacement
Timeline	July 2010 – January 2011
Position Title	MMIS Consultant

Mr. DeMaskey served as a claims/financial SME/ business analyst/ business architect for the Georgia HP interchange MMIS implementation.

Education

Degree	• B.A. in Economics, Rider University, 1989

References

Company Name	United Health Group - Optum
Contact Name	Mark Ballinger
Address	Denver, CO
Phone Number	(720) 624-9951
Email Address	VIP.com

Company Name	United Health Group - Optum
Contact Name	Pratima Nallagatia
Address	Alpharetta, GA
Phone Number	(404) 414-8484
Email Address	Truven.com

Company Name	Centers for Medicare & Medicaid Services (CMS)
Contact Name	Cindy Cockman
Address	Raleigh, North Carolina
Phone Number	(919) 946-5100
Email Address	Cindy.cockman@cms.dhhs.gov

Albert Decker

Privacy and Security Subject Matter Expert

Professional Experience

Mr. Decker is an award winning technology leader. He brings over 30 years of experience as a business and IT consultant, with 10 years of management and business ownership. He has experience with a wide variety of frameworks, platforms, tools and methodologies. Mr. Decker has held positions in both management and technology.

Relevant Experience

Company Name	First Data Government Solutions, LLP
Project Name	Various
Timeline	October 2012 – Present
Position Title	Senior Government Consultant

Mr. Decker most recently served on a project for Illinois' State Department of Insurance as a Data and Security Architect. He was responsible for leading security and privacy documentation and implementation for distributed and outsourced multi-vendor environments. He assisted with the data architecture vision, and was responsible for the development of security and architecture work products.

Mr. Decker also supported a project for Arkansas' Health Insurance Marketplace, serving as the Lead Security Assessor. He created the audit plan, reviewed documentation, and performed site visit due diligence. He also created deliverables with findings and recommendations.

Company Name	Xentity, LLC
Project Name	New York State Office of Temporary and Disability Assistance Transformation Project
Timeline	September 2010 – August 2012
Position Title	Enterprise Architect

Mr. Decker was responsible for the migration plan and architecture vision. He was accountable for the development of the architecture products, documenting the to-be architecture. Mr. Decker managed a team of business and technical analysts. He led the business and technical requirements analysis effort, and developed a migration plan.

Company Name	Career Education Corporation
Project Name	Various
Timeline	August 2010 – February 2011
Position Title	Adjunct Professor

Mr. Decker taught various IT-related courses for the International Academy of Design and Technology in an online format.

Company Name	Northrop Grumman
Project Name	Various
Timeline	October 2005 – May 2010
Position Title	Lead Enterprise Architect

Mr. Decker performed a variety of architecture and software development related duties for clients within county, state, and federal governments. His duties included delivering architecture training, leading teams, writing white papers, implementing repositories, transition planning, and project planning. He defined standard Enterprise Architecture Service offerings and deliverables. Mr. Decker advised clients on methodologies, processes and best practices. He performed analyses, authored white papers and other deliverables. He managed the Enterprise Architecture work stream as well.

Company Name	G&B Solutions, Inc.
Project Name	Department of the Interior
Timeline	June 2003 – October 2005
Position Title	Enterprise Architect/Business Analyst

Mr. Decker was directly involved in creating and enhancing the Department's award winning methodology, architecture repository, application and business architectures and modernization blueprints. He analyzed data for the creation of blueprints, participated in developing and documenting the methodology, and performed quality checks and data cleansing. Mr. Decker received the Award of Excellence from the client, as he moved the client from "worst to first" among federal departments for enterprise architecture.

Company Name	Systems Engineering Services Corporation
Project Name	Various
Timeline	December 2002 – June 2003
Position Title	Consultant

Mr. Decker provided clients with a broad range of analytical and technical expertise including data modeling and database design. He also assisted with application integration, security, telecommunications, and enterprise system performance tuning. Mr. Decker performed all phases of software engineering and solution implementation.

Company Name	Agent Life, Inc.
Project Name	Various
Timeline	June 2000 – December 2002
Position Title	Software Architect

Mr. Decker served as a solution architect for a SOA-based life insurance quoting platform. He implemented secure sites, including search, content management, and template based

look and feel. He provided technical leadership and coordination between management, marketing, clients and the implementation team. Mr. Decker developed enterprise standards for security, and general IT policies and procedures.

Education

Degree	• Masters of Business Administration, Strayer University, expected completion in 2017 • B.S. in Computer Information Systems, Excelsior College, 2002 • A.S. in Computer Systems, Daytona Beach Community College, 1989
Certifications	• Certified Enterprise Architect (CEA), FEAC Institute • Certified Information Systems Security Professional (CISSP) • Microsoft Certified Solution Developer (MCSD) • Microsoft Certified Database Administrator (MCDBA) • Microsoft Certified Systems Engineer (MCSE) • Sun Certified Java Programmer (SCJP)

References

Company Name	Illinois Health Insurance Marketplace
Contact Name	Mark Chudzinski
Address	Reference prefers email contact
Phone Number	312-814-4448
Email Address	Mark.chudzinski@illinois.gov

Company Name	Arkansas Department of Human Services
Contact Name	Mark Riley
Address	Reference prefers email contact
Phone Number	501-320-3968
Email Address	Mark.riley@dhs.arkansas.gov

Company Name	CDC Enterprise Architecture Project
Contact Name	John Fitzpatrick
Address	Reference prefers email contact
Phone Number	Reference prefers email contact
Email Address	jjjfitzpatrick@gmail.com

Julie Mauldin

CMS Gate Review Subject Matter Expert

Professional Experience

Ms. Mauldin is a PMP-certified senior consultant and project manager with 15 years of proven experience leading projects for public and private clients and delivering results on very tight timeframes. She has planned, designed and deployed multi-million dollar projects from RFP composition and planning to project launch and delivery. She is an expert in the implementation of Health Insurance Exchanges and integrated Medicaid eligibility, and has demonstrated experienced in the development of APDs, APD Updates and Level 2 grant applications.

Relevant Experience

Company Name	First Data Corporation
Project Name	State of Connecticut Health Insurance Exchange (Access Health CT)
Timeline	October 2014 – June 2015
Position Title	Senior IV&V Consultant / ACA and CMS SME

Ms. Mauldin is leading the IV&V for the IRS 1095 Monthly and Annual reporting requirements supporting the premium tax credit. She provides an independent confirmation that all testing expectations prior to a production submission were met. Ms. Mauldin's reviews confirmed test outcomes for each stage of testing were completed as expected. She also participates in meetings and calls with the Exchange, CMS and the IRS.

Company Name	SRA, International
Project Name	Center for Medicare & Medicaid Services Financial Management Support Program RFP Response
Timeline	February 2014 – April 2014
Position Title	IT Specialist – SRA International

Ms. Mauldin was recruited to write the technical response for the Center of Medicare & Medicaid Services (CMS) Financial Management Support Program RFP. Ms. Mauldin analyzed the RFP, Federal Regulation, and Business Process Models to establish the program technical response and work plan for a timely submission. She held daily stand-up meetings and collaborated with SRA and subcontractors to assure efficiency.

Company Name	DC Health Benefit Exchange
Project Name	DC Health Benefit Exchange
Timeline	July 2013 – December 2013
Position Title	IT Specialist – Health Insurance Exchanges

Ms. Mauldin supported the following projects during her employment:

- **IAPD-Update for Medicaid Eligibility & Enrollment** - Ms. Mauldin completed the documentation requirements to support the IAPD-Update for Medical Eligibility & Enrollment request for additional funding based on revised scope. Ms. Mauldin gathered requirements, wrote justifications and provided cost estimates for Medical Eligibility for long-term care programs, DHS Service Center Expansion, DHS Service Center(s) business process assessment and remediation project, Data Conversion of Medicaid data for renewals in the system, and SalesForce CRM software licenses. She worked with the DHS budget administrator to complete an updated budget, and cost sharing distribution, based on state and federal grant funding. She completed all documentation requirements and MOU for submission of IAPD-U.
- **DC HIX Open-Enrollment Command Center** - Ms. Mauldin managed the Command Center for the Department of Human Services to support the launch of the District of Columbia's Health Insurance Exchange. She designed and implemented the DHS Command Center to centralize communications between HIX support teams and technical teams to insure the prompt triage resolution of HIX website issues during open enrollment. She participated in the deployment and launch of the DC HIX website and transition from development to operation and maintenance in compliance with statutory requirements, SLAs, and contract agreement.

Company Name	Hawaii Health Connector
Project Name	Hawaii Health Connector
Timeline	July 2012 – October 2013
Position Title	IT Specialist & Contact Center Director

Ms. Mauldin provided technical expertise to establish a State-based Exchange with a $190M budget. She led a special team to complete the Level 2 grant application, using best practices and lessons learned, for HHS submission, under a tight timeframe. She authored three RFPs and documented the HIX Blueprint, technical and security sections for HHS approval of Hawaii's State-base exchange. She developed a detailed procurement scoring method utilizing CMS Medicare/Medicaid protocols for executing HIX IT, Contact Center, and IV&V procurements.

Company Name	Center for Medicare and Medicaid Services (CMS)
Project Name	Various
Timeline	March 2009 – July 2012
Position Title	Various

Ms. Mauldin supported the following projects:

- **Health Insurance Exchanges – IT Project Manager** - Ms. Mauldin implemented health insurance exchanges and integrated Medicaid eligibility while serving as the CMS IT Project Manager for 14 states in the Great Lakes and Pacific Coast regions. She completed the IT cost reasonable assessment for state establishment grant applications, and provided input during budget discussions between states and CMS. She defined technical guidance to establish a common baseline and standards for the HIX blueprint and artifact requirements to support the stage gate review process. She

also provided technical direction and CMS approvals for state procurements, RFPs, contracts, technical documents and artifacts, and the stage gate review process.

- **Health Insurance Oversight System (HIOS) - Contracting Officer Representative** - Ms. Mauldin managed all aspects of the HIOS contract implementation, including scope, budget, schedule, communications, and deliverables while working closely with third-party CGI-Federal. Utilizing an Agile/Scrum methodology, she managed and released the first Affordable Health Care Act system, executing the base-year HIOS contract on-time and on-budget.
- **Web Chat Integration – Government Task Lead** - Ms. Mauldin designed Medicare's website chat feature to support internet-based beneficiary inquiries.

Education

Degree	• B.S. in Computer Science, Washington University

References

Company Name	Access Health CT
Contact Name	Edith Lortie
Address	By Request
Phone Number	860-839-5838
Email Address	edith.lortie@yahoo.com

Company Name	Hawaii Health Connector
Contact Name	Kevin Hause
Address	By Request
Phone Number	808-321-0102
Email Address	kevin@hawaiihealthconnector.com

Company Name	DC Health Link
Contact Name	Stephen Haines
Address	By Request
Phone Number	808-398-5669
Email Address	srh9807@gmail.com

Matthew J. Cullen

ACA/7 Standards Subject Matter Expert

Professional Experience

Mr. Cullen has worked in the healthcare industry for over 20 years. He is an expert in his field and understands the challenges with changing regulations and compliance requirements. He is able to identify, coordinate and implement state of the art information management systems tailored to public sector organization cultures. His experience includes both public and private sector healthcare program oversight and ranges from development of agency-specific solutions to creation of complex statewide systems. Mr. Cullen is a seasoned senior level industry expert and project manager with the ability to drive positive outcomes for our customers.

Relevant Experience

Company Name	First Data Government Solutions, LP
Project Name	Illinois Health Insurance Exchange
Timeline	June 2015– Present
Position Title	Project Manager

Mr. Cullen oversees a team of technical architects, web developers, mapping specialists, business analysts and financial analysts. The team has developed three SharePoint databases for use by consumers, internal staff and individuals working on behalf of GCI in the field (assisters and a help desk). He collaborates with GCI in the process development to be adhered to by staff to verify the protection of the data.

Company Name	First Data Government Solutions, LP
Project Name	Nebraska Eligibility and Enrollment Solution
Timeline	January 2014– June 2015
Position Title	IV&V Project Consultant

Mr. Cullen functioned as the IV&V consultant on a project to replace the legacy eligibility and enrollment environment with a SOA-compliant solution. As part of his responsibilities, he completed an assessment of the functional and non-function requirements and the system integrator's ability to meet these requirements for the client. Mr. Cullen participated in confirmation of requirements traceability, reviewing test plans, test scenarios and performance and stress testing. Mr. Cullen conducted attestation reviews of the state's existing eligibility environment's interfacing with the Federal Data Services Hub.

Company Name	First Data Government Solutions, LP
Project Name	Connecticut Health Insurance Exchange (HIX) IV&V Project
Timeline	April 2013 – November 2013
Position Title	IV&V Project Manager

As the engagement's project manager, Mr. Cullen was responsible for the development and execution of the IV&V project plan. Mr. Cullen managed a team of independent contractors that served as subject matter experts for the evaluation and technical solution testing. Mr. Cullen managed the IV&V Wave, Blueprint and End-to-End testing efforts and reporting all findings to the Exchange's Board of Directors and at the CMS Operational Readiness Review.

Company Name	First Data Government Solutions, LP
Project Name	Louisiana Medicaid Management Information System (MMIS) IV&V
Timeline	January 2012 – March 2013
Position Title	IV&V DDI Lead

As part of the IV&V team in Louisiana, Mr. Cullen functioned as the IV&V DDI Lead. He reviewed business and technical requirements, participated in requirement confirmation sessions, detail system design sessions, reviewed documentation and identified risks and mitigation strategies. Mr. Cullen focused on regulatory compliance, Affordable Care Act, and system conformance based upon the state's MITA Self-Assessment.

Company Name	First Data Government Solutions, LP
Project Name	Arkansas Health Benefit Exchange (HBE) Planning Project
Timeline	October 2011 – January 2012
Position Title	Health Benefits Exchange Subject Matter Expert

Mr. Cullen was responsible for development and confirmation of the business requirements necessary for the development of the Exchange. He facilitated sessions within the agency to develop the business processes for the Exchange operations. He conducted research in areas impacting plan certification as well as providing content for grant applications.

Company Name	First Data Government Solutions, LP
Project Name	Indiana MMIS Planning and Procurement
Timeline	January 2010 – September 2010
Position Title	Requirements Validation Project Lead

Mr. Cullen was responsible for development/oversight of the business and technical requirements for the MMIS replacement RFP. He established the processes and materials used to complete the requirement validation process and building quality assurance measures into the RFP.

Company Name	First Data Government Solutions, LP
Project Name	Ohio Medicaid Management Information System (MMIS) Replacement Business Transformation
Timeline	September 2009 – January 2010
Position Title	Organization Assessment/Gap Analysis Team

Mr. Cullen was part of the First Data Team responsible for the development of the organization assessment and gap analysis document. He facilitated information-gathering sessions, participated in business process review sessions and developed a survey tool used for interviewing other states regarding their past MMIS implementation efforts.

Company Name	First Data Government Solutions, LP
Project Name	North Dakota MMIS Replacement
Timeline	September 2007 – September 2009
Position Title	Independent Verification and Validation Project Lead

Mr. Cullen was responsible for developing the test strategy, test scenarios, and user acceptance testing oversight. In addition to his IV&V role, he served as a subject matter expert in the following areas: MMIS, HIPAA, and MITA. He completed a crosswalk between the user requirements, workflows and use cases and the CMS Certification Checklist.

Education

Degree	• MS, Health Services Management, Concordia University • Speech, National College of Education

References

Company Name	Accenture/Texas Medicaid & Healthcare Partnerships
Contact Name	Bradley Jackson
Address	12357-B Riata Trace Parkway, Austin, TX 78727
Phone Number	(512) 658-2432
Email Address	bradley.d.jackson@accenture.com

Company Name	North Highland Company
Contact Name	Timothy Walker
Address	3333 Piedmont Rd., Suite 1000, Atlanta, GA 30305
Phone Number	(303) 757-4660
Email Address	timothy.f.walker@northhighland.com

Company Name	Public Consulting Group
Contact Name	Lynda Douglas
Address	999 18th. Street, #1425N, Denver, CO 80202
Phone Number	(303) 601-1436
Email Address	ldouglas@pcgus.com

Kristie Abraham

Eligibility Certification Subject Matter Expert

Professional Experience

Ms. Abraham has 15 years of overall experience in Health and Human Service information systems technology experience. She brings twelve years' experience in business and systems analysis and system testing with experience in HHS data modeling. She has demonstrated success streamlining, optimizing, and maintaining system functionality and performance in highly sensitive government environments and an excellent capacity to work with executives and IT managers (state and vendors) to effectively prioritize activities, achieve defined IT objectives, and translate business requirements into IT secure solutions.

Relevant Experience

Company Name	First Data Government Solutions, LP
Project Name	New Mexico MMISR and CSE R PMO Project
Timeline	August 2015 – Current
Position Title	Senior Consultant / Eligibility and Enrollment SME

Ms. Abraham functions in a State Staff Augmentation role, working within the Medical Assistance Division. She reviews requirements for the Integrated Platform Services RFP and provides feedback. She reviewed the Statement of Work for the Integrated Platform Service RFP. She also reviewed the IV&V contract for potential vendors and provided feedback. Ms. Abraham is responsible for creating change orders to move the enrollment functionality into the eligibility system. She reviews any change orders or work requests for the eligibility system and assists with prioritizing the request. She is responsible for overseeing any new Medicaid functionality to the eligibility system and attends various meetings with stakeholders on the eligibility system and the MMISR project.

Company Name	First Data Government Solutions, LP
Project Name	Nebraska EES System IV&V Project
Timeline	October 2014 – June 2015
Position Title	IV&V Business Consultant

Ms. Abraham was responsible for providing Independent Validation and Verification of business processes and requirements for the Nebraska Eligibility and Enrollment System. She attended business process and reengineering sessions/functional requirement sessions, as well as communication and organizational change management meetings, and provided feedback and recommendations to the State and SI vendor. She reviewed the State's deliverables to CMS and provided recommendation through the deliverable review report. She also prepared First Data contractual deliverables and provided them to the State of Nebraska.

Company Name	Arkansas Department of Human Services
Project Name	Arkansas EEF system
Timeline	October 2012 –August 2014
Position Title	Program Manager

Ms. Abraham was responsible for the development and implementation of all DHS Division of County Operation eligibility systems. She managed a staff of five professionals in the implementation of the EEF system. She monitored the Arkansas EEF system performance and compliance with CMS and State requirements. She assisted with the development and implementation of various entities interfacing with the Arkansas EEF system. She served as liaison between Arkansas executive staff and IT contractors. She provided technical guidance and project management for IT and security solutions reporting directly to the DCO Director. She also served as the Information System Manager while the position was vacant.

Company Name	Arkansas Department of Human Services
Project Name	Various
Timeline	October 2009 – September 2012
Position Title	Information System Coordinator

Ms. Abraham reported to the Director of DHS DCO, leading the development and testing of all DHS DCO eligibility systems and application. She coordinated the development and implementation of the eligibility systems and programs. She reviewed system changes, policies and procedures to define system needs. She analyzed the system to evaluate current and future development of system applications. Ms. Abraham served as a subject matter expert for testing all system applications. She developed system test documents for enhancements and changes.

During her employment, Ms. Abraham implemented the citizen online application portal for Medicaid, TANF, and SNAP (Access Arkansas) to streamline the application process for clients. She also implemented the interface for electronic case records (Docushare system) to eliminate the need for paper case files in the county offices, saving time on record retrieval and transferring of paper records to follow clients who relocated. The caseworker interface (AAMI) from Access Arkansas Citizen Portal was also implemented, in order to transform the manual process of caseworkers keying application data from Access Arkansas system into the ANSWER system into a worker interface with data validation and rules that saved county field staff many hours of data entry and improved data quality.

Company Name	Arkansas Department of Human Services
Project Name	Various
Timeline	November 2000 – September 2009
Position Title	Program Coordinator

Ms. Abraham was responsible for leading the development and implementation of DCO eligibility systems and interfaces to other entities. She performed gap and risk analysis of the existing system and evaluated benefits of the new system. She prepared business requirements documents and collected functional requirements, and prioritized business and system problems, analyzed legislation and conducted impact analysis. Ms. Abraham developed system test plans and system test documents. She performed system functionality and regression testing. She also monitored system functionality, by updating system tables, performing queries, and monitoring the system defects and proposing solutions.

Education

Degree	• B.A. in Psychology, Henderson State University

References

Company Name	Arkansas Department of Human Services
Contact Name	Brenda Butler
Address	700 Main Street Little Rock, AR 72201
Phone Number	501-682-1518
Email Address	Brenda.f.butler@arkansas.gov

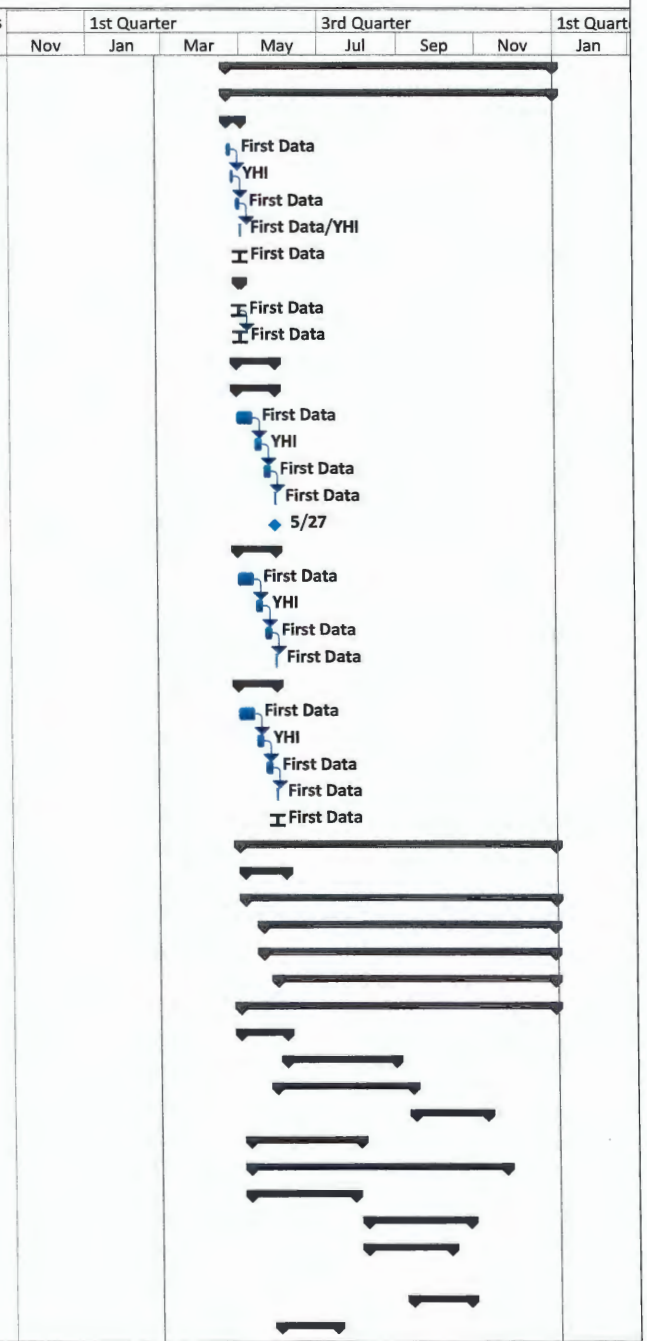
Company Name	New Mexico Department of Human Services
Contact Name	Russell Toal
Address	2055 S. Pacheco Street-South Park, Suite 500 Santa Fe, NM 87504
Phone Number	505-827-3114
Email Address	Russell.toal@state.nm.us

Company Name	Arkansas Department of Health
Contact Name	Pamela Henry
Address	4501 West Markham, Slot 17 Little Rock, AR 72205
Phone Number	501-280-4799
Email Address	Pamela.henry@arkansas.gov

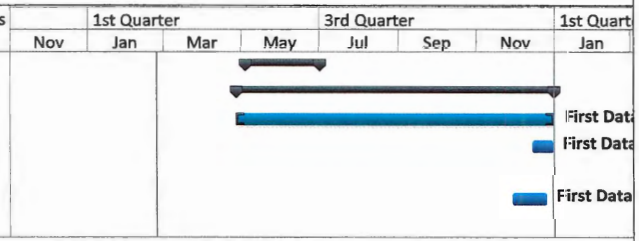
Appendix 3

Idaho IV&V HIX

ID	WBS	Task Name	Duration	Start	Finish	Predecess	Resource Names
1	1	**YHI IV&V Project**	**177 days**	**Mon 4/21/14**	**Wed 12/31/14**		
2	1.1	**Project Planning and Administration**	**177 days**	**Mon 4/21/14**	**Wed 12/31/14**		
3	1.1.1	**Project Initiation**	**9 days**	**Mon 4/21/14**	**Thu 5/1/14**		
4	1.1.1.1	Meet client, discuss requirements	3 days	Mon 4/21/14	Wed 4/23/14		First Data
5	1.1.1.2	YHI reviews and provides comments	2 days	Thu 4/24/14	Fri 4/25/14	4	YHI
6	1.1.1.3	IV&V Vendor incorporates YHI Comments	3 days	Mon 4/28/14	Wed 4/30/14	5	First Data
7	1.1.1.4	Conduct Project Kick-Off Meeting	1 day	Thu 5/1/14	Thu 5/1/14	6	First Data/YHI
8	1.1.1.5	**Milestone: Project Kick-Off Meeting Completed**	**1 day**	**Thu 5/1/14**	**Thu 5/1/14**		First Data
9	1.1.2	**Project IVV Artifact Repository**	**2 days**	**Wed 4/30/14**	**Thu 5/1/14**		
10	1.1.2.1	Develop Project IVV Artifact Repository (Share Point Site)	1 day	Wed 4/30/14	Wed 4/30/14		First Data
11	1.1.2.2	Provide Access to YHI to Share Point Site	1 day	Thu 5/1/14	Thu 5/1/14	10	First Data
12	1.1.3	**Project Planning**	**21 days**	**Mon 4/28/14**	**Tue 5/27/14**		
13	1.1.3.1	**IV&V Management Plan**	**21 days**	**Mon 4/28/14**	**Tue 5/27/14**		
14	1.1.3.1.1	Develop IV&V Management Plan	10 days	Mon 4/28/14	Fri 5/9/14		First Data
15	1.1.3.1.2	State reviews and provides comments	5 days	Mon 5/12/14	Fri 5/16/14	14	YHI
16	1.1.3.1.3	IV&V Vendor incorporates YHI Comments	5 days	Mon 5/19/14	Fri 5/23/14	15	First Data
17	1.1.3.1.4	Final Management Plan delivered to the YHI	1 day	Tue 5/27/14	Tue 5/27/14	16	First Data
18	1.1.3.1.5	**Milestone: IV&V Management Plan Complete**	**0 days**	**Tue 5/27/14**	**Tue 5/27/14**		**First Data**
19	1.1.3.2	**IV&V Work Plan**	**21 days**	**Mon 4/28/14**	**Tue 5/27/14**		
20	1.1.3.2.1	Develop IV&V Work Plan	10 days	Mon 4/28/14	Fri 5/9/14		First Data
21	1.1.3.2.2	YHI reviews and provides comments	5 days	Mon 5/12/14	Fri 5/16/14	20	YHI
22	1.1.3.2.3	IV&V Vendor incorporates YHI Comments	5 days	Mon 5/19/14	Fri 5/23/14	21	First Data
23	1.1.3.2.4	Final Work Plan delivered to the YHI	1 day	Tue 5/27/14	Tue 5/27/14	22	First Data
24	1.1.3.3	**IV&V Review Checklists**	**21 days**	**Mon 4/28/14**	**Tue 5/27/14**		
25	1.1.3.3.1	Develop IV&V Review Checklists	10 days	Mon 4/28/14	Fri 5/9/14		First Data
26	1.1.3.3.2	YHI reviews and provides comments	5 days	Mon 5/12/14	Fri 5/16/14	25	YHI
27	1.1.3.3.3	IV&V Vendor incorporates YHI Comments	5 days	Mon 5/19/14	Fri 5/23/14	26	First Data
28	1.1.3.3.4	Final Review Checklists delivered to the YHI	1 day	Tue 5/27/14	Tue 5/27/14	27	First Data
29	1.1.3.3.5	**Milestone: IV&V Review Checklist Completed**	**1 day**	**Tue 5/27/14**	**Tue 5/27/14**		First Data
30	1.1.4	**Project Execution, Monitoring and Controlling**	**171 days**	**Mon 4/28/14**	**Tue 12/30/14**		
31	1.1.4.1	**Initial IV&V Review**	**21 days**	**Fri 5/2/14**	**Mon 6/2/14**		
41	1.1.4.2	**Weekly IV&V Review Reports**	**167 days**	**Fri 5/2/14**	**Tue 12/30/14**		
76	1.1.4.3	**Monthly IV&V Review Reports**	**156 days**	**Fri 5/16/14**	**Mon 12/29/14**		
85	1.1.4.4	**Monthly IV&V Status Reports**	**156 days**	**Fri 5/16/14**	**Mon 12/29/14**		
94	1.1.4.5	**Monthly Management Briefings (Per YHI Request)**	**150 days**	**Tue 5/27/14**	**Mon 12/29/14**		
103	1.1.4.6	**Project Management Assessment**	**170 days**	**Mon 4/28/14**	**Mon 12/29/14**		
148	1.1.4.7	**Requirements Validation Phase**	**25 days**	**Mon 4/28/14**	**Mon 6/2/14**		
176	1.1.4.8	**System Design Phase**	**60 days**	**Tue 6/3/14**	**Tue 8/26/14**		
210	1.1.4.9	**Technical Environment Assessment**	**73 days**	**Mon 5/26/14**	**Mon 9/8/14**		
242	1.1.4.10	**Operations Environment Assessment**	**40 days**	**Thu 9/11/14**	**Wed 11/5/14**		
280	1.1.4.11	**System Development**	**60 days**	**Mon 5/5/14**	**Tue 7/29/14**		
291	1.1.4.12	**Testing**	**140 days**	**Mon 5/5/14**	**Thu 11/20/14**		
309	1.1.4.13	**Pre-Operational Readiness Review (PORR)**	**57 days**	**Mon 5/5/14**	**Thu 7/24/14**		
316	1.1.4.14	**Operational Readiness Review (ORR)**	**57 days**	**Mon 8/4/14**	**Wed 10/22/14**		
323	1.1.4.15	**Privacy and Security Pre-Implementation Assessment Report**	**46 days**	**Mon 8/4/14**	**Tue 10/7/14**		
329	1.1.4.16	**Implementation Phase**	**33 days**	**Mon 9/8/14**	**Wed 10/22/14**		
343	1.1.4.17	**Corrective Action Plan (Per YHI Request)**	**31 days**	**Tue 5/27/14**	**Wed 7/9/14**		



ID	WBS	Task Name	Duration	Start	Finish	Predecess	Resource Names
352	**1.1.4.18**	**Deliverable Observation Reports (Per YHI Request)**	**41 days**	**Mon 5/5/14**	**Tue 7/1/14**		
360	**1.1.5**	**Project Closeout**	**172 days**	**Mon 4/28/14**	**Wed 12/31/14**		
361	1.1.5.1	Archive IV&V documents	172 days	Mon 4/28/14	Wed 12/31/14		First Data
362	1.1.5.2	Provide Assessment of all documentation and processes for system acceptance	11 days	Mon 12/15/14	Tue 12/30/14	349FS-1(days	First Data
363	1.1.5.3	Deliver final report of IV&V tasks, activities, findings, lessons learned, and outstanding technical issues/risks	19 days	Mon 12/1/14	Fri 12/26/14	349FS-1(days	First Data



Appendix 4

Office of Systems Integration
"SERVING CALIFORNIA"

CalHEERS R16.2 Release Performance Report

- Release Performance Metrics
- Recommendations & Improvement Tracking

Office of Systems Integration – CalHEERS Quality Assurance Section

April 14, 2016

Version 1.10

Report Structure

R16.2 Release Performance Report is organized into 4 main sections:

1. Summary *Slide 4*
   Overview, achievements and challenges

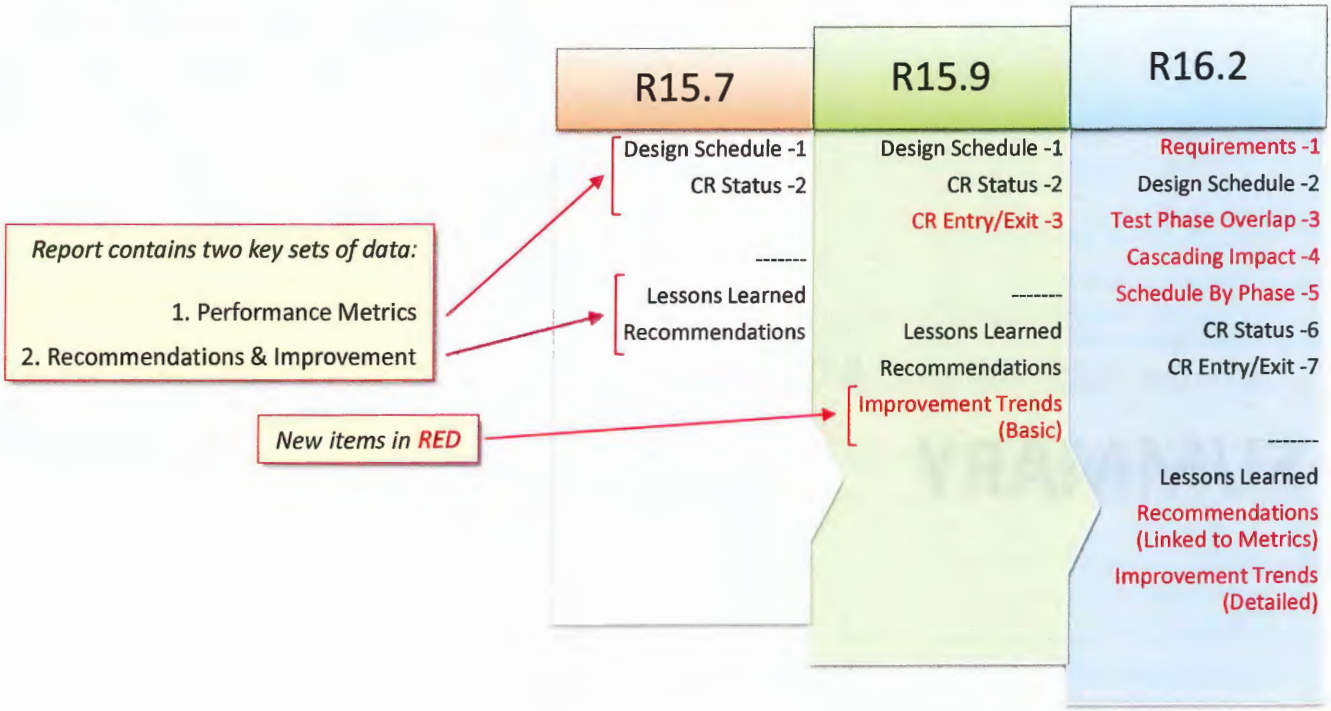
2. Requirements & Design *Slide 8*
   Impact of early phase activities on overall release performance, and future releases

3. Release Portfolio Metrics *Slide 17*
   CR status throughout the release lifecycle

4. Improvement Tracking *Slide 23*
   Lessons learned and recommendations for process improvement

Report Evolution

- **CalHEERS Release Performance Report** began with R15.7.
- Metrics, analysis, and recommendations continue to increase in sophistication.
- Report utilized for **external communication** and **internal optimization strategy**.



Overview, Achievements & Challenges

SUMMARY

Overview

- Overall, R16.2 performance followed a similar pattern as R15.9
  - CR requirements and functional designs changed throughout the release
  - Early schedule slippage caused substantial overlap between work phases, including ongoing Requirements, Design and Build during the Test activity.

- A Release Planning Summit improved the definition of R16.2 scope
  - CRs introduced prior to the functional design approval deadline increased from 32% during R15.9 to 73% during R16.2
  - The total number of active CRs was more consistent throughout the R16.2 lifecycle compared to earlier releases

- Challenges in meeting schedule milestones and successfully implementing the full scope of R16.2 at Go-Live were similar to prior releases
  - Early phase (Design & Build) schedule slippage
    - 64% (7 out of 11) of CRs that were successfully implemented at Go-Live experienced significant schedule slip during Design and/or Build phases.
  - Completion
    - 50% of CRs attempted were successfully implemented at Go-Live (11 implemented of the 22 attempted).

Achievements

- The project team instituted several notable changes during the R16.2 delivery cycle to improve its outcomes
  - Improvements to Weekly Director's Report, including:
    - More consistent criteria for determining CR status
    - Improved defect tracking, reporting, and mitigation plan
    - New release master work plan (MS Project schedule)
  - Refined 24-Month Roadmap
  - R16.2 scope (number of active CRs) was more consistent throughout release
  - R16.2 was first to launch with a Release Planning Summit
  - Focus on improving timeliness of requirements submission from the Sponsors
  - Focus on improving Change Evaluation Team (CET) to ensure qualified requirements prior to Change Control Board (CCB) approval
  - Improved communication and timing for Go/No-Go reporting
  - Increased measurement of release performance

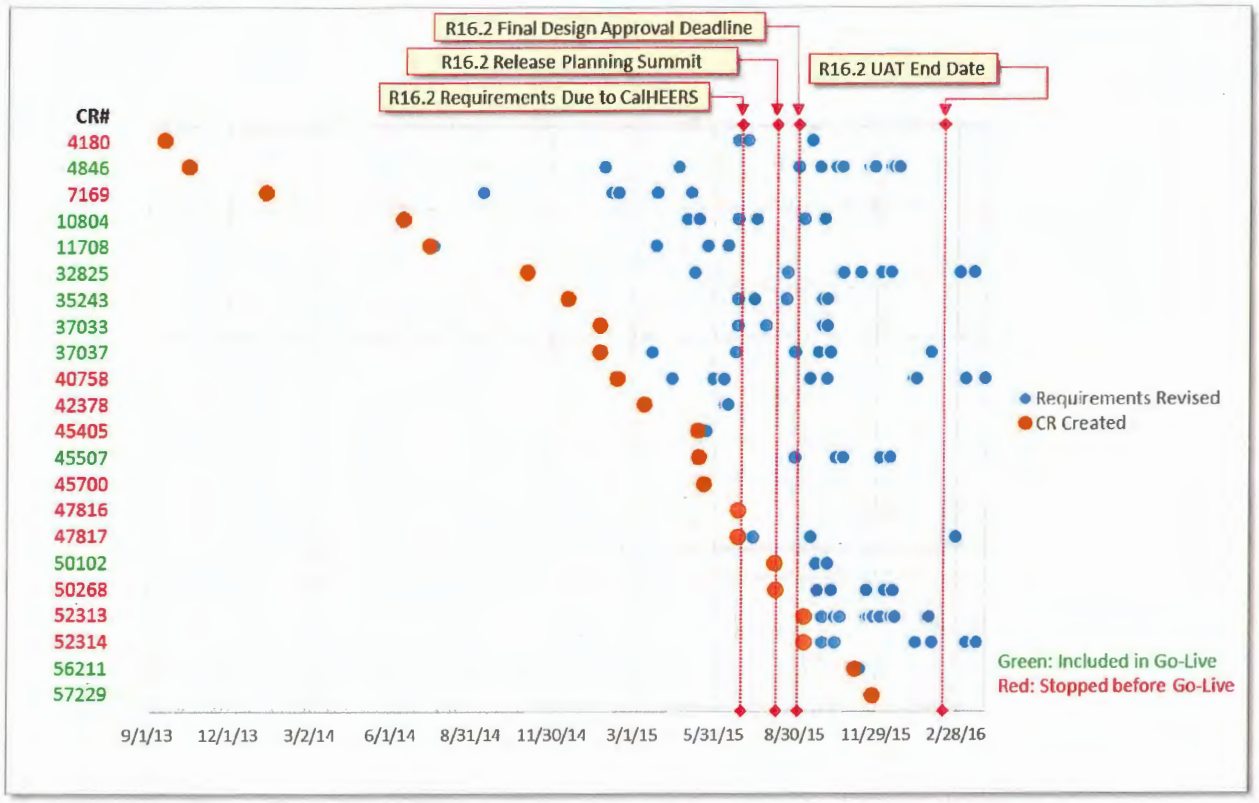
Challenges

- Several aspects of the project continue to deserve attention to reach optimal effectiveness
  - Significant effort was focused on improving CR initiation and scope planning for R16.2 but requirements and designs continued to change through the entire release lifecycle
  - In November 2015, the CalHEERS Project Steering Committee approved an extension of the R16.2 Integration Test schedule and a two-week delay for Go-Live, in part to avoid risks associated with overlapping System Test and Integration Test
    - Despite the time added, schedule slippages in Requirements, Design, and Build stages extended the System Test timeframe putting it in parallel with Integration Test and UAT activities
  - As observed in prior releases, missed milestone dates at the start of the 16.2 release schedule had downstream impacts to subsequent development phases and later releases
  - R16.2 design activity spanned across all 2016 release design phases: R16.4, R16.7, and R16.9
  - Eight (8) of the CRs addressed during R16.2 were carried over from R15.9, further demonstrating a need for design, development, and testing time beyond that originally planned

Setting The Pace For A Release

REQUIREMENTS & DESIGN

CR Design: R16.2 Requirement Revisions Timeline



CR requirements were updated continuously through the design, build, and test periods, impacting the quality and timeliness of R16.2.

CR Design: R16.2 Requirement Revisions Timeline

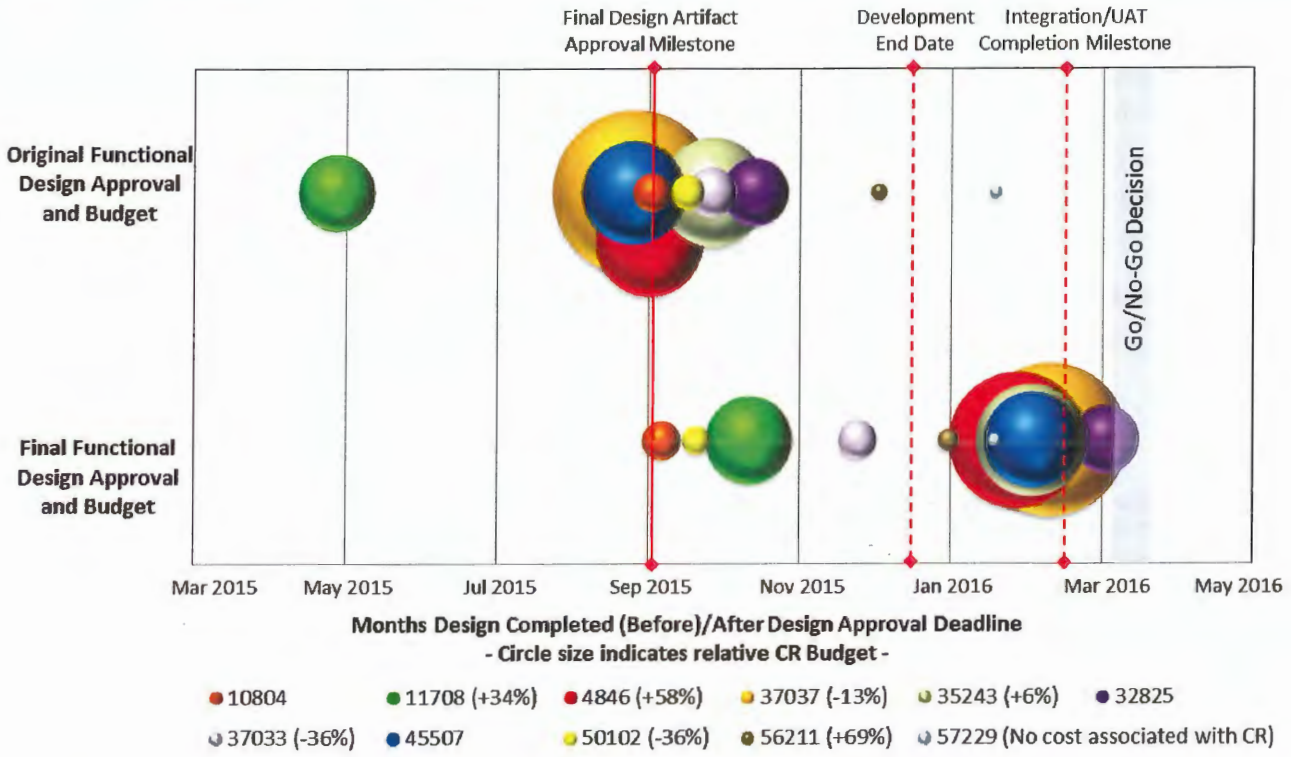
Observations

- CR requirements were updated throughout the entire release lifecycle.
- Most requirement updates occurred parallel to the design effort suggesting "discovery" was prompted by detailed design efforts.
- Even though CRs were often created well in advance, requirements updates continued after the scheduled Final Design Approval Deadline.
- As observed in prior releases, splitting CR functionality across multiple releases may result in significant increases to cost and scope, as well as cause duplicated effort and time spent in delivery (e.g., Build and Test phases).

Recommendations / Improvements

- If the project team elects to follow a sequential scheduling method (e.g., "waterfall") the scope and requirements for all CRs should be clearly and completely defined before the first planning milestone date to avoid delays and cost overruns.
- If the project team and sponsors need detailed designs to fully understand the associated business requirements, a more iterative development method may be beneficial and should be weighed for corresponding trade-offs.
- CRs should not be split over multiple releases unless cost implications are well understood and approved.

CR Design: R16.2 Schedule Performance



Similar to the performance in prior releases, CR designs in R16.2 continued to evolve well beyond the established milestone dates.

CR Design: R16.2 Schedule Performance

Observations

- Functional design changes for many CRs continued throughout – or even after – the scheduled completion of Build, System Test, Integration Test, and User Acceptance Testing.
- Although four CR designs were initially approved on time, none of the functional designs were finalized until after the scheduled Design Approval Deadline.
- The majority of CR designs were finalized within 30 days of Go-Live.
- The pattern of late design completion is similar between R15.7, R15.9 and R16.2.
- This pattern of late design completion appears to be continuing in future releases R16.4, R16.7 and R16.9.

Recommendations / Improvements

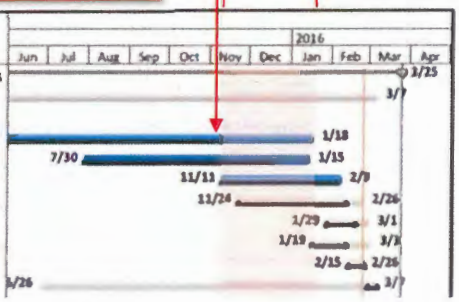
- Associate the time allowed for completing CRs with expectations of the volume and quality of work to be delivered in a release.
- The project team should strive to create CR schedules based on the scale and complexity of the scope, or limit the number of CRs included in a release to allow sufficient numbers of resources to complete all stages of work on time.
  - For exceptionally large or complex CRs, the team should create a design/build/test schedule based on the full CR scope, even if it necessitates targeting a finish date in the more distant future.
- The project team and sponsors should manage performance against interim milestone dates to help ensure steady progress towards go-live dates.
  - Missed dates early in the release lifecycle (e.g., requirements and design complete) should be considered more critically as cause for rescheduling a CR's release.

CR Design: R16.2 Test Phase Overlap

Design Complete Actual
(Overlap ST and IT)

Design Complete Target
(Finish Before ST)

% Compl	Task Name	Duration	Start	Finish	Baseline Start	Baseline Finish	Finish Variance
98%	Release 16.2 Master Work Plan	381 days	10/10/14	3/25/16	6/18/15	2/26/16	20 days
99%	Release 16.2 Master Work Plan	367 days	10/10/14	3/7/16	NA	NA	0 days
0%	Release R16.2 Level Milestones	278 days	2/12/15	3/7/16	2/12/15	NA	0 days
100%	Release 16.2 (Milestone) Design	243 days	2/12/15	1/18/16	2/12/15	11/9/15	50 days
100%	Release 16.2 (Milestone) Build	122 days	7/30/15	1/15/16	7/30/15	12/18/15	20 days
100%	Release 16.2 (Milestone) System Test	65 days	11/11/15	2/9/16	11/11/15	2/5/16	2 days
	Release 16.2 (Milestone) Integration Test	69 days	11/24/15	2/26/16	11/24/15	2/12/16	10 days
	Release 16.2 (Milestone) Performance/Security Test	23 days	1/29/16	3/1/16	1/29/16	2/19/16	7 days
[illegible]	Release 16.2 (Milestone) UAT Test	33 days	1/19/16	3/3/16	1/18/16	2/12/16	14 days
0%	Release 16.2 (Milestone) Regression Test	10 days	2/15/16	2/26/16	2/15/16	2/26/16	0 days
0%	Release 16.2 (Milestone) Implementation Readiness	181.13 days	6/26/15	3/7/16	3/1/16	3/7/16	0 days



Source: Operational Release Work Plan, excerpted from Weekly Director's Report 2/29/2016

Ongoing design changes extended the System Test timeframe, offsetting the intended benefits of extending the R16.2 Integration Test schedule.

CR Design: R16.2 Test Phase Overlap

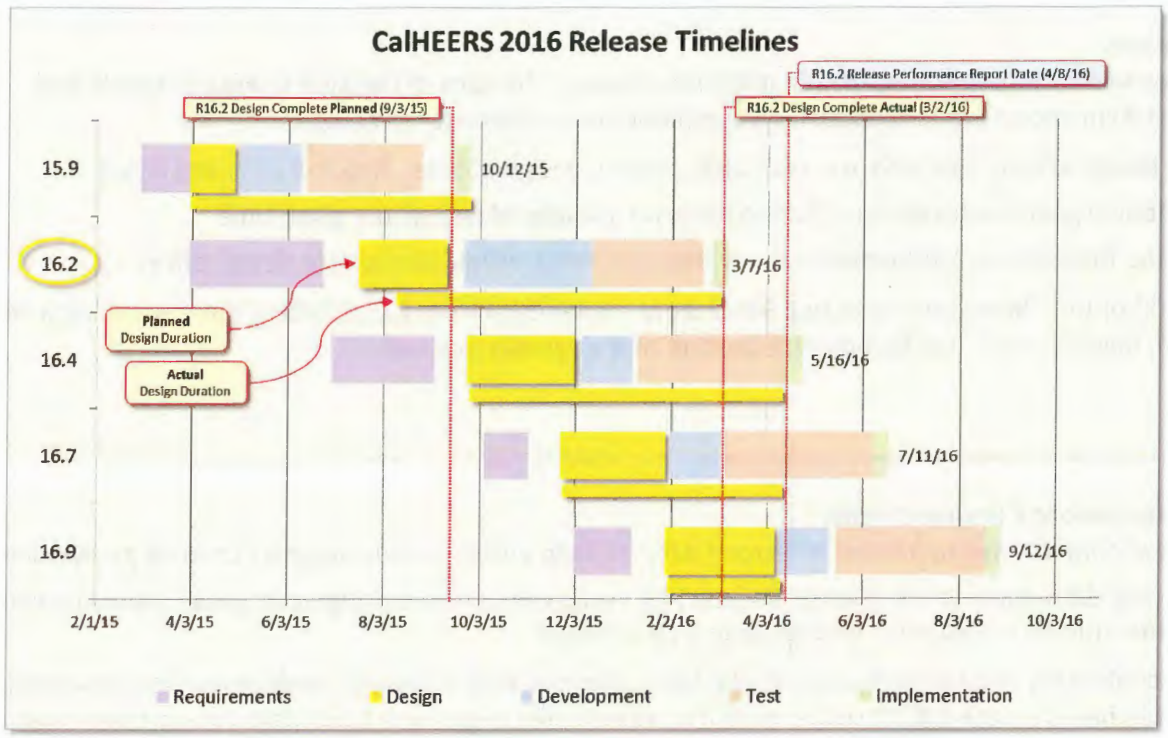
Observations

- In November 2015, the CalHEERS Project Steering Committee approved an extension of the R16.2 Integration Test schedule and a two-week delay for Go-Live, in part to avoid quality and timeliness risks associated with overlapping System Test and Integration Test.
- Despite the time added, schedule slippages in Requirements, Design, and Build stages extended the System Test timeframe putting it in parallel with Integration Test and UAT activities.
- Some CR Design Complete/Acceptance dates extended as far as 3/2/2016 – five days prior to Go-Live and later than the planned end of all testing cycles.

Recommendations / Improvements

- Under a sequential schedule approach, the project team will need to complete early requirements and design work with greater accuracy, thoroughness, and timeliness to increase the likelihood of achieving build and test phases on time and with the full scope intended.
  - If early schedule milestones are missed or work is not sufficiently complete when needed, the project team could consider an early termination/rescheduling of affected CRs rather than jeopardizing the timeliness and quality of the release by continuing to expend resources on delayed CRs throughout the build and test phases.

CR Design: 2016 Cascading Schedule Impact



Similar to the effects noted from prior releases, ongoing CR design efforts through the entire R16.2 lifecycle impacted the schedules of future releases.

CR Design: 2016 Cascading Schedule Impact

Observations

- As observed in prior releases, missed milestone dates at the start of the 16.2 release schedule had downstream impacts to subsequent development phases and later releases.
- R16.2 design activity spanned across all 2016 release design phases: R16.4, R16.7, and R16.9
  - Schedule goal was for design effort to focus on a single release at any given time
  - At the time of R16.2 implementation, a total of 4 releases had concurrent design effort
- Eight (8) of the CRs addressed during R16.2 were carried over from R15.9 further demonstrating a need for design, development, and testing time beyond that originally planned.

Recommendations / Improvements

- Teams should manage to interim milestone dates to help ensure steady progress towards go-live dates.
  - Missed dates early in the release lifecycle (e.g., requirements and design complete) should be considered more critically as cause for rescheduling a CR's release
- For exceptionally large or complex CRs, the team should create a design/development/implementation schedule based on the full CR scope, even if it necessitates targeting a finish date two or three releases away.

R16.2 CRs – Scope And Status

RELEASE PORTFOLIO METRICS

R16.2 Schedule Performance By Phase

		Finish Variance (Days)				
		Design	Build	ST	IT	UAT
	16.2 Release – Performance of CRs Remaining at Go-Live	**50**	**20**	**2**	**10**	**14**
CR #	**CR Description**					
4846	CCHIP Interface & integration into CalHEERS (Amend)	59	29	27	1	14
10804	Utilize the administrative verifications from SAWS at application intake in the first run to grant a full eligibility determination(Amend)	0	14	-2	0	14
11708	Do not display Non-MAGI screening and citizenship/immigration questions on the online application for household members not applying for health benefits (Amend)	0	19	-4	0	14
32825	Implementation of CalHEERS Functionality for E-mail/Electronic Notification to View Notice Securely Available in CalHEERS (Amend)	28	13	7	--	14
35243	Implementation of SB 1341 - Transfer Notice/NOA generation to the SAWS (Amend)	67	30	0	10	14
37033	Update the Business Rules Engine to calculate income using begin and end dates of each income source	7	21	5	0	14
37037	SAWS eHIT Interface: 4.0 updates	50	28	10	0	14
45507	Former Foster Youth (FFY) Phase II Page Flow & Schema Changes (CR 3066 - Phase II) (Amend)	28	19	1	10	14
50102	Implement Functionality for Discontinuance and Denial NOA	0	2	6	10	14
56211	Expand CalHEERS logic to support eligibility programs that are not prospective	0	7	8	--	14
57229	Remove usage of Arial Monotype fonts	1	0	0	--	14

Green (On time or ahead of schedule)
Yellow (1-14 days late)
Red (15 or more days late)

Source: Director's Report 2/29/2016

Although the project team improved performance against schedule over the course of R16.2, delays in the Design phase were not entirely offset.

R16.2 CR Status Over Time

CR #	8/17	8/24	8/31	9/8	9/14	9/21	9/28	10/5	10/12	10/19	10/26	11/2	11/9	11/16	11/23	11/30	12/7	12/14	1/4	1/11	1/19	1/25	2/1	2/8	2/16	2/22	2/29	Included in Final Release 16.2	
4180	U	U	U	G																								✗	
4846	U	U	U	G	G	G	G	G	G	G	G	Y	Y	Y	G	G	G	Y	Y	G	G	G	G	G	G	G	G	✓	Yes
7169										G	G	G	G	G	Y	Y	Y	G	G	G	G	G	G	G	G	G	G	✗	
10804	U	U	U	G	G	G	G	G	G	G	G	Y	Y	Y	G	G	G	G	G	G	G	G	G	G	G	G	G	✓	Yes
11708	U	Y	Y	G	G	G	G	G	G	G	G	Y	Y	Y	G	G	G	G	G	G	G	G	G	Y	G	G	G	✓	Yes
32825					Y	Y	Y	Y	Y	Y	Y	Y	Y	G	Y	Y	Y	Y	Y	Y	Y	Y	Y	G	Y	Y	G	✓	Yes
35243	U	U	U	G	G	Y	Y	Y	Y	Y	Y	Y	Y	Y	G	G	G	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	✓	Yes
37033	U	U	U	G	G	Y	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	Y	Y	Y	Y	✓	Yes
37037	U	U	U	Y	G	Y	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	Y	Y	Y	Y	✓	Yes
40758	U	U	U	G	Y	Y	Y	R																				✗	
42378										Y	Y	Y	Y	Y	Y	Y	Y	Y	G	G	G	G	G	G	G	G	G	✗	
45405	U																											✗	
45507	U	U	U	G	G	G	G	G	G	G	G	Y	Y	Y	G	G	G	G	G	G	G	G	G	Y	Y	Y	Y	✓	Yes
45700	U	U	U	Y	G																							✗	
47816	U																											✗	
47817	U	U	U	Y	Y	R	R	R	R	R	R	R	R	Y	R	R	R	Y	Y									✗	
50102	U	U	U	U	G	Y	G	G	G	G	G	Y	Y	Y	G	G	G	G	G	G	G	G	Y	Y	Y	Y	Y	✓	Yes
50268	U	U																										✗	
52313					Y	Y	Y																					✗	
52314					Y																							✗	
56211															Y	Y	Y	Y	G	G	G	G	G	G	G	G	G	✓	Yes
57229																		Y	Y	Y	Y	G	G	Y	G	G	G	✓	Yes

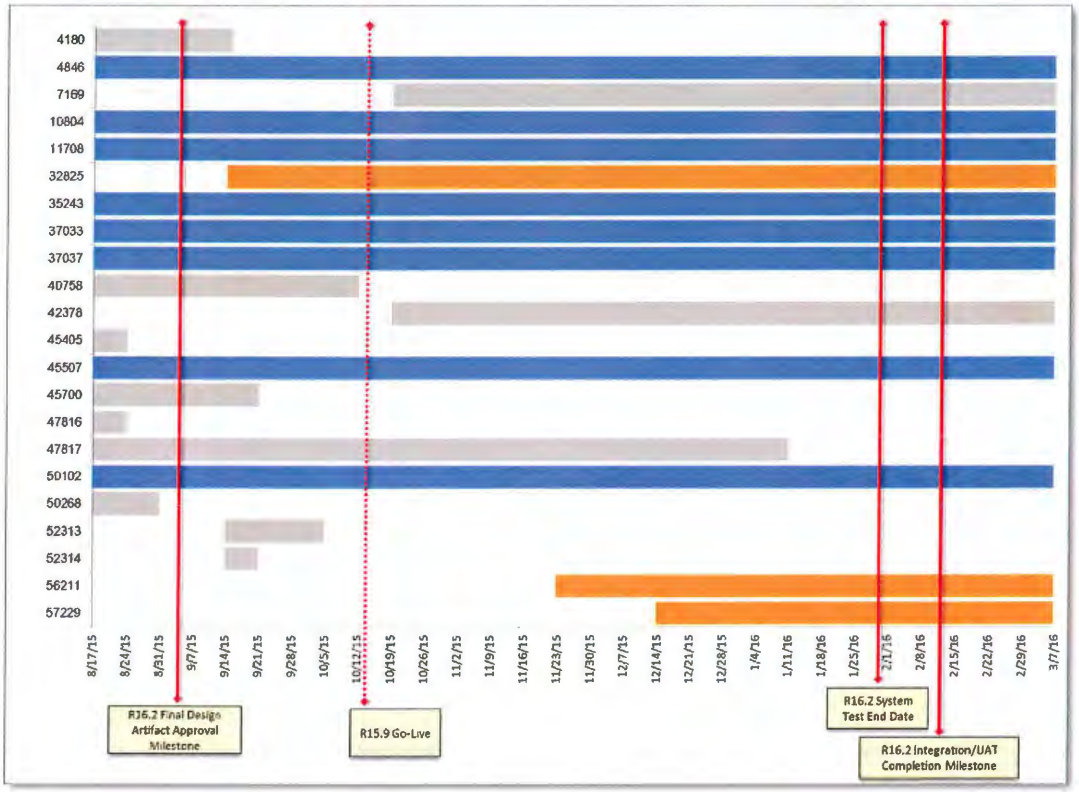
Legend: U – Unassigned; G – Green; Y – Yellow; R – Red

Source: CalHEERS Weekly Director Meeting Reports

Weekly reporting did not give a consistent indication of the likelihood individual CRs would be included in the Go-Live release.

- 2 of the 13 CRs slated for Go-Live failed to make the release despite consistent conditions of "Green" throughout testing and Go/No-Go reporting periods
- Conversely, 5 CRs reported in "Yellow" condition for the final four weeks were put into Production

R16.2 CR Entry / Exit Timelines



Blue: Start **PRIOR TO** design freeze (Go-Live)

Amber: Start **AFTER** design freeze (Go-Live)

Grey: **REMOVE** from release

R16.2 contained 1/3 the number of CRs of R15.9,
yet only 50% (11 of 22) were included in the release at Go-Live.

Descriptions of CRs Included in Final Release 16.2

CR #	CR Description
4846	CCHIP Interface & Integration into CalHEERS (Amend)
10804	Utilize the administrative verifications from SAWS at application intake in the first run to grant a full eligibility determination(Amend)
11708	Do not display Non-MAGI screening and citizenship/immigration questions on the online application for household members not applying for health benefits (Amend)
32825	Implementation of CalHEERS functionality for E-mail/Electronic Notification to View Notice Securely Available in CalHEERS (Amend)
35243	Implementation of SB 1341 - Transfer Notice/NOA generation to the SAWS (Amend)
37033	Update the Business Rules Engine to calculate income using begin and end dates of each income source
37037	SAWS eHIT Interface: 4.0 updates
45507	Former Foster Youth (FFY) Phase II Page Flow & Schema Changes (CR 3066 - Phase II) (Amend)
50102	Implement functionality for Discontinuance and Denial NOA
56211	Expand CalHEERS logic to support eligibility programs that are not prospective
57229	Remove usage of Arial Monotype fonts

Descriptions of CRs Removed From Release 16.2

CR #	CR Description
4180	Begin Date and End Date on eHIT Data Elements
7169	Expedited/Flexible Application Entry for SCRs - (Amend)
40758	Projected Annual Income (PAI) Logic Updates (Amend)
42378	EDR-C Mitigation of Near Consecutive Eligibility Determination Request submissions (Amend)
45405	Add a secondary SFTP drop location for the bi-directional exchange of non-X12 (834) files
45700	New NACK Response Code (HX005005) for IRS files EOM H36 and EOY H41
47816	Medi-Cal Access Program Integration (AB 1296) Phase II
47817	2016 FPL Table Update
50268	2015 1095 Federally Mandated Changes (Amend)
52313	Dup App Quick Wins-Prevent multiple/duplicate accounts, applications and cases in CalHEERS and additional enhances to support preventing duplicates
52314	Dup App – Long Term CR - Noticing Consumers for closed accounts/cases and Delinking and Relinking SAWS Cases from CalHEERS Cases via eHIT

Lessons Learned And Recommendations For Process Improvement

IMPROVEMENT TRACKING

Recommendations & Improvement Tracking

- The following pages summarize Lessons Learned and Recommendations for Improvement identified by the CalHEERS Project Team, Sponsors, and Partners.
  - Lessons Learned was originally conducted in R15.7.
  - Improvement trends for R15.9 and R16.2 are listed in the following table, along with improvement activity descriptions for R16.2.

- Recommendations are categorized as follows:
  1. **Product Quality**: Recommendations for improving the quality of CalHEERS enhancements
  2. **Vision and Collaboration**: Recommendations for ensuring common expectations for release outcomes
  3. **Scope Delivery**: Recommendations to improve delivery of approved CalHEERS enhancements
  4. **Budget and Efficiency**: Recommendations to reduce cost of service and scope delivery

Improvement Tracking

Product Quality

#	15.7 Lessons Learned	15.7 Recommendation	Improvement		16.2 Improvement Description
			15.9	16.2	
Product Quality					
1	Early missed release and CR schedule milestones have downstream impacts to other development phases.	- Improve capacity management to alleviate overloading releases with CRs. - Associate the time allowed for completing CRs with expectations of the volume and quality of work to be delivered in a release.	↑	↑	In conjunction with the Release Planning Summit approach, Accenture instituted a model for gauging the team's capacity to support various categories of functional changes. Continuing improvements to requirements development, cost estimating, and change management will help reduce volatility during the release development lifecycle. In turn, such improvements should result in better resource management.
2	Defect correction priorities in release 15.7 were inconsistent between project teams and the business, e.g.: - Defects were primarily fixed late in the release cycle limiting test time. - Business priorities for defect correction were provided late in the development cycle.	Standardize and clarify the business and development teams' priorities for CR functionality and defect correction early in release planning.	↑	↑	Improvement: Defect tracking and prioritization was a major focus for 16.2. Improvements include additional charts and tables added to the weekly Director's Report and weekly review of defect status. Opportunity for continuing improvement: CR7169 has been attempted in Releases 15.7, 15.9 and 16.2 but has not been successfully put into production. This has caused the project team, sponsors, and integration partners to repeat testing and defect fixing activities for the same CR mulitple times. Further work is needed to improve the timing of defect identification and closure before the release date, particularly in functional areas involving integration partners.

Improvement Tracking

Product Quality

#	15.7 Lessons Learned	15.7 Recommendation	Improvement		16.2 Improvement Description
			15.9	16.2	
Product Quality					
3	Due to the schedule compression in 15.7, many System Test, Integration Test, and UAT activities occurred in parallel reducing efficacy and coverage.	Leave sufficient time for the intended progression of test cycles to ensure adequate quality is confirmed before release go-live.	↓	↑	*Improvement:* Beginning with 16.2, the modified release schedule provides additional time for sequential test phases. Additionally, the schedule was adjusted to accommodate a longer period for SAWS integration testing. *Opportunity for continuing improvement:* During the course of 16.2, the sponsors and partners agreed to delay the release date to 3/7 to allow more time for testing. Despite the extension, late changes, additional development, integration test delays, and ongoing defect corrections resulted in concurrent System Test, Integration Test, and User Acceptance Test activities.

Improvement Tracking

Vision & Collaboration

#	15.7 Lessons Learned	15.7 Recommendation	Improvement 15.9	Improvement 16.2	16.2 Improvement Description
Vision & Collaboration					
4	CR scope and requirements should be clearly and completely defined upfront to avoid delays and cost overruns.	- Engage sponsors to fully define scope at CR initiation. - Document the Sponsor executive management's expectations for each CR. - Collaborate with the Sponsors to describe and confirm complete requirements.	↑	↑	Early CR scope definition and understanding of sponsor executives' expectations improved via the new Release Planning Summit and improved JAD participation.
5	The intention of the Sponsor executive management may not be well understood by the project or the sponsor BAs. This can lead to additional requirements and scope increases that are not aligned to the wishes of the executives.	Implement processes to: - Obtain Sponsor executive management expectations early in CR planning - Communicate expectations to JAD SMEs Manage to the Sponsor's expectations during JAD sessions.	↑	↑	Requirements definition improved as a result of the new Release Planning Summit and improved JAD participation. Sponsor executives have typically attended the Release Planning Summits, aiding the collective understanding of needs and expectations. In addition, key executives have remained more closely involved with the evolution of release development in recent months through venues such as the PSC and PCC.
6	Communication and information sharing on release status to all stakeholders needs improvement to manage expectations and avoid late surprises.	- Share release readiness progress with Sponsors throughout the release lifecycle to avoid surprises and deliver to expectations. - Define, document and manage to go/no-go criteria throughout the release lifecycle.	↑	↑	Several modes of communication between CalHEERS and Sponsors/Stakeholders have been enhanced, including the Release Planning Summit, participation in JADs, membership in the PSC and PCC, participation in weekly Director's Meetings, and more robust Release Planning and Go/No-Go meetings.

Improvement Tracking

Vision & Collaboration

#	15.7 Lessons Learned	15.7 Recommendation	Improvement		16.2 Improvement Description
			15.9	16.2	
Vision & Collaboration					
7	The two-step Go/No-Go process worked well for 15.7.	- Retain the Go/No-Go meeting. - Refine communication of impacts expected from incomplete work or outstanding defects.	↑	↑	The Go/No-Go status reporting and sponsor meeting format has been effective for the last two releases. The project team should maintain and continue to refine this format for future releases.
8	Decisions made outside of formal committees can appear to be: - Communicated inconsistently - Based on unknown criteria - Made without appropriate input	- Utilize a formal decision-recording process including decision requests, inventory, and communication. - Reinforce the use of Decision Logs including confirming stakeholder access.	↑	↑	The project team routinely records key decisions in a central log accessible by most participants. Communication has been enhanced in recent releases through increased participation by dedicated representatives from the sponsor and partner organizations. Improvements in meeting management (agendas, notes), consistent participation, and lines of reporting have also helped improve communication effectiveness.

Improvement Tracking

Scope Delivery

#	15.7 Lessons Learned	15.7 Recommendation	Improvement 15.9	Improvement 16.2	16.2 Improvement Description
Scope Delivery					
9	CR Impact Assessments are not performed consistently which can lead to unexpected impacts late in the CR lifecycle.	Define expectations and criteria for State and Accenture to follow when completing Impact Assessments.	↑	↑	The State and Accenture teams expanded and refined the criteria that are to be used for performing impact assessments. While these standards may help improve the sponsors' and project team's understanding of CRs, their effectiveness will depend on continued diligence by the State and Accenture to complete the evaluations thoroughly, accurately, and consistently.
10	Milestone dates may be missed when they are based on the release schedule rather than the work needed for individual CRs.	Create CR schedules based on scope and manage to realistic milestones within the release schedule.	→	↑	The overall schedule for R16.2 was intentionally extended early in the design and planning stage when it was determined that the contents of the release warranted more time for integration testing with partners. The CalHEERS team and its partners were able to identify the additional time needs early in the development lifecycle due, in part, to a clear definition of scope and the completion of necessary work according to early milestones. The team should continue to plan the scope of future releases based resource capacity and the time available between the Planning Summits and respective go-live dates.
11	The delays incurred during the Design phases were not well communicated to Release Management which resulted in planning challenges for downstream impacts.	Release Management tracking should begin before Approved for Implementation in order to track the planning and design activities.	↑	↑	With the addition of new Initiate Change Request (ICR) and release planning activities, schedule tracking now begins prior to Approved for Implementation.
12	Duplicate and incomplete solutions have been put in place when solutions are addressed with multiple CRs that are not all completed concurrently.	The sponsors' program leaders should steward changes with consideration of related requests to ensure business needs are fully described and defined in a cohesive manner.	→	↑	This recommendation primarily refers to sponsor activities that take place prior to the project team initiating work against a Change Request. However, the new Release Planning Summit increases the opportunity for coordinating functional needs among CRs and clarifying business requirements.

Improvement Tracking

Scope Delivery

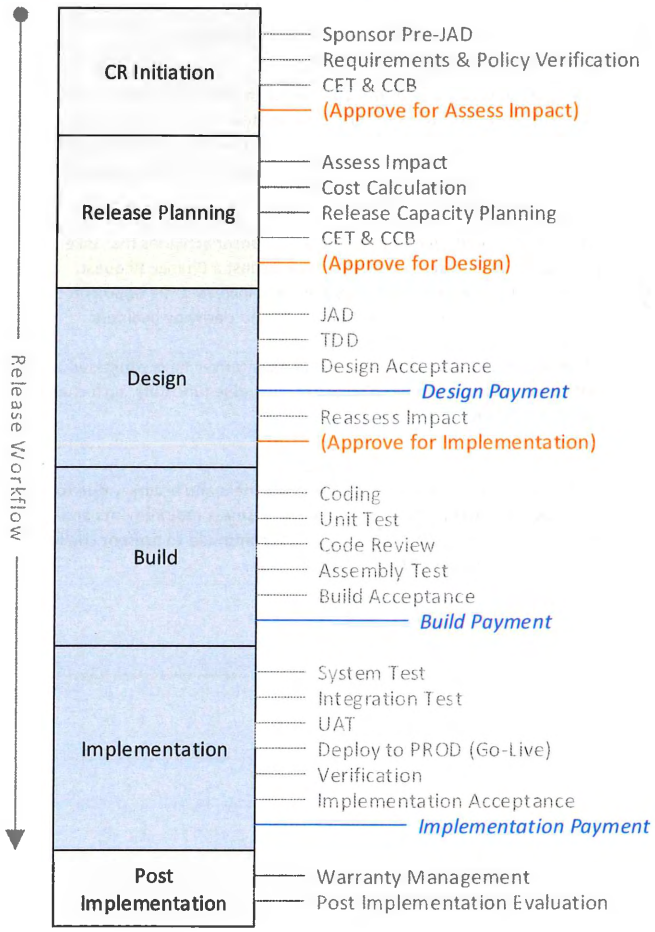
#	15.7 Lessons Learned	15.7 Recommendation	Improvement		16.2 Improvement Description
			15.9	16.2	
Scope Delivery					
13	Developers can help improve enhancement designs and better understand the sponsors' goals by being included in planning and JADs.	Consult with the developers during CR planning, as appropriate. Continue involving developers in JAD sessions.	⇨	↑	Some 16.2 CRs included Accenture development and technical team members in JADs and pre-JADs.
14	SAWS partners experienced repeated lack of proper environment setup and batch processes for the integration environment following the deployment of new builds.	Improve configuration management for test environments.	↑	↑	Test environment configurations prioritized for 16.2 release, including holding environments static until UAT is complete.
15	Teams managed 15.7 activities to the go-live date, extending design, build and test activities well past their planned completion dates.	Teams should manage to interim milestone dates to help ensure steady progress towards go-live dates.	⇨	↑	The overall schedule for R16.2 was intentionally extended early in the design and planning stage when it was determined that the contents of the release warranted more time for integration testing with partners. However, 9 of 13 CRs experienced schedule slip of greater than 14 days during the Design, Build or System Test phases.

Improvement Tracking

Budget & Efficiency

#	15.7 Lessons Learned	15.7 Recommendation	Improvement 15.9	Improvement 16.2	16.2 Improvement Description
Budget & Efficiency					
16	Splitting CR functionality across multiple releases may: - Result in significant increases to cost and scope - Duplicate effort and time spent in delivery (e.g., testing)	CRs should not be split over multiple releases unless cost implications are well understood and approved.	⇨	⇨	Among the CRs included in R16.2 following the Planning Summit, there were at least three that were split from related scope in earlier changes. In some cases, this approach was used to help meet mandatory delivery deadlines. However, it also appears that at least one CR was separated into multiple phases from the outset.
17	The State can gain efficiencies in planning, development and cost by combining similar CRs before the Assess Impact step.	- CRs with like functionality should be combined. - CRs should be drafted to ensure business needs are fully described and not piecemeal.	↑	↑	This recommendation primarily refers to sponsor activities that take place prior to the project team initiating work against a Change Request. However, the new Release Planning Summit increases the opportunity for coordinating functional needs among CRs and clarifying business requirements.
18	Repeatable system changes should be configurable to reduce overall cost to change.	Assess system changes that happen annually to determine if they can be more configurable and less reliant on development resources (e.g., FPL COLA table update).	⇨	⇨	Although project team and sponsor representatives have expressed a desire to investigate and implement configurable functions, such changes were not included in R16.2.
19	Approved design documents were modified several times prior to implementation. Late changes impact quality and cost.	- Limit design discussions to the approved scope. - Review designs for completeness and accuracy before final approval. - Consider freezing design upon approval. Limit further changes to only the most critical items on an exception basis.	↓	↑	16.2 experienced improved design completeness and accuracy due to new planning and JAD processes. Completing business requirements and designs by the scheduled milestone dates continued to present challenges for many of the CRs in R16.2.

Reference: Release Workflow



Three Payment Points

1. Design
2. Build
3. Implementation

The Importance of Scope

- Fixed scope = fixed price
- Important to agree upon desired functionality (scope) early in the workflow.
- Well defined requirements are necessary to achieve successful designs.
- Changes in scope may result in increased cost and lower quality (more defects).

CalHEERS Final eHIT Assessment

September 26, 2014

First Data.
b›yond the transaction

RECORD OF CHANGES

This document is controlled through the Document Management Process. To verify that the document is the latest version, please contact the First Data Team.

Date	Version	Responsible	Reason for Revision
8/11/2014	1.0	Karen Covey	Initial draft submission
9/3/2014	2.0	Karen Covey	Updated based on comments to Draft Assessment
9/12/2014	3.0	Karen Covey	Updated based on comments to DRAFT Assessment
9/19/2014	4.0	Karen Covey	Updated based on comments to DRAFT Assessment
9/26/2014	5.0	Karen Covey	Updated based on comments to Final Assessment

Table of Contents

1.0 EXECUTIVE SUMMARY 1
2.0 RELATED DOCUMENTATION 8
2.1 Documents and Standards Referenced 8
2.2 Acronyms 8
3.0 APPROACH / METHODOLOGY 11
4.0 ASSESSMENT RECOMMENDATIONS 15
4.1 MAGI Medi-Cal Rules Options 15
4.1.1 MAGI Medi-Cal Rules Recommendation 20
4.1.2 MAGI Rules Option Detailed Descriptions and Analysis 22
4.2 Global Recommendations 59
5.0 ASSESSMENT OBSERVATIONS 73
5.1 Technical Observations 73
5.2 Functional/Business Observations 94
5.3 General Observations 102
6.0 DELIVERABLE ROLES AND RESPONSIBILITIES 106
7.0 DELIVERABLE SCHEDULE 108
8.0 DELIVERABLE ASSUMPTIONS 109
9.0 APPENDIX A – LIST OF DOCUMENTS REVIEWED 110
APPENDIX B – LIST OF INTERVIEW PARTICIPANTS BY ORGANIZATION 115
APPENDIX C – EHIT PERFORMANCE GRAPHS 119
APPENDIX D – EHIT MAGI MEDI-CAL RULES OPTIONS ASSUMPTIONS 123

1.0 Executive Summary

Under the Patient Protection and Affordable Care Act (ACA) of 2010, the California Health Benefit Exchange, known as Covered California, and the Department of Health Care Services (DHCS) as co-Sponsors, developed and implemented a new web portal and eligibility and enrollment system to streamline the availability of health coverage to individuals, families and employers in the state of California. The California Healthcare Eligibility, Enrollment, and Retention System (CalHEERS) is the system for supporting the maintenance, operations, and ongoing business of Covered California and is one of a number of systems that support the maintenance, operations, and ongoing business of the DHCS. CalHEERS supports account creation, consumer application, eligibility rules, and health plan selection for insurance affordability programs. CalHEERS interfaces via the Electronic Health Information Transfer (eHIT) with the Statewide Automated Welfare Systems (SAWS) for Modified Adjusted Gross Income (MAGI) Medi-Cal eligibility, enrollment and reporting and to provide data for potential eligibility to other programs such as non-MAGI Medi-Cal, CalFresh and California Work Opportunity and Responsibility to Kids (CalWORKS).

The eHIT interface was developed to exchange critical MAGI Medi-Cal data between the SAWS Consortia (CalWIN, C-IV, and LEADER) and CalHEERS. eHIT is a real-time interface, including automated and real-time case creation, verifications via the Federal Data Service Hub (FDSH). Accenture, as the Systems Integrator, is responsible for the design, development, implementation, maintenance and operations of CalHEERS, including the eHIT interface.

The CalHEERS portal was initially deployed to the public on October 1, 2013. In order to meet the October 1, 2013 effective date of ACA related programs, the project created a schedule that implemented baseline aspects of the system after the initial October release. Implementation of the eHIT interface to begin processing for MAGI Medi-Cal was deployed in January 2014. Since January 2014, additional baseline functionality and some enhancements have been implemented through multiple production releases and are planned over the next several months to support the 2015 Covered California open enrollment period.

Since the implementation of the ACA, the State's and Counties' experiences with CalHEERS and eHIT afford the opportunity to further optimize MAGI Medi-Cal eligibility and verification processing.

Assessment Report Purpose

The purpose of the First Data CalHEERS eHIT Assessment Report is to examine opportunities for improvements to the eHIT and supporting CalHEERS Project processes. This report documents the findings from the review and analysis of the current eHIT interface between CalHEERS and the SAWS, presents options and recommendations for the placement of the MAGI Medi-Cal eligibility rules, discusses options for Notices of Action (NOAs) and presents global opportunities for improvement, regardless of which MAGI Medi-Cal rules Option is selected.

Assessment Scope

The scope of the CalHEERS eHIT Assessment Report as defined in the First Data Scope of Work included:

- Examining the operations and performance of the eHIT interface.
- Determining whether the division of system functionality between CalHEERS and SAWS is the most efficient and effective.
- Determining whether the current design of the eHIT interface is sustainable and maintainable.
- Examining the extent to which the design supports the business needs of the Sponsors and SAWS.
- Examining the extent to which the technical architecture supports the intended performance and maintenance goals.

Approach and Methodology

The assessment was accomplished through a series of information gathering interviews, documentation reviews and analysis along with follow-up working sessions to resolve inconsistent or incomplete findings. The assessment interviews included stakeholders, sponsors, partners and contractors including:

- Covered California
- DHCS
- California Department of Social Services (CDSS)
- CalHEERS State Project Management Team
- County Welfare Directors Association (CWDA)
- SAWS Consortia
- Office of Systems Integration (OSI)
- Accenture

The results of the Assessment are captured as Observations, and are the synthesis of interviewees' opinions and perceptions combined with information found in documentation. The Observations were used to help form First Data's recommendations.

Key Recommendations

Several key recommendations are highlighted in this Executive Summary; details are found within the body of each section.

MAGI Medi-Cal Rules Options

First Data defined and presents three different go-forward options for the eHIT architecture and the placement of MAGI Medi-Cal rules. These options were identified based on their ability to improve the (1) sustainability and maintainability of the system; (2) support program and business operations; and (3) extent to which the technical

architecture supports the intended performance and maintenance goals. The three identified options are as follows:

1. **Option 1 - Continue Enhancing the Current eHIT Architecture and Business Functionality**

- Retain the MAGI Medi-Cal business rules within CalHEERS.
- Continue to use the eligibility and verification and case management workflows within eHIT.
- CalHEERS and SAWS continue to make the planned enhancements to the current eHIT architecture.
- Update CalHEERS Notice functionality to support APTC/CSR and MAGI Medi-Cal mixed households.

2. **Option 2 – Modify the eHIT Architecture to Leverage SAWS Workflows and CalHEERS MAGI Medi-Cal Business Rules**

- Retain the MAGI Medi-Cal business rules within CalHEERS.
- Modify the CalHEERS Business Rules Engine to a simple and distinct service through SAWS, which is accessible by County Eligibility Workers (CEW) via SAWS as needed.
- Remove MAGI Medi-Cal Case Management functions from CalHEERS, decouple them from eHIT, and move them to SAWS.
- Move MAGI-Medi-Cal Notices of Action (NOAs) to SAWS.
- Provide a mechanism to support notices for the various types of mixed households (e.g. MAGI Medi-Cal, Non-MAGI Medi-Cal, Advanced Premium Tax Credit/Cost Share Reduction (APTC/CSR)).
- Decouple the verification process (VIED) from the eligibility business rules.
- Modify eHIT to create a simple and distinct electronic verification service.

3. **Option 3 - Distribute/Replicate MAGI Medi-Cal Workflow and Rules to SAWS**

- Replicate the MAGI Medi-Cal rules in CalHEERS and each of the three SAWS systems.
- Remove MAGI Medi-Cal Case Management functions from CalHEERS and move to SAWS.
- Move MAGI-Medi-Cal Notices of Action (NOAs) to SAWS.
- Provide a mechanism to support notices for the various types of mixed households (e.g. MAGI Medi-Cal, Non-MAGI Medi-Cal, and APTC/CSR).
- CalHEERS will continue to support MAGI Medi-Cal functions via the CalHEERS Portal in the same manner as today.
- CalHEERS would remain as the "gateway" to electronic verification sources.

The division of functionality for each option is summarized in the following charts. The detailed analysis of each option can be found in the, MAGI Medi-Cal Rules Options Section 4.1.

TABLE 1 - CONTINUE ENHANCING CURRENT EHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY OPTION 1 SUMMARY

Option 1 – Continue Enhancing Current eHIT Architecture and Business Functionality	CalHEERS	SAWS
MAGI Medi-Cal Case Management Functions	✔	✔
MAGI Medi-Cal Eligibility Rules	✔	
MAGI Medi-Cal Eligibility and Verification Workflow	✔	✔
Federal Data Services Hub Connectivity	✔	
MAGI Medi-Cal NOA Generation	✔	
MAGI Medi-Cal Case Worker Alerts	✔	✔

TABLE 2 - LEVERAGE SAWS WORKFLOW AND CALHEERS MAGI RULES OPTION 2 SUMMARY

Option 2 – Modify the eHIT Architecture to Leverage SAWS Workflows and CalHEERS MAGI Medi-Cal Business Rules	CalHEERS	SAWS
MAGI Medi-Cal Case Management Functions		✔
MAGI Medi-Cal Eligibility Rules	✔	
MAGI Medi-Cal Eligibility and Verification Workflow	✔	✔
Federal Data Services Hub Connectivity	✔	
MAGI Medi-Cal NOA Generation		✔
MAGI Medi-Cal Case Worker Alerts		✔

TABLE 3 - DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS OPTION 3 SUMMARY

Option 3 – Distribute/Replicate MAGI Medi-Cal Business Rules and Workflows to SAWS	CalHEERS	SAWS
MAGI Medi-Cal Case Management Functions		✔
MAGI Medi-Cal Eligibility Rules	✔	✔
MAGI Medi-Cal Eligibility and Verification Workflow		✔
Federal Data Services Hub Connectivity	✔	
MAGI Medi-Cal NOA Generation		✔
MAGI Medi-Cal Case Worker Alerts		✔

Based on the observations in this assessment and options identified, First Data's recommendation is as follows:

- Implement Option 2 - Modify the eHIT Architecture to Leverage SAWS Workflows and CalHEERS MAGI Medi-Cal Business Rules.
- Establish evaluation checkpoints as Option 2 is being developed and tested, and after it is implemented, to determine if the level of improvement/simplification is realized.
- If additional improvements are required that cannot be achieved via Option 2, proceed to Option 3.

Options 2 and 3 are not exclusive to one another: Option 2 implements a portion of the functionality also required for Option 3. For example, the updates required for the SAWS to integrate with CalHEERS business rules also supports potential localization of business rules within their systems. This approach provides a gradual set of changes and builds upon existing investments within the SAWS and CalHEERS. The first phase in the process provides more control and independence to the SAWS to implement business processes that better align with County operations. Additionally, simplifying the shared services provided by CalHEERS will potentially reduce the time required to implement new functionality related to MAGI Medi-Cal case management.

The First Data team recognizes that the State will need to perform additional planning for any adopted option. Planning would include conducting a detailed cost assessment and preparing schedule estimations.

Global Recommendations

The following group of recommendations represents global opportunities for improvement responding to our Assessment Observations, delineated in the body of this report. First

Data recommends adoption of the global recommendations, regardless of which MAGI Medi-Cal Rules Option is selected.

- Develop a strategic vision for the project to align stakeholder goals.
- Create and gain consensus of an enterprise-wide Governance Plan for all stakeholders.
- Create and gain consensus of an enterprise-wide Communication Strategy that will encompass communication needs for all stakeholders.
- Prioritize and implement critical defect resolution and change requests according to impact to County and Service Center business operations, especially enhanced error handling and worker alerts.
- Examine potential quick wins through technology optimizations.
- Adopt and implement a Use Case methodology to improve documentation and establish standardized program policy implementation.

Assessment Team

First Data selected a highly experienced team to conduct this assessment, who are named below:

- **Betty Uzupis**, Engagement Manager - Ms. Uzupis has over 30 years of experience in systems planning, procurement, development, and quality assurance (QA), including 24 years in the health and human services automation arena. Ms. Uzupis has provided oversight and for the CalHEERS Project through procurement, development and implementation. Ms. Uzupis also provides QA oversight for the SAWS C-IV and CalWIN projects. Ms. Uzupis lead the Cover Oregon Assessment team earlier in 2014.
- **Karen Covey**, Project Manager - Ms. Covey is a certified Project Management Professional, and has more than 30 years of experience in various management, marketing and technical positions. Ms. Covey provides project manager services for the CalHEERS Project and is responsible for monitoring, assessing and evaluating the system integrator's processes, procedures, controls, key deliverables and other artifacts for contract compliance, adherence to applicable standards, traceability, consistency, completeness and accuracy
- **Chris Dunham**, Communication/Governance - Ms. Dunham has over 40 years of County, state and private sector experience and leadership in the California Health and Human Services arena. She has extensive experience in project planning, project management and technology and expertise in managing large scale and complex information projects. Ms. Dunham provides project management and oversight services for the CalHEERS project. She served as the Acquisition Lead on the California Health Benefit Exchange planning project. Ms. Dunham was a team member on the Cover Oregon Assessment team in early 2014. Ms. Dunham provided executive leadership as the Acting Director for the Office of System Integration at its inception.
- **Wendy Battermann**, Business Functional - Ms. Battermann has over 21 years of experience in government consulting on information technology and management projects and over 15 years of direct project team supervision. Ms. Battermann

participated as the contract partner/communication and fiscal lead, and implementation lead for the CalHEERS project. She served as the Project Manager on the California Health Benefit Exchange planning project. She also participated in the initial development of the C-IV system.

- **Nathan Merrill**, Technical - Mr. Merrill is a certified Project Management Professional and has 15 years of experience with the public and private sectors providing systems project management, portfolio management, procurement support, quality assurance, and strategic planning. Mr. Merrill participated in the Procurement support for the CalHEERS project. He also participated as the QA Project Manager for the CalWIN Maintenance & Operations Project. Mr. Merrill supported the development of the C-IV system during the initial development and implementation.
- **Brendan McGuire**, Technical – Mr. McGuire has over 15 years of experience as a project delivery executive and enterprise architect. He has run large-scale program implementation efforts including areas such as application development, Commercial-Off-the-Shelf (COTS) implementations, infrastructure deployment, testing and design. Mr. McGuire was an Infrastructure and Solutions Architect for Hewlett Packard on the CalWIN Project before leaving for Oracle as a State and Local Government Enterprise Solutions Director. Most recently, Mr. McGuire was the Project Delivery Director for the State of Hawaii Medicaid Eligibility System ACA compliance implementation.
- **Larry Risser**, Technical – Mr. Risser is an accomplished Information Technology (IT) strategist with a 21+ year track record of improving IT operations. Mr. Risser is the technical QA specialist on the CalWIN Maintenance and Operations project. He served as the Senior Departmental Systems Analyst in Placer County.
- **Suds Pati**, Technical - Mr. Pati has over 17 years in IT in architecting, building, managing, and supporting Oracle, Java, Microsoft, VMware, IBM and HP products. Mr. Pati is an Oracle Certified Exadata Specialist, Oracle Certified ExaLogic Specialist, Oracle Certified WebLogic Administrator, Oracle Certified Solaris Administrator, Oracle Certified RAC Expert, Oracle Certified Professional, Oracle Certified Master (OCM), VMware Certified Professional, Sun Certified Java Developer and Java Programmer, Sun Certified Business Component Developer and Sun Certified Enterprise Architect.

Report Audience

The intended audience for the CalHEERS eHIT Assessment Report includes the Office of Systems Integration (OSI) and the key stakeholders who will participate in the implementation of any resultant recommendations. These stakeholders include, but are not limited to, Covered California, DHCS, CDSS, SAWS Consortia (CalWIN, C-IV, and LEADER/LRS), CWDA, and the CalHEERS Project.

2.0 Related Documentation

The following provides a listing of the documents, standards, and acronyms used and/or referenced in completing the CalHEERS eHIT Assessment.

2.1 Documents and Standards Referenced

The full list of documentation and standards used or referenced by the team as part of completing the assessment activities can be found in Appendix A – List of Documentation Reviewed.

2.2 Acronyms

The following acronyms are used within this document.

TABLE 4 – ACRONYMS

Acronym	Definition
ACA	Affordable Care Act
AHBX	Accenture Health Benefits Exchange
APTC/CSR	Advanced Premium Tax Credit/Cost Share Reduction
BPEL	Business Process Execution Language
BRE	Business Rules Engine
BTM	Business Transaction Monitoring
CDSS	California Department of Social Services
CalHEERS	California Healthcare Eligibility, Enrollment, and Retention System
CalWIN	CalWORKS Information Network
CalWORKS	California Work Opportunity and Responsibility to Kids
CEW	County Eligibility Worker
CFR	Code of Federal Regulations
CIN	Client Identification Number
CMS	Centers for Medicare and Medicaid Services
CoC	Change of Circumstances
COLA	Cost of Living Adjustments
CR	Change Request

Acronym	Definition
CWDA	County Welfare Directors Association of California
C-IV	Consortium IV
DB	Database
DED	Deliverable Expectation Document
DER	Determination of Eligibility Response
DHCS	Department of Health Care Services
EBDC	Eligibility Benefit Determination Calculation
EDD	Employment Development Department
EDR	Eligibility Determination Request
eHIT	Electronic Health Information Transfer
eICT	Electronic Inter-County Transfer
ESC	Executive Steering Committee
FDSH	Federal Data Service Hub
First Data	First Data Government Services
FTB	Franchise Tax Board
ITSM	IT Service Management
IV&V	Independent Verification and Validation
JAR/JAD	Joint Application Requirements/Joint Application Design
JMS	Java Message Service
LEADER	Los Angeles Eligibility Automated Determination, Evaluation and Reporting
LIHP	Low Income Health Plan
LRS	LEADER Replacement System
MAGI	Modified Adjusted Gross Income
MEDS	Medi-Cal Eligibility Data System
MEDIL	Medi-Cal Eligibility Division Information Letter

Acronym	Definition
NOA	Notice of Action
OPA	Oracle Policy Automation
OSB	Oracle Service Bus
OSI	Office of Systems Integration
O&M	Operations and Maintenance (a.k.a., Maintenance and Operations or M&O)
PCL	Printer Control Language
PDF	Portable Document Format
PSC	Project Steering Committee
QA	Quality Assurance
RAC	Real Application Clusters
RFP	Request for Proposal
SAWS	Statewide Automated Welfare System
SCI	State Client Index
SLA	Service Level Agreement
SLO	Service Level Objective
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SSA	Social Services Administration
SSN	Social Security Number
TR	Technical Requirement
VIED	Verification and Income Eligibility Determination
WSDL	Web Service Definition Language
XA	eXtended Architecture
XML	Extensible Markup Language

3.0 Approach / Methodology

The CalHEERS eHIT Assessment was conducted over a fourteen-week time period and included interviewing key staff and stakeholders, reviewing documentation, and developing the final assessment report. The team conducted a limited review of highly important eHIT factors, including:

- Sustainability and maintainability of the interface and system functionality designs
- The division of functionality between SAWS and CalHEERS
- The ability to meet business needs of Project Sponsors and SAWS

Due to the short timeframe, information was primarily obtained during interviews and through the review of available documentation. More in-depth reviews typically include validation of code, configuration settings, and architecture; however time and required materials were not available.

The First Data team took a no-surprises approach to conducting assessment activities, from the discussions and approval of the Deliverable Expectation Document (DED), to ensure interviewees understood how their information and identities would be included in the Report, to keeping management apprised of observations, risks, and issues throughout the process. The following summarizes the approaches and methods employed to complete the assessment:

- **Project Management Methodology and Approach** – At project initiation, First Data worked closely with the OSI management team to confirm direction and create a detailed work plan that provided sufficient time for stakeholder involvement in the assessment activities and review of the draft and final Report. The First Data team conducted a project kickoff meeting with stakeholders to introduce the project team and provide an overview of the assessment objectives, approach, timelines, and milestones. The First Data team met daily to coordinate activities and discuss issues, risks, and observations. On a weekly basis, the First Data Manager met with the OSI management team to apprise them of status, issues, risks, and preliminary observations.
- **Interview Approach** – First Data initiated its assessment activities by interviewing many of the key staff and stakeholders associated with the decision-making, creation, maintenance, and/or use of the eHIT interface. The interviews were conducted using a set of standardized questions that were customized for each group (i.e., management, technical, functional, or user group). In total, First Data interviewed over 70 people as part of the assessment, including leadership and representatives of Covered California, DHCS, CDSS, CalHEERS state project management team, CWDA, SAWS Consortia; Counties (one per consortium), OSI, Accenture, and Oracle. First Data requested interviews with three people who were either not available or elected to not be interviewed. The complete list of people interviewed is provided in Appendix B – List of Interview Participants by Organization. The results of the interviews were validated

through documentation (where available or appropriate) and incorporated into the key observations.

- **Global Documentation Analysis Approach** – A key part of First Data's approach involved conducting a detailed review of global project artifacts and documentation. Global documentation included:
    - Project status reports (i.e., Independent Validation and Verification (IV&V) reports, Accenture status reports, and CalHEERS Project status reports)
    - Materials from Executive Steering Committee (ESC), Program Policy Committee, Project Integration meetings, Technology Committee, and Release Readiness Assessments
    - CalHEERS deliverables
    - Applicable CalHEERS, SAWS Consortia, DHCS, and Covered California communication and governance plans, processes, and procedures
    - Meeting documentation and minutes from SAWS-specific meetings with CalHEERS and/or DHCS
    - Support processes for eHIT and other SAWS-specific interactions

  These documents were made available to the First Data team via email and/or via the CalHEERS SharePoint site. Reviewing the global documentation served to:

    - Validate information obtained in the interviews
    - Provide a historical perspective of decisions made, including when or how many times they were made, by whom, and through which forum(s)
    - Provide a historical perspective of risks, issues, and other escalated items
    - Highlight areas for improvement

- **Functional/Business Analysis Approach** – The First Data team collected and analyzed eHIT functional design documentation, relevant Medi-Cal Eligibility Division Information Letters (MEDILs), eHIT-related change requests and defects, and special assessments (e.g., DHCS' Negative Action: Assessment of Options). The information was used to validate information obtained from the business, program, and policy interview participants. The documentation also assisted the First Data team to obtain perspective on functionality agreed upon and delivered, functional design choices, the timing and purpose of policies implemented, and changes requested to either fix or improve eHIT functionality. Through interviews, documentation review, and follow-up on initial observations, the team:
    - Evaluated the design and implementation of the eHIT interface from a functional/business perspective
    - Analyzed related State and Federal policies and publications
    - Analyzed open eligibility, SAWS, and/or eHIT interface change requests to determine validity and inclusion in baseline functionality
    - Assessed the impact of eHIT on the Covered California Service Center and County business operations

- **Technical Analysis Approach** – The First Data team collected and analyzed the available eHIT technical infrastructure, architecture, and interface design

documentation, eHIT-related change requests and defects, error reports, defect and performance trends. The information was used to validate information obtained from the technical interviews and to obtain perspective on the technical solution agreed upon and delivered, and changes requested to either fix or improve eHIT technical stability and performance. Through interviews, documentation review, and follow-up on initial observations, the team:

- Reviewed eHIT technical design and data sharing strategy to assess system stability and performance given the current and projected transaction volumes and throughput. Specifically, the team analyzed the design to determine if it is well architected or overly complicated and whether there are areas for tuning or reducing points of failure.
- Reviewed the business rules engine (BRE) architecture for MAGI with consideration for impact to Non-MAGI programs that reside within SAWS.
- Determined the feasibility of having MAGI rules reside in CalHEERS and each SAWS application. Specifically evaluated if that configuration would improve stability and performance, or if other potential alternatives could be used. The team also analyzed the possibility of the MAGI rules simply being duplicated in all applications or if eHIT and VIED are too interrelated to untangle. The team further:
  - ✓ Discussed how mixed household cases could be managed in CalHEERS and SAWS and the impact to the consumer (Note: "mixed households" refers to APTC and Medi-Cal members as well as MAGI and non-MAGI members with the same household.)
  - ✓ Proposed a maintenance approach (technology and governance) to keep all systems synchronized.
  - ✓ Identified cost implications of the proposed maintenance approach
  - ✓ Identified concerns that may surface from State and Federal Partners and approval agencies
- Determined whether the NOA architecture is easy to maintain or overly complicated. Specifically, the team:
  - ✓ Reviewed notice hand-offs between CalHEERS and SAWS
  - ✓ Explored the feasibility of MAGI Medi-Cal notices being built into SAWS instead of CalHEERS
  - ✓ Conducted initial analysis on mechanisms to support notices for mixed households across the three presented Options
  - ✓ Discussed consumer impacts, including consumer experience of the current NOA strategy and moving NOAs to SAWS

- **Assessment Report Development and Review Approach** – The team initiated the development of the CalHEERS eHIT Assessment Report by submitting a DED to the OSI. The intent of the DED was to ensure the Final Report would meet the expectations of the OSI and be useful to all stakeholders involved in implementing recommendations. The DED provided a clearly defined structure for the deliverable, the content expected

in each deliverable section, and the high-level approach to be used during the assessment effort. The DED was approved by the OSI on July 8, 2014.

The First Data team developed the draft Report by consolidating, discussing, and documenting its observations internally, identifying clear themes that surfaced across interviews and documentation reviews. As necessary, team members followed up with the interview participants and others to clarify information and/or obtain greater detail to support observations and recommendations (including pros and cons). Throughout the development of the Report, the First Data management kept the OSI management team apprised to ensure there were no surprises when the draft report was delivered. On August 11, 2014, First Data submitted the Draft CalHEERS eHIT Assessment Report for formal review and on August 12, 2014 conducted a walkthrough of the draft observations and recommendations with Stakeholders/ Sponsors.

The team has incorporated the feedback from the Stakeholder/Sponsor review into the Final CalHEERS eHIT Assessment Report. The team conducted another walkthrough of the document with State Project Management Team on September 3, 2014 and incorporated their feedback. The final CalHEERS Assessment Report was submitted to the OSI for final review on September 19, 2014.

4.0 Assessment Recommendations

This section contains the detailed recommendations that resulted from analyzing the observations and documentation. While some recommendations may stem from a single observation, in some cases, multiple observations will lead to a single recommendation. Our recommendations are split between sections:

- Section 4.1 – MAGI Medi-Cal Rules Options – Includes MAGI Medi-Cal Rules Options, with considerations for the eHIT architecture, disposition of the MAGI Medi-Cal Rules and NOA options.
- Section 4.2 – Global Recommendations – Includes recommendations that should be considered regardless other decisions made regarding MAGI Medi-Cal Rules, eHIT architecture, or other long-term plans.

4.1 MAGI Medi-Cal Rules Options

The following section examines the different go-forward options for the eHIT MAGI Medi-Cal Rules architecture. The First Data team is presenting three options that were identified based on their ability to support MAGI Medi-Cal processing, implementation time constraints, and existing investments in CalHEERS and the SAWS. The team initially identified several options, and after consideration, a number were discarded as not viable, including the following:

- Moving all MAGI Medi-Cal caseload management functions to CalHEERS
- Using an independent provider to manage and maintain a Business Rules Engine service

Three promising options were selected for full analysis and consideration. The team framed its analysis based on several criteria as depicted in Figure 1. Each criterion was evaluated against a highest fit **(green)**, medium fit **(yellow)**, and lowest fit **(red)** rating

Below is a definition for each of the elements that were considered in the scoring analysis. The criteria were developed and selected based on the First Data team's expert opinion.

Criteria and Score	
County/Consumer Experience	○
Business Rules Maintenance Effort	○
Case Management	○
Uniform Policy Implementation	○
Mixed Household	○
County Operations	○
Implementation Risk	○
Implementation Cost	○

Figure 1 Scoring Criteria

County/Consumer Experience:

- The ability of the consumer to receive a minimum preliminary eligibility determination during intake with a CEW. (Note: the scope of this assessment reviews consumer experience with the CEW.)
- The ability for a CEW to receive immediate feedback as to the status of an eligibility and verification request and promptly process an action.

- The ability to generate timely and easily understood (non-duplicated notices) to be provided to consumers.

Business Rules Maintenance Effort

- The level of effort and complexity to leverage technical tools and processes to update and maintain the functional business rules that are utilized to determine MAGI Medi-Cal eligibility.
- The level of coordination required to manage business rules on an ongoing basis.

Case Management

- The ability to adapt functions and processes to changing operating patterns over time.
- The level of technical interaction and interdependency across systems.
- Avoidance of proprietary software or need for highly specialized skill sets.
- Incorporation of industry standard technologies and architectures.

Uniform Policy Implementation

- Coordination required to implement consistent policies.
- Implementation of policy changes across all impacted systems in a timely manner.

Mixed Households

- Provide seamless consumer experience (e.g., portal functions) along with a holistic view of households to consumers, CEWs and Service Center staff for all mixed household scenarios, including:
    - APTC/CSR and MAGI Medi-Cal
    - Non MAGI Medi-Cal and MAGI Medi-Cal.
- Ability to support notices across the various combinations of mixed households.
- Provide reporting capability across all health programs.

County Operations

- Technology solution aligns with various county operating models (e.g., task function-based processes).
- Technology solution mitigates need for manual interventions, such as workarounds or minimizes the need for data synchronization between systems.
- System provides "real time" feedback to consumers or CEWs regarding eligibility status.
- Avoids duplicate data entry in multiple systems.
- Avoids impacting other supported county health programs.

Implementation Risk

- Complexity and coordination needed among parties to implement system changes and resolve defects.

- Introduction of new functionality; potential of need for system stabilization period.
- Uncertainty around effectiveness of technical and business architecture.

Implementation Cost

- A full cost/benefit analysis of the three options was not in scope for the assessment. Implementation cost scoring is based on relative costs between the three options based on First Data's expert opinion by evaluating the level the change within CalHEERS and SAWS.

Descriptions of the three options evaluated are as follows:

- **Option 1 Continue Enhancing Current eHIT Architecture and Business Functionality** – Continue efforts to enhance eHIT to align with County operations and add new workflows for functions such as renewals, negative action and Cost of Living Adjustments (COLA). This option includes the following::
    - ✓ Retains the MAGI Medi-Cal business rules within CalHEERS.
    - ✓ Continues to use the eligibility and verification and case management workflows within eHIT.
    - ✓ CalHEERS and SAWS continue to make the planned enhancements to the current eHIT architecture.
    - ✓ Updates CalHEERS Notice functionality to support APTC/CSR and MAGI Medi-Cal mixed households.
- **Option 2 Modify the eHIT architecture to leverage SAWS Workflows and CalHEERS MAGI Medi-Cal Business Rules** – Implement a phased approach to first simplify the CalHEERS eHIT architecture to provide specific web services for the MAGI Medi-Cal business rules and electronic verifications. Move case management functions out of CalHEERS to SAWS. Leverage pre-ACA Medi-Cal workflows within the SAWS to incorporate the CalHEERS provided web services. This option includes the following:
    - ✓ Retains the MAGI Medi-Cal business rules within CalHEERS.
    - ✓ Modify the CalHEERS Business Rules Engine to a simple and distinct service through SAWS, which is accessible by County Eligibility Workers (CEW) via SAWS as needed.
    - ✓ Removes MAGI Medi-Cal Case Management functions from CalHEERS, decouples them from eHIT, and moves them to SAWS.
    - ✓ Moves MAGI-Medi-Cal Notices of Action (NOAs) to SAWS.
    - ✓ Provides mechanism to support notices for the various types of mixed households (e.g. MAGI Medi-Cal, Non-MAGI Medi-Cal, and APTC/CSR).
    - ✓ Decouples the verification process (VIED) from the eligibility business rules.
    - ✓ Modifies eHIT to create a simple and distinct electronic verification service.

- **Option 3 Distribute/Replicate MAGI Medi-Cal Workflow and Rules to SAWS** – Develop, test and perform ongoing maintenance for MAGI Medi-Cal business rules within the SAWS EBDC sub-systems. Leverage pre-ACA Medi-Cal workflows within the SAWS for newly developed MAGI Medi-Cal rules and to incorporate the CalHEERS provided web services for the Federal Data Services Hub. Continue to maintain MAGI Medi-Cal rules within CalHEERS to support the Covered California Portal and Service Centers. This option includes the following:
    - ✓ Replicates the MAGI Medi-Cal rules in CalHEERS and each of the three SAWS systems.
    - ✓ Removes MAGI Medi-Cal Case Management functions from CalHEERS and move to SAWS.
    - ✓ Moves MAGI-Medi-Cal Notices of Action (NOAs) to SAWS.
    - ✓ Provides mechanism to support notices for the various types of mixed households (e.g. MAGI Medi-Cal, Non-MAGI Medi-Cal, and APTC/CSR).
    - ✓ CalHEERS continues to support MAGI Medi-Cal functions via the CalHEERS Portal in the same manner as today.
    - ✓ CalHEERS remains as the "gateway" to electronic verification sources.

The options are summarized in the following tables. The accompanying analysis, pros, con, scoring and recommendations are embedded in each option's detailed description.

TABLE 5 – CONTINUE ENHANCING CURRENT EHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY OPTION 1 SUMMARY

Option 1 – Continue Enhancing Current eHIT Architecture and Business Functionality	CalHEERS	SAWS
MAGI Medi-Cal Case Management Functions	✔	✔
MAGI Medi-Cal Business Rules	✔	
MAGI Medi-Cal Eligibility and Verification Workflow	✔	✔
Federal Data Services Hub Connectivity	✔	
MAGI Medi-Cal NOA Generation	✔	
MAGI Medi-Cal Case Worker Alerts	✔	✔

TABLE 6 – LEVERAGE SAWS WORKFLOW AND CALHEERS MAGI RULES OPTION 2 SUMMARY

Option 2 – Modify the eHIT architecture to leverage SAWS Workflows and CalHEERS MAGI Medi-Cal Business Rules	CalHEERS	SAWS
MAGI Medi-Cal Case Management Functions		✔
MAGI Medi-Cal Business Rules	✔	
MAGI Medi-Cal Eligibility and Verification Workflow	✔	✔
Federal Data Services Hub Connectivity	✔	
MAGI Medi-Cal NOA Generation		✔
MAGI Medi-Cal Case Worker Alerts		✔

TABLE 7 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS OPTION 3 SUMMARY

Option 3 – Distribute/Replicate MAGI Medi-Cal Business Rules and Workflows to SAWS	CalHEERS	SAWS
MAGI Medi-Cal Case Management Functions		✔
MAGI Medi-Cal Business Rules	✔	✔
MAGI Medi-Cal Eligibility and Verification Workflow		✔
Federal Data Services Hub Connectivity	✔	
MAGI Medi-Cal NOA Generation		✔
MAGI Medi-Cal Case Worker Alerts		✔

Since the implementation of the ACA and eHIT, numerous lessons learned have been identified creating the opportunity to further optimize MAGI Medi-Cal eligibility and verification processing. For example, the current eHIT architecture was designed to address federal requirements to utilize electronic sources of verification data prior to eligibility determination. The implications created by the current eHIT architecture are documented in the Technical and Functional observations of this assessment. The new information and experience supporting the ACA and eHIT provide an opportunity to review the implementation and make adjustments to the architecture.

4.1.1 MAGI Medi-Cal Rules Recommendation

The First Data team is recommending this approach as Option 2 provides the State, Counties and Federal stakeholders with the following benefits:

- Leverages existing investments in SAWS workflows for functions such as redetermination, COLAs and notices, along with change request work completed on the CalHEERS MAGI Medi-Cal business rules and eHIT data interface.
- Provides an architecture that allows the SAWS to create a MAGI Medi-Cal eligibility and verification process while aligning with early communication from the Centers for Medicare and Medicaid Services (CMS).
- Reduces the maintenance effort of MAGI Medi-Cal eligibility rules within multiple rule engine sets.
- Facilitates long-term sustainability and maintainability by reducing the design, implementation and testing constraints generated by the current centralization of portions of the MAGI Medi-Cal workflow within CalHEERS.

The MAGI Medi-Cal rules options could build upon one another allowing for a gradual implementation. This adoption could provide a roadmap that allows for the implementation of a MAGI Medi-Cal business architecture that addresses the various MAGI Medi-Cal stakeholder's needs. Given the short amount of time available between this assessment and the 2015 Open Enrollment period, the First Data team recommends continue focusing the change requests that are currently in development to enhance the eHIT architecture that provide the most impact on County MAGI Medi-Cal processing while making preparations to implement Option 2. Several change requests that should have positive impacts on MAGI Medi-Cal processing are already incorporated into the CalHEERS release plan.

Options 2 and 3 are not exclusive to one another. The work to update pre-ACA workflows within the SAWS is also required for localized business rules. For example, the pre-ACA Medi-Cal workflows will need to be modified to utilize the CalHEERS provided connection to the FDSH and to perform various business logic to prepare and validate data transmission to the central MAGI Medi-Cal rule base. An additional basis for the recommendation to pursue Option 2 is that if the centrally deployed MAGI Medi-Cal business rules continue to negatively impact County operations, updates to the SAWS can be leveraged for a local implementation of the business rules.

Additionally, some of the system functions of the current architecture implemented within SAWS and eHIT can be leveraged to implement the Option 2 architecture. The backend services supporting eHIT (e.g., VIED) utilize a service-oriented architecture that is conducive to implementing Option 2. Based on the observations in this assessment and options identified First Data's recommendation is as follows:

- Continue efforts to update and optimize eHIT in preparation for the 2015 Open Enrollment.

- Once an agreed upon minimal set of functionality is achieved, freeze eHIT enhancements related to the SAWS.
- Implement the Option 2 architecture updates and assess its effectiveness and long-term sustainability.
- Identify and incorporate Key Performance Indicators (KPI)s to measure the progress of eHIT such as:
    - ✓ Response time of transactions
    - ✓ Error resolutions time periods
    - ✓ The amount of workarounds required to process applications
- Continue to conduct progress evaluation (checkpoint) assessments to determine the level of improvement and simplification with the eHIT interface and if additional changes as outlined in Option 3 are warranted.

4.1.2 MAGI Rules Option Detailed Descriptions and Analysis

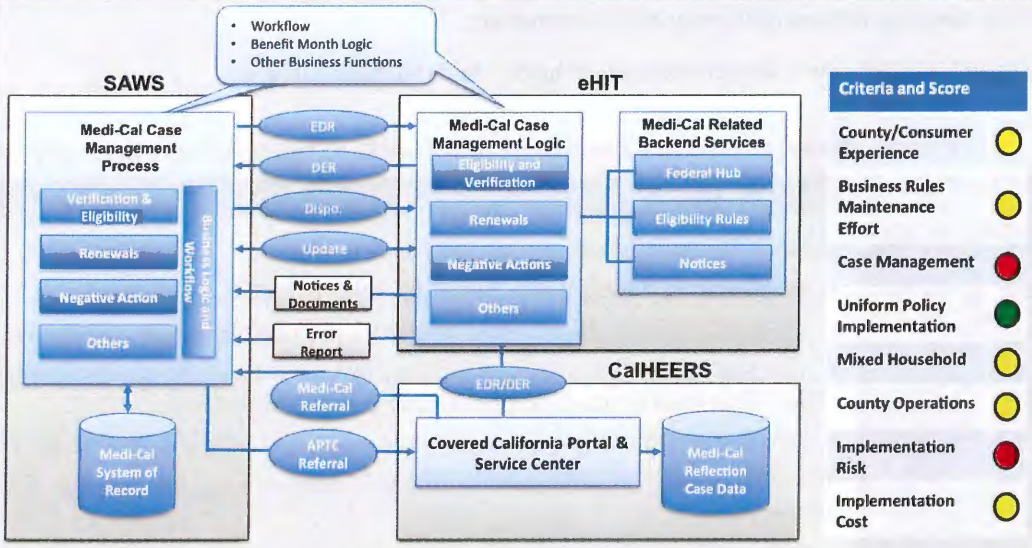
4.1.2.1 Continue Enhancing Current eHIT Architecture

The table below provides a detailed overview of Option 1 for MAGI Medi-Cal rules.

TABLE 8 – OPTION 1 – CONTINUE ENHANCING CURRENT EHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY

OPTION 1 – CONTINUE ENHANCING CURRENT EHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY	
Proposed Solution	Option 1 continues the existing CalHEERS and eHIT Design • Retain the MAGI Medi-Cal business rules within CalHEERS. • Continue to use the eligibility and verification and case management workflows within eHIT. • CalHEERS and SAWS continue to make the planned enhancements to the current eHIT architecture including implementing identified change requests and defects. • Update CalHEERS Notice functionality to support APTC/CSR and MAGI Medi-Cal mixed households. The following diagram illustrates how eHIT and SAWS work together in Option 1 for Medi-Cal related functions:

OPTION 1 – CONTINUE ENHANCING CURRENT EHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY

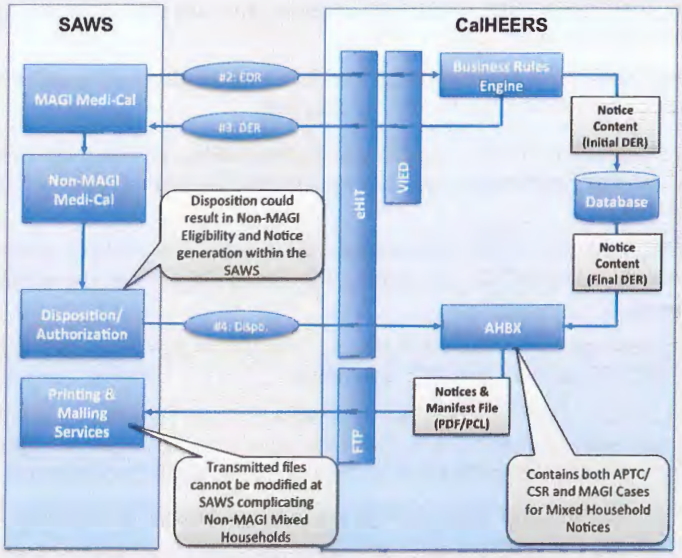


Notice Architecture

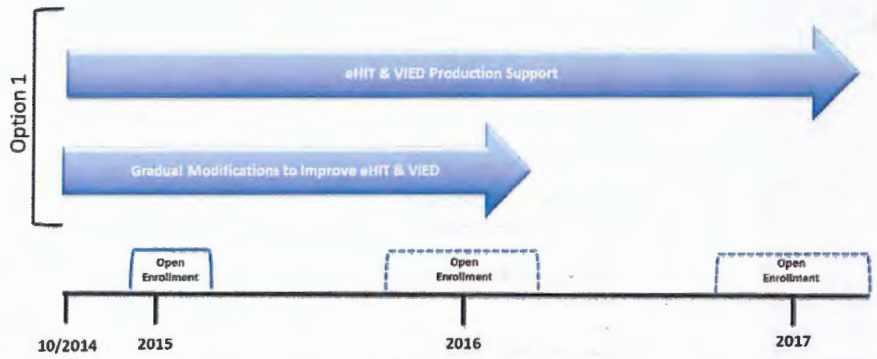
The next diagram and list below provides an overview of the current architecture for MAGI Medi-Cal notices. For a more detailed overview of the Notice generation process please see Technical Observation T14.

OPTION 1 – CONTINUE ENHANCING CURRENT EHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY

1. CalHEERS processes eligibility and verification functions and returns response (DER Transaction #3).
2. Once approved by the CEWs, SAWS transmits the disposition (#4 Disposition) to CalHEERS.
3. CalHEERS receives the case disposition data and associates the DERs authorized by the SAWS with the previously generated notice content (Step 2).
4. CalHEERS batch reads the disposition information and generates the notices requested by the SAWS
5. SAWS receive the files from CalHEERS and prepares a subsequent file transmission to the print vendor.
6. Print vendor receives files and produces mailings.



OPTION 1 – CONTINUE ENHANCING CURRENT eHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY	
Pros	• Builds upon investment already made in infrastructure, resources, schedule, and cost to build the eHIT interface and VIED. • Includes a number of currently planned improvements. Multiple change requests and updates to the eHIT schema (3.0) are scheduled to be implemented within the next six months to resolve a variety of technical/functional challenges with the eHIT interface, including: ✓ Addition of income types to help address income calculation workarounds performed by CEWs. ✓ Addition of effective dates for income and deductions to provide case history. ✓ Caching verification data to improve processing time for both companion and single Eligibility Determination Request (EDR). • Utilizes the interface infrastructure that has already been procured to address projected processing needs for open enrollment and renewal processing.
Cons	• Eligibility workers have limited access to EDR status and no automated "alerts" to address exceptions. Manual tracking of case status complicates operations particularly for the Counties using task function based operations. • The time required to generate and print a notice is lengthy due to the complexity of the interactions between SAWS and CalHEERS. The lengthy timing is a risk for negative action and notice delivery requirements. • The central management of the VIED process complicates the SAWS' ability to manage the impact of the ACA policies on other non-health programs. • The centralization of the workflow and its related business rules (non-eligibility) requires that all Consortia implement CalHEERS releases at the same time. Simultaneous change requires resources to coordinate and limits the speed at which improvements can be implemented. • A data reconciliation process is needed to synchronize data between CalHEERS and SAWS. • Management of eligibility and verification functions within CalHEERS will continue to require CEWs to access both CalHEERS and SAWS.

OPTION 1 – CONTINUE ENHANCING CURRENT eHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY	
	• Coupling the verification and eligibility process limits the ability to mitigate the impact of nightly Federal Data Services Hub outages on SAWS and CalHEERS batch processing.
Time Frame	The CalHEERS eHIT assessment is forward looking and evaluates the projected state of the current eHIT architecture at the onset of the 2015 Open Enrollment. The following figure provides an overview of this timeline. The figure below provides a notional timeline for the completion of eHIT functionality required to address county operation needs: 
Maintenance Approach	CalHEERS continues to perform the following maintenance functions: • Maintain MAGI Medi-Cal business rules. • Maintain eligibility functions related to APTC/CSR. • Maintain and expand current SAWS workflows required to support MAGI Medi-Cal processing. • Maintain workflow and business rule functions required to provide real-time eligibility for applications received via the Covered California portal. • Manage change and release plan for eHIT including all current VIED functions.

OPTION 1 – CONTINUE ENHANCING CURRENT eHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY	
	• Maintain FDSH connectivity and interfaces. SAWS continues to perform the following maintenance functions: • Maintain eHIT integration to the SAWS applications. • Continue to maintain and expand other portions of the SAWS, to incorporate eHIT updates. **Data Sharing** • Continue to optimize the data synchronization mechanisms between the SAWS and Accenture Health Benefit Exchange (AHBX) to reduce related processing errors. • Clearly communicate system of record for various data elements and modify VIED accordingly to reduce eHIT errors generated from data comparison between CalHEERS and SAWS (EDRs). **Release and Change Management** • Requires significant effort to coordinate amongst CalHEERS, SAWS, DHCS, Covered California, and CWDA program and technical groups. • Prioritize some of the major issues that are the highest impact on County operations. **Support** • Increase cross-organizational resources to track and address issues end-to-end. CalHEERS has conducted individual working sessions with SAWS to address integration issues. • Recommend that CalHEERS deploy staff to work on site with each consortium directly until key issues are resolved.
County/ Consumer Experience	• The timely processing of consumer applications by CEWs may be inhibited until issues such as providing eligibility worker alerts and business level errors are addressed. • Consumers are impacted with a delay of application or change processing when SAWS, CalHEERS, and MEDS are out of sync. • The ability for the CEWs to process all programs in a single session experience with a consumer is

OPTION 1 – CONTINUE ENHANCING CURRENT EHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY	
Score: Yellow	limited to the ability of the eHIT interface to process information timely and exchange verification data with the federal data hub. • The ability to provide timely benefits is contingent on aligning the eHIT workflows with SAWS business processes.
Business Rules Maintenance Effort *Score: Yellow*	• Although a single repository of business rules is utilized, the level of effort to continue to communicate and coordinate business rules releases and impacts among the Project, Sponsors, and Partners continues to be a significant effort, and reduces speed to implement changes.
Case Management *Score: Red*	• Continues to require a significant responsibility on CalHEERS to develop a system that aligns with the various needs and operating patterns within the Counties. • Centralization of the eligibility and verification process slows the ability to address defects and implement new features due to extensive design and approval times by requiring a solution that addresses DHCS and county needs.
Uniform Policy Implementation *Score: Green*	• Leverages existing CalHEERS project processes to implement policy consistently.
Mixed Household Cases *Score: Yellow*	**MAGI and Non-MAGI Mixed Households** • Although possible, the management of combined MAGI and Non-MAGI Medi-Cal households is more complex as the workflow for the intake and eligibility processes are distributed across two systems. During our assessment we did not encounter any change requests that appeared to have material impact on improving management of MAGI and Non-MAGI households. • The current architecture may create complications to generate combined notices for MAGI and Non-MAGI households as the SAWS receive pre-rendered documents.

OPTION 1 – CONTINUE ENHANCING CURRENT eHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY	
	MAGI and APTC/CSR Mixed Households • The lack of an effective date-based data model within CalHEERS limits the ability to service MAGI Medi-Cal consumers. Several change orders are under various states of implementation that will help address this issue. Once the effective date based model is in place, the current architecture provides CalHEERS information on both types of consumers in order to address service requests. • The existence of both MAGI Medi-Cal and APTC case information is located within CalHEERS facilitates an application update to support Notice generation for this scenario of mixed households. This functionality has not yet been implemented within CalHEERS. **Notice Generation** • The time required to generate and print a notice is lengthy due to the complexity of the business process and interactions between SAWS and CalHEERS. The timing creates concern for negative action and other requirements for timely notifications to clients.
County Operations *Score: Yellow*	• CEWs and Service Center representatives do not have visibility into the eHIT system contributing the following: ✓ Lack of worker alerts disrupts task function based operations ✓ Workers do not have information on EDR failure reasons to address problems ✓ Workers do not have visibility into the eligibility determination reasons (decision tree) to troubleshoot potential determination errors • County and Consortia service desks are encountering significant workload increases because of the additional effort to manage issues between the workers, SAWS, and CalHEERS. • County staffs have been redirected from supporting other programs (e.g., CalFresh) to support Medi-Cal cases. • Data issues resulting from transfer of data between Service Center and Counties may continue to exist, creating additional workload for Service Center representatives and County workers to manually review all data fields to identify discrepancies.

OPTION 1 – CONTINUE ENHANCING CURRENT eHIT ARCHITECTURE AND BUSINESS FUNCTIONALITY	
Implementation Risk *Score: Red*	• Continual additional coordination and effort between SAWS and CalHEERS will be needed for required improvements needed to further stabilize eHIT • The modifications needed to fully functionalize eHIT should be prioritized with other CalHEERS system changes.
Implementation Cost *Score: Yellow*	Costs have already been estimated for approved change requests and defect resolution efforts are included in establishing maintenance contracts. The following activities are required to address additional issues with eHIT and the accompanying SAWS integrations and may result in a cost increase: • Design effort to create a business process that addresses end-to-end lifecycle of case and capabilities to address exception handling (e.g., Worker Alerts). • Assessment effort to identify all potential cross-program conflicts, such as differences in data collection and household composition within the SAWS applications. • Design effort to create user interface and workflow within the SAWS that incorporates form validation to reduce some sources of eHIT error rates. • Initiation of a data reconciliation effort between CalHEERS, SAWS, and MEDS; this effort requires system support as well as County operations resources.

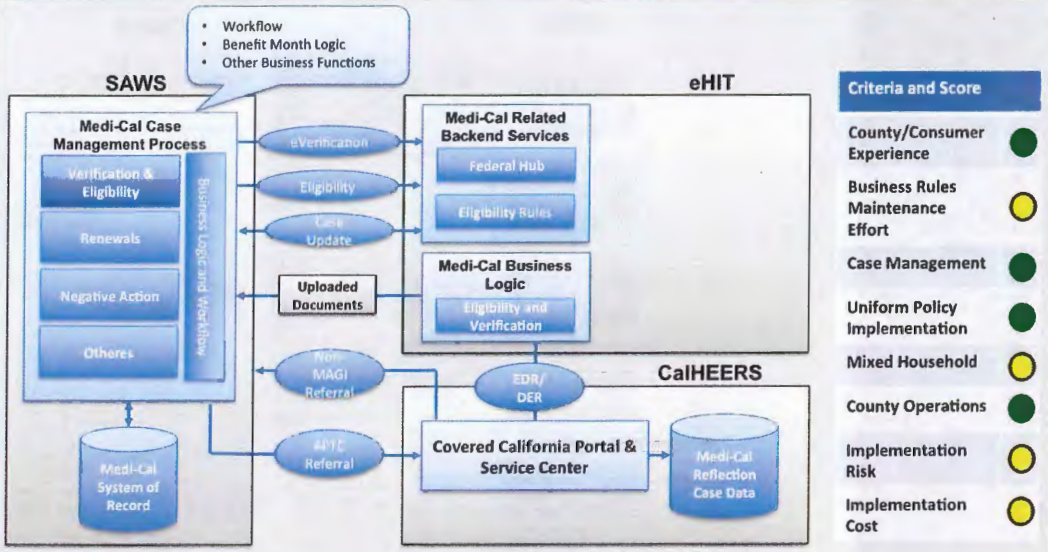
4.1.2.2 Leverage SAWS Workflow and CalHEERS MAGI Rules

The table below provides a detailed overview of Option 2 for MAGI Medi-Cal rules.

TABLE 9 – OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES	
Proposed Solution	Option 2 simplifies the eHIT architecture by: • Retaining the MAGI Medi-Cal business rules within CalHEERS • Removing Case Management functions from CalHEERS, decoupling them from eHIT, and moving them to SAWS • Moving Notices of Action (NOAs) to SAWS • Decoupling VIED from the CalHEERS Business Rules Engine • Modifying the CalHEERS Business Rules Engine to a simple and distinct service • Modifying eHIT to create a simple and distinct electronic verification service This option modifies the current eHIT web services to enable individual web services to be enacted for specific purposes (i.e., verifications, business rules). It allows the Consortia to modify the respective SAWS systems to access to the BRE when needed. During design, an additional web service needs to be identified to create records of MAGI Medi-Cal cases within AHBX database (reflection cases) to support the Covered California Service Center and reporting purposes. Periodic eHIT assessments should be conducted to evaluate progress and monitor results against key performance indicators (KPIs) established during project initiation. If the eHIT interface does not meet agreed upon eHIT KPI, proceed to implementing the remaining elements of Option 3. The following diagram illustrates at a high-level how eHIT and SAWS work together for Medi-Cal related functions in Option 2 and displays this option's scoring:

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES

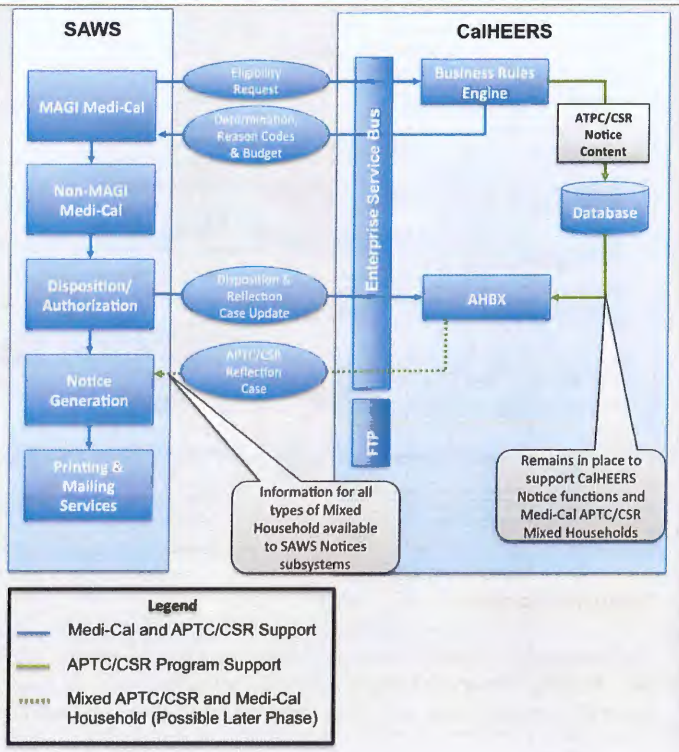


Criteria and Score	
County/Consumer Experience	●
Business Rules Maintenance Effort	○
Case Management	●
Uniform Policy Implementation	●
Mixed Household	○
County Operations	●
Implementation Risk	○
Implementation Cost	○

Notice Architecture

The diagram below represents an initial recommendation for the notices architecture under Option 2 in which the information returned from the CalHEERS MAGI Medi-Cal rule base is extended to include information required to generate notices such as Budgets and additional Reason Codes:

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES



1. The SAWS initiate and receive eligibility results from the CalHEERS provided business rules engine.
   a. The CalHEERS business rules engine is currently producing the information required for notice generation (e.g. Budgets) however it is stored within the CalHEERS database and may

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES

not be included in the current DER data structure. Under Option 2, the eligibility response message will need to be extended to include this information.

   b. Additional information provided within the eligibility response will also be helpful to CEW in situations when the eligibility result needs further analysis.

2. The SAWS incorporate the eligibility and verification results into their database.
3. The SAWS conduct additional case management activities such as review of the MAGI Medi-Cal result and potential eligibility for MAGI Medi-Cal.
4. Based on the final eligibility determination, the SAWS notice subsystems assemble the content into a viewable and printable format.
   a. Note: Under this architecture CEW will have the capability to view notices prior to distribution as they could prior to implementation of the ACA if the SAWS elect to implement this functionality.
5. Notices are transmitted to the County printing and mailing services. CEW will also have the capability for local office printing if this functionality is implemented with the SAWS.

Mixed Household Notices

During discussions on notice generation within the SAWS, the CalHEERS project team noted a need to be able to access MAGI Medi-Cal and mixed household notices. Several options are available to address this need based on identified use cases. For example, notices could be transmitted in bulk via FTP transfer, however this will increase infrastructure costs. Additional options include creating a federated notice service for CalHEERS staff to retrieve notices on an ad-hoc basis. Further analysis and information on CalHEERS notice access requirements is required to identify a candidate solution.

Members of the First Data assessment team have supported several HBE and ACA Medicaid implementations outside of the State of California; we are not aware of any of these projects currently providing combined notices for mixed households. Due to the complexity of this functionality we recommend that support for mixed household notices be implemented as a later phase of the project. The mixed household notices solution will need to address the following concerns and undoubtedly others that will be identified during the design phase:

- Aggregating the information to generate notices

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES

- Method of data transmission such as "snippets" of pre-generated notice text or leveraging existing case data replication mechanisms
- Timing of the transmission of required notice data between systems to avoid duplicate notices
- Creation of templates capable of addressing the various combinations of mixed households

We recommend that a design team be assembled as resources are available to create use cases that identify the various scenarios of mixed household notices and sequence diagrams that incorporate timing of notice generation. This information is critical to determine the optimal system(s) in which to generate mixed household notices as well as coordinating data transmission.

Division of Functionality

A high-level break down of the distribution of functionality is:

CalHEERS

- Maintains the "gateway" to the Federal Data Services Hub
- Maintains APTC/CSR and MAGI Medi-Cal business rules and support for applications submitted to CalHEERS by the counties
- Deploy and maintain individual web services for electronic verification and the State Verification Plan
- Deploy and maintain individual web services for eligibility determination
- Maintain eHIT and VIED workflow functions for Medi-Cal applications submitted through the Covered California portal and to support CalHEERS programs

SAWS

- Use existing SAWS workflow to coordinate the various eligibility related processes such as the following:
  - ✓ Notices

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES

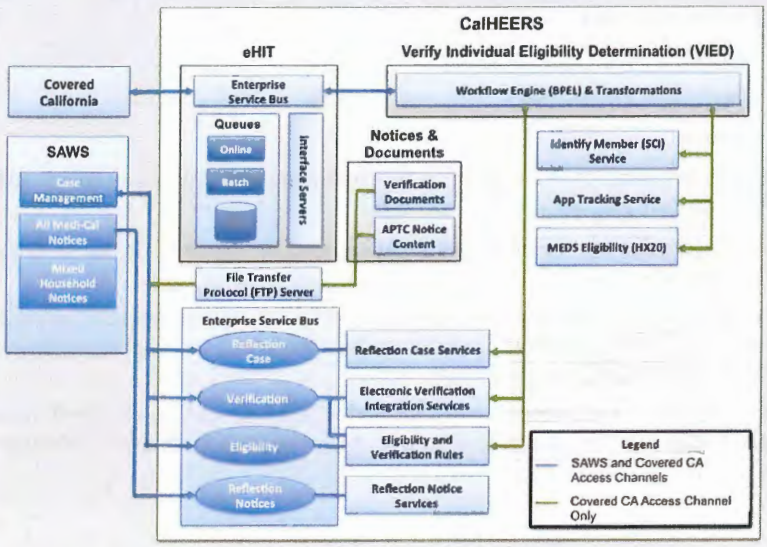
- ✓ Renewals
- ✓ Redeterminations
- ✓ Negative Action
- ✓ Cost of Living Adjustment
- ✓ Electronic verification

- Use application logic to form message requests that comply with CalHEERS data integrity and business requirements.
- Development of business level error handling, such as incorporating an eHIT Alerts capability within the SAWS systems.
- In order to support the Covered California Service Center and reporting needs, the SAWS will continue to transmit data to CalHEERS (Reflection Cases); this data transmission is not part of the eligibility and verification process.

The diagram below represents a conceptual architecture for Option 2 in which the current business services utilized by VIED (e.g. verification and eligibility) are modified for direct integration with the SAWS:

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES

Option 2 – Conceptual Architecture (MAGI Medi-Cal Functions)



The following provides a list of the application modifications between the current architecture and Option 2:

- Notices
  - ✓ **APTC/Notices:** Notice functionality remains within CalHEERS support programs other than Medi-Cal
  - ✓ **Medi-Cal Notices:** MAGI Medi-Cal notices content generation and document assembly are relocated to the SAWS

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES	
	✓ **Reflection Notices:** Mechanism for CalHEERS to retrieve MAGI Medi-Cal notices from the SAWS for use by their Service Center and to support the Portal • VIED ✓ VIED remains in place to serve the Covered California access channels ✓ SAWS no longer utilizes VIED to access backend business services (e.g. verification and eligibility) • **Business Services** - Web services currently accessed through VIED are made directly accessible to the SAWS ✓ **Reflection Cases:** Data access services to create and update reflection cases are placed on the externally facing ESB. ✓ **Electronic Verification:** A verification service is established that retrieves data from third party sources (e.g. FDSH, EDD). To avoid multiple service calls, we recommend that the service also run the retrieved verification data through the CalHEERS State Verification rule base. The SAWS will need both the verification results and the verification data for notice generation. For example, the results of the Non-ESI MEC (e.g. TRICARE) service are often required within denial notices. ✓ **Eligibility:** The eligibility business rules service is made available for direct access. The service will also need to be modified to include information required to generate notices within the eligibility determination message response (e.g. budgets). • **MEDS/DHCS:** At this time no anticipated changes have been identified to the current MEDS services.
Pros	• The SAWS will be responsible for maintaining the work flows in their systems introducing a higher degree of independence to implement business practices based on local needs. • CEWs will have the ability to access the CalHEERS BRE through SAWS as needed. • Localizing the eligibility workflow within the SAWS reduces the need for coordinating changes

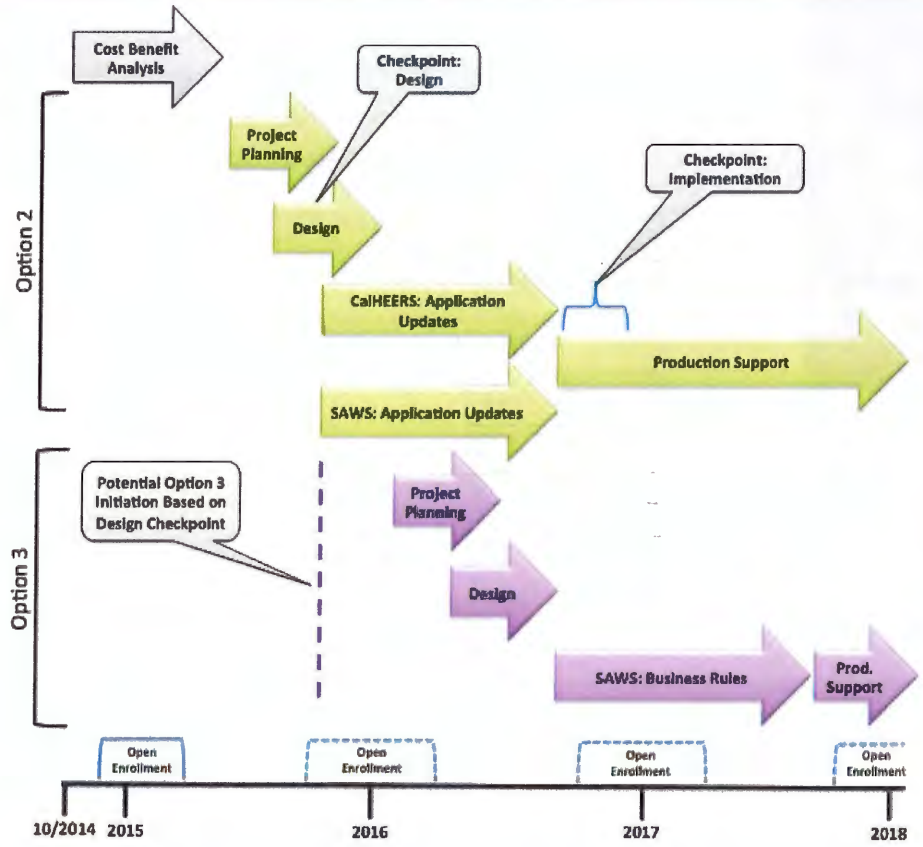
OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES

among the three SAWS and CalHEERS and increases speed of change.

- Provides counties an improved ability to detect Non-MAGI cases more easily.
- The architecture provides better controls to ensure that the program benefit hierarchy is maintained (e.g., Aged Blind Disabled individuals in Non-MAGI, even if they financially qualify for MAGI).
- The eligibility process is expedited by continuing to utilize the eHIT business rules that contain the policies for both MAGI Medi-Cal and APTC/CSR.
- Improves control of notice mass printing to avoid duplicate notices (e.g., notice per benefit month) and distribution of notices in the various threshold languages
- Localizing Notice generation within the SAWS improves the ability to support mixed households as their current data models support APTC/CSR, MAGI Medi-Cal and Non-MAGI Medi-Cal
- Minimizes the overall amount of transactions from the current eHIT architecture by eliminating the need for the following steps:
- DER
- Disposition
- Error report
- Notice transfer (pending design sessions to determine need for CalHEERS staff to access notices) reduces the size of several transactions by reducing the number of times case demographic data is transmitted between the SAWS and CalHEERS.
- Helps to mitigate the impact of the daily FDSH outages that occur during the SAWS batch windows. For example, the SAWS could implement a process to request electronic verifications outside of the FDSH outage windows to pre-populate the electronic verification data cache within CalHEERS (CR 9495). This approach would make the electronic verification data available to SAWS while running their EDBC batch cycles even during FDSH outages. The impact to online electronic verification requests during FDSH outages would remain unless the consumer's information had been

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES	
	previously stored within the electronic verification cache. • Environments management is simplified within CalHEERS. Option 2 also provides the capability for the SAWS to deploy local test environments prior to integration testing with CalHEERS.
Cons	• Modifications may be required to the Companion EDR message generation process • Requires implementation efforts across both the SAWS and CalHEERS teams. Data transmissions over a wide area network (WAN) are still required, which adds milliseconds of processing time to each eligibility determination. Although not an issue during regular processing, the added time is a consideration for COLA processing • Requires time and funding to modify rules and create workflow modifications within SAWS.
Time Frame	The completion of design and implementation efforts would require roughly eight – twelve months to implement Option 2. The figure below provides an estimated timeline for Option 2 and includes the estimated time period for incorporating Option 3 if the checkpoint evaluation deems necessary.

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES



Option 2 Implementation

- Much of the technical architecture required to implement Option 2 is already in place in the form of pre-ACA capabilities within SAWS along with several existing eHIT components.

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES	
Maintenance Approach	**Data Sharing** • SAWS will transmit case information updates to CalHEERS to support reporting and the Covered California Service Center. The current data synchronization process is simplified to a data replication process. • CalHEERS continues to push uploaded images related to MAGI Medi-Cal referrals received through the Covered California Portal. **Case Management Functions** • The SAWS perform ongoing maintenance of the case management functions. The SAWS will be responsible for maintaining the work flows in their systems along with any validation and transformations required to integrate with the CalHEERS business rules engine web service. • SAWS process changes to notices based on state provided guidance in the same manner as the pre-ACA notices. **Release and Change Management** • Reducing the scope of VIED by providing direct access to the CalHEERS BRE and FDSH should: ✓ reduce the number of releases and change management efforts that require coordination between CalHEERS and SAWS ✓ increase speed of change ✓ reduce overall complexity. • The SAWS can incorporate case management functionality independently of CalHEERS and other consortia based on their priorities and resource and can develop their independent release plans.
County/ Consumer Experience	• By maintaining the current eHIT workflow for use by the Covered California portal, online user experience is not impacted. • Consumers interacting with the Counties will likely see improvements in service through the following:

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES	
Score: Green	✓ Improved operational efficiency by allowing Counties control of their business processes. ✓ Expedited eligibility determinations in situations where consumers have provided paper-based verifications during office visits by avoiding potential processing delays from the FDSH. CEWs have reported a requirement to attempt electronic verification prior to paper verification; in the event eHIT errors occur the verification process is delayed. Counties have paper -based verifications availability in the majority of office visits as they are also applying for other programs (e.g. CalFresh). ✓ Ability to provide immediate feedback to in-person consumer encounters, such as preliminary eligibility results. ✓ Allowing access to the individual eHIT functions may provide options to add additional or real-time services on the County self-service portals.
Business Rules Maintenance Effort *Score: Yellow*	• As CalHEERS will continue to house the MAGI Medi-Cal rule base, maintenance of the business rules remains the same as Option 1; however the level of effort to communicate and coordinate business rules releases and impacts with Sponsors, Partners and stakeholders continues to be a high level of effort.
Case Management *Score: Green*	• The level of coordination effort among Sponsors, Partners and the Project will be less than that required in Option 1. Caseload management functionality and MAGI-Medi-Cal NOAs would be located at the local level and the Counties and respective Consortia can develop case management functions independently vs. coordinating among three Consortia and/or CalHEERS to implement simultaneously. • The reduced complexity required for change coordination due to the movement of the caseload management and NOA functionality, would also help simplify the change and release processes for Option 2.
Uniform Policy	• Leverages existing CalHEERS project processes to implement policy consistently.

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES	
Implementation *Score: Green*	
Mixed Household *Score: Yellow*	Provides improvements to manage mixed MAGI and Non-MAGI households while maintaining the benefits of the current eHIT architecture for mixed MAGI and APTC/CSR households: **Mixed MAGI and Non-MAGI:** • Localizing the eligibility workflow within the SAWS provides improved ability to detect Non-MAGI cases more easily. • The architecture provides better controls to ensure that the program benefit hierarchy is maintained (e.g., Aged Blind Disabled individuals in Non-MAGI, even if they financially qualify for MAGI). • The existence of both MAGI and Non-MAGI Medi-Cal case information within the SAWS facilitates Notice generation for this scenario of mixed households. **Mixed MAGI and APTC/CSR** • The eligibility process is expedited by continuing to utilize the eHIT business rules that contain the policies for both MAGI Medi-Cal and APTC/CSR. • Generation of combined MAGI Medi-Cal and APTC/CSR requires a carefully designed notices architecture. For example, an analysis effort needs to be undertaken to determine if all mixed households are tracked within SAWS. Case information for APTC/CSR may need to be extracted from CalHEERS via an additional web service.
County Operations *Score: Green*	• County Operations will have improved visibility into the eligibility and verification process through detail alerts assisting both regular case management operations and those performed by the County service centers • Ability to provide consumers with immediate feedback such as preliminary eligibility. • Control over the workflow to best align the eligibility and verification process with task function

OPTION 2 – LEVERAGE SAWS WORKFLOWS AND CALHEERS MAGI MEDI-CAL BUSINESS RULES	
	operations. • Ability to preview notices prior to print and mailing.
Implementation Risk *Score: Yellow*	• Requires coordination efforts between SAWS and CalHEERS to redesign current eHIT functionality • Requires SAWS to coordinate activities within their existing development priorities. • The implementation of Option 2 will require leveraging the following architecture components: ✓ Pre-ACA SAWS functionality along with several existing eHIT components. ✓ Updating the current eHIT technical architecture to provide backend services for electronic verifications, the State Verification Plan rules and Eligibility rules. The current eHIT architecture will need to remain in place to support consumers interacting with the Covered California portal. ✓ Modify the existing data integrations within SAWS to reflect the updated eHIT technical architecture (distinct services).
Implementation Cost *Score: Yellow*	• This option will require additional funding for both CalHEERS and SAWS. Enhanced funding that has already been allocated by OSI to the Consortia could possibly be leveraged to support this effort, but may not be sufficient to complete all tasks. A Change Request will also be required for Accenture for CalHEERS modifications.

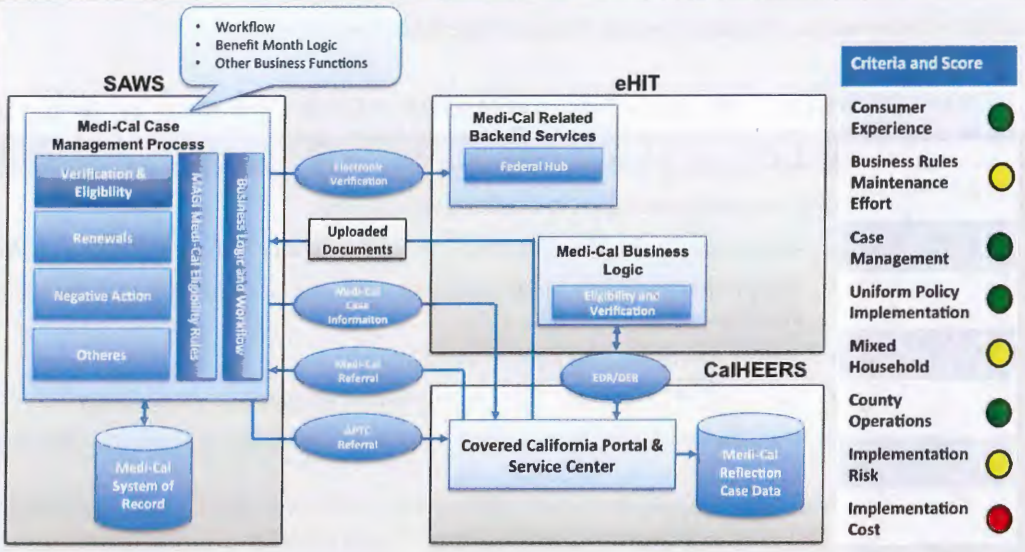
4.1.2.3 Distribute/Replicate MAGI Medi-Cal Business Rules

The table below provides a detailed overview of Option 3 for MAGI Medi-Cal rules.

TABLE 10 – OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS

OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS	
Proposed Solution	Option 3 further simplifies the eHIT architecture by: • Copying/replicating the MAGI Medi-Cal business rules within CalHEERS and SAWS • Removing MAGI Medi-Cal Case Management functions from CalHEERS, decoupling them from eHIT, and moving them to SAWS • Moving Notices of Action (NOAs) to SAWS • Modifying eHIT to create a simple and distinct electronic verification service • CalHEERS will continue to support MAGI Medi-Cal functions via the Covered California access channels In order to support the Covered California Service Centers, the Covered California portal and reporting needs, the SAWS will continue to transmit data to CalHEERS; this data transmission is not part of the eligibility and verification process. The following diagram illustrates at a high-level how eHIT and SAWS work together in Option 3 for MAGI Medi-Cal functions and displays this option's rating:

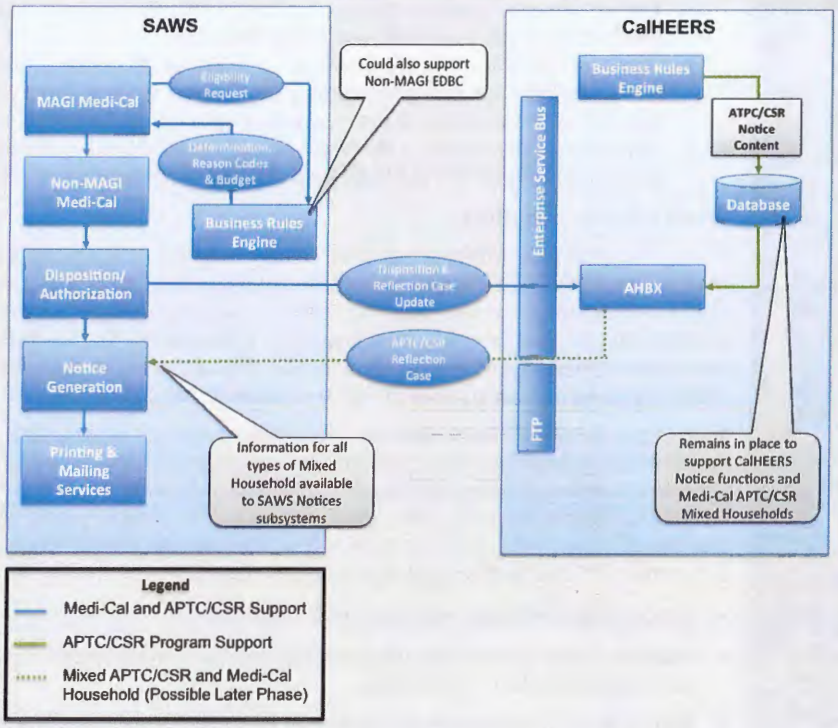
OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS



Notice Architecture

The diagram below represents an initial recommendation for the notices architecture under Option 3 in which notices for Medi-Cal and mixed households are generated by the SAWS from the results of the local business rules:

OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS



1. The SAWS initiate and receive eligibility results from their local business rules engines.
   a. The SAWS business rules currently provide functionality to support notice generation for programs other than MAGI Medi-Cal.
2. The SAWS incorporate the eligibility and verification results into their database.

OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS

3. The SAWS conduct additional case management activities such as review of the MAGI Medi-Cal result and potential eligibility for MAGI Medi-Cal
4. Based on the final eligibility determination, the SAWS notice subsystems assemble the content into a viewable and printable format. The current notice subsystems within the SAWS provide the CEW with the ability to preview notices prior to distribution.
5. Notices are transmitted to the County printing and mailing services. The current notice subsystems within the SAWS provide the CEW with local office printing.

Mixed Household Notices

During discussions on notice generation within the SAWS, the CalHEERS project team noted a need to be able to access MAGI Medi-Cal and mixed household notices. Several options are available to address this need based on identified use cases. For example, notices could be transmitted in bulk via FTP transfer however this will increase infrastructure costs. Additional options include creating a federated notice service for CalHEERS staff to retrieve notices on an ad-hoc basis. Further information on CalHEERS notice access requirements is required to identify a candidate solution.

Members of the First Data assessment team have supported several HBE and ACA Medicaid implementations outside of the State of California; we are not aware of any of these projects currently providing combined notices for mixed households. Due to the complexity of this functionality we recommend that support for mixed household notices be implemented as a later phase of the project. The mixed household notices solution will need to address the following concerns and undoubtedly others that will be identified during the design phase:

- Aggregating the information to generate notices
- Method of data transmission such as "snippets" of pre-generated notice text or leveraging existing case data replication mechanisms
- Timing of the transmission of required notice data between systems to avoid duplicate notices
- Creation of templates capable of addressing the various combinations of mixed households

We recommend that a design team be assembled as resources are available to create use cases that identify the various scenarios of mixed household notices and sequence diagrams that incorporate

OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS

timing of notice generation. This information is critical to determine the optimal system(s) in which to generate mixed household notices as well as coordinating data transmission.

Division of Functionality

A high level distribution of the major business functions between the SAWS and CalHEERS is:

CalHEERS/State Functions

- Intake and refer MAGI Medi-Cal applicants applying through the Covered California Portal will continue.
- Intake, determination, notices, and plan selection for ATPC/CSR applicants including those submitted by the counties.
- Maintain MAGI Medi-Cal business rules for use by the Covered California Portal and other CalHEERS functions.
- Maintain FDSH connectivity and provide access to a discrete electronic verification service accessible by the SAWS.
- Support efforts to implement MAGI Medi-Cal rules through mechanism such as:
  - ✓ Distribution of MAGI Medi-Cal rules guidance and policy documentation
  - ✓ Providing copies of the CalHEERS MAGI Medi-Cal business rules
- Transmit documents related to MAGI Medi-Cal intakes received by CalHEERS to SAWS.

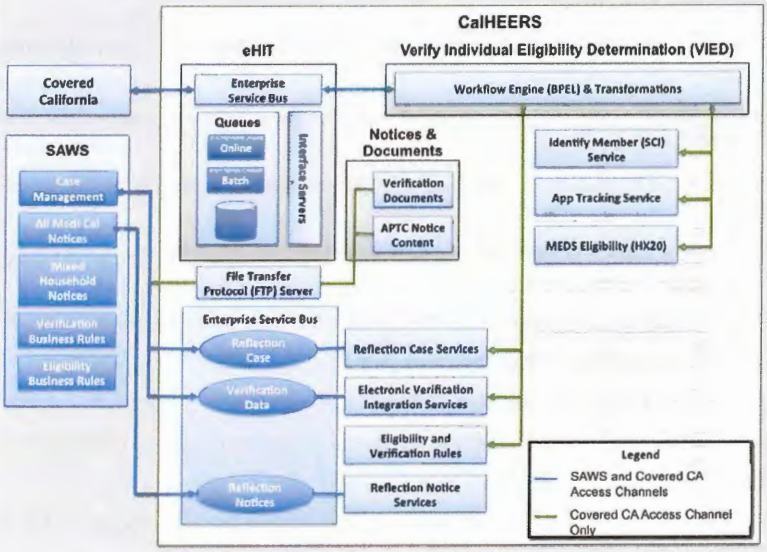
SAWS Functions

- Development and maintain business rules for MAGI Medi-Cal eligibility and the State Verification Plan.
- Complete MAGI Medi-Cal intake, determination and maintenance.
- MAGI Medi-Cal notice generation and distribution.
- Maintain the current referral interface for APTC/CSR transmissions to CalHEERS.

OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS

The diagram below represents a conceptual architecture for Option 3 in which the eligibility and verification business rules are localized within the SAWS:

Option 3 – Conceptual Architecture (MAGI Medi-Cal Functions)



The following provides a list of the application modifications between the current architecture and Option 3:

- Notices
  - ✓ **APTC/Notices:** Notice functionality remains within CalHEERS support programs other than

OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS	
	Medi-Cal ✓ **Medi-Cal Notices:** MAGI Medi-Cal notices content generation and document assembly are relocated to the SAWS ✓ **Reflection Notices:** Mechanism for CalHEERS to retrieve MAGI Medi-Cal notices from the SAWS for use by their Service Center and to support the Portal • VIED ✓ VIED remains in place to serve the Covered California access channels ✓ SAWS no longer utilizes VIED to access backend business services (e.g. verification data) • **Business Services** - Web services currently accessed through VIED are made directly accessible to the SAWS ✓ **Reflection Cases:** Data access services to create and update reflection cases are placed on the externally facing ESB. ✓ **Electronic Verification Data:** A verification service is established that retrieves data from third party sources (e.g. FDSH, EDD). The electronic verification data will be run through the SAWS local State Verification Plan rule bases. • **MEDS/DHCS:** At this time no anticipated changes have been identified to the current MEDS services. If Option 3 is implemented after implementation of Option 2, many of the services noted above will already be in place. Under the phased implementation the following updates would be required to implement Option 3: • Modify the Option 2 verification web service to not call the CalHEERS verification rule base. Remove data elements related to the State Verification Results. • Potentially decommission the CalHEERS provided externally facing eligibility rule base web service.
Pros	**General** • Provides control to the Consortia to implement workflows and user interfaces that align with their

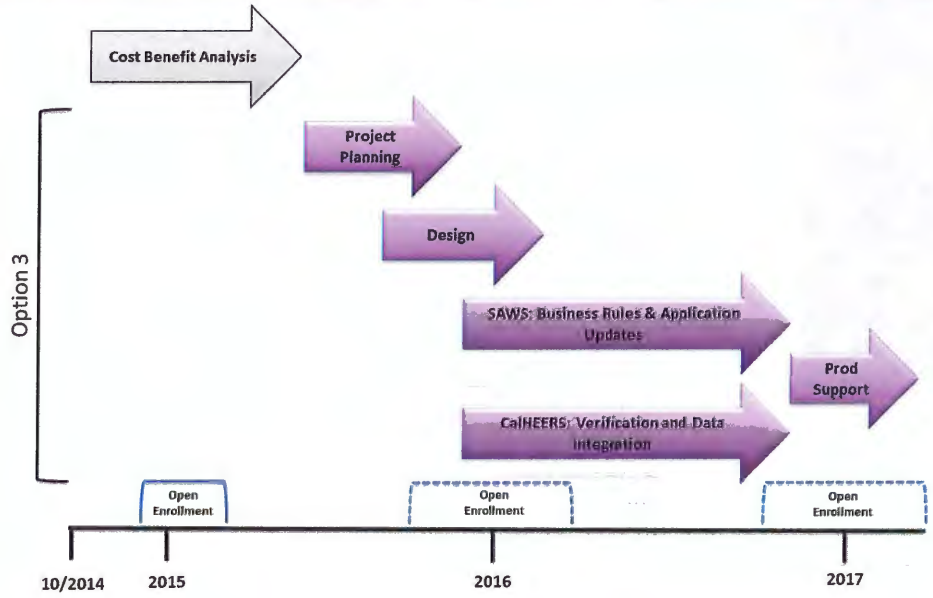
OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS

specific business processes.

- Provides improved performance and control for the SAWS to implement business rules that return results data (e.g. budgets, reason codes).
- Allows for fully integrated case maintenance across all programs currently supported by the Counties.
- Provides better ability to develop workflow that integrates the MAGI and Non-MAGI eligibility determination process. Real-time, preliminary eligibility determination allows for streamlined business processes between the two programs.
- Reduces the overall transactions amounts by eliminating the need for the following steps:
  - ✓ EDR (Replaced by call to CalHEERS FDSH Gateway)
  - ✓ DER
  - ✓ Disposition
  - ✓ Error report
  - ✓ Notice transfer (Pending design sessions to determine need for CalHEERS staff to access notices)
- Improved control of notice mass printing to avoid duplicate notices (e.g., notice per benefit month) and distribution of notices in the various threshold languages.
- Localizing Notice generation within the SAWS improves the ability to support mixed households as their current data models support APTC/CSR, MAGI Medi-Cal and Non-MAGI Medi-Cal.
- CalHEERS does not perform data comparisons with the SAWS EDRs as the eligibility and verification process is contained with the SAWS.
- CEW will no longer have to utilize the CalHEERS application to synchronize data with their records.
- Provides some mechanisms to mitigate the impact of the daily FDSH outages that occur during the SAWS batch windows. For example, the SAWS could implement a process to request electronic verifications outside of the FDSH outage windows and pre-populate an electronic verification data

OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS	
	cache within their databases. This approach would make the electronic verification data available to SAWS while running their EDBC batch cycles even during FDSH outages. The impact to online electronic verification requests during FDSH outages would remain unless the consumer's information had been previously stored within the electronic verification cache.
Cons	• Time and cost required to modify rules and create workflow modifications within SAWS. • Would require a new data reconciliation process to synchronize SAWS and CalHEERS. • Multiple rule development and testing efforts would be required for the three SAWS and CalHEERS.
Time Frame	It is likely the time to implement this option would be the lengthiest of all options presented. The figure below provides a notional timeline for the implementation of Option 3:

OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS



Maintenance Approach

Option 3 presents the least complex approach since each Consortium will subsume the rules and caseload management functionality and maintenance into their existing application maintenance processes. The following points are noteworthy.

Data Sharing

- Data comparison with CalHEERS is no longer part of the eligibility process simplifying and reducing

OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS	
	potential errors in the same manner as Option 2. • SAWS will transmit case information updates to CalHEERS to support reporting and the Covered California Service Center. The current data synchronization process is simplified to a data replication process. • CalHEERS continues to push uploaded images related to MAGI Medi-Cal referrals received through the Covered California Portal. • Implement a reconciliation process to synchronize data between SAWS and CalHEERS where eligibility results potentially may be different. **Release and Change Management** • SAWS will be responsible for maintaining a release plan that applies required policy updates within required timelines.
County/ Consumer Experience *Score: Green*	• Consumers accessing through the servicing County and were processed for MAGI Medi-Cal, they could perceive an improved consumer experience. • The Covered California Portal continues to provide online capabilities to MAGI Medi-Cal consumers.
Business Rules Maintenance Effort *Score: Yellow*	• The level of effort to communicate and coordinate business rules releases and impacts is less by leveraging existing SAWS processes. • The level of effort to coordinate business rules across four systems is higher than Option 1 and 2.
Case Management *Score: Green*	• The SAWS perform ongoing maintenance of the case management functions. The SAWS will be responsible for maintaining the workflows in their applications along with integrations with their local business rules implementations. • SAWS process changes to notices based on state provided guidance in the same manner as the pre-ACA notices.

OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS	
Uniform Policy Implementation *Score: Green*	• Leverages existing SAWS project processes to implement policy consistently.
Mixed Household *Score: Yellow*	**Mixed MAGI and Non-MAGI Medi-Cal** • Localizing all steps of the eligibility and verification process provides improved ability to create workflows that address both MAGI and Non-MAGI Medi-Cal households. • The existence of both MAGI and Non-MAGI Medi-Cal case information within the SAWS facilitates Notice generation for this scenario of mixed households. **Mixed MAGI and APTC/CSR** • SAWS will need to continue integration to eHIT to support APTC/CSR applications received by the counties and for mixed households. • Generation of combined MAGI Medi-Cal and APTC/CSR requires a carefully designed notices architecture. For example, an analysis effort needs to be undertaken to determine if all mixed households are tracked within SAWS. Case information for APTC/CSR may need to be extracted from CalHEERS via an additional web service.
County Operations *Score: Green*	• CEWs would have a single system of record to manage service delivery. • Service Center Representatives will still have access to MAGI Medi-Cal information to aid in servicing customers.
Implementation Risk *Score: Yellow*	The implementation of Option 3 will require leveraging the following architecture components: • A majority of the technical architecture required to implement Option 3 can be leveraged from pre-ACA SAWS functionality along with several existing eHIT components. • Updating the current eHIT technical architecture to provide backend services for electronic verifications, the State Verification Plan rules and Eligibility rules. The current eHIT architecture

OPTION 3 – DISTRIBUTE/REPLICATE MAGI MEDI-CAL BUSINESS RULES AND WORKFLOWS TO SAWS	
	will need to remain in place to support consumers interacting with the Covered California portal. • Modify the existing data integrations within SAWS to reflect the updated eHIT technical architecture (distinct services). However the following implementation risks have been identified: • Requires coordination efforts between SAWS and CalHEERS to redesign current eHIT functionality. • Requires the development of MAGI Medi-Cal rules within the SAWS systems. • Requires SAWS to coordinate activities within existing SAWS development priorities.
Implementation Cost *Score: Red*	• Due to the duplication of development and maintenance efforts of the three Consortia and the eHIT modifications needed - Option 3 is anticipated to incur the highest cost.

4.2 Global Recommendations

The following recommendations should be considered regardless of where the MAGI Medi-Cal rules and workflows reside (i.e., in CalHEERS or SAWS).

Column Guide

- **Rec#** - This column contains the recommendation number
- **Category** – This column contains the finding/recommendation categories being addressed by the recommendation
- **Description** – This column contains a description of the recommendation, including the pros and cons of implementing it
- **Finding Reference** – This column contains a cross-reference to the related Finding number(s) from the tables found in the Assessment Observation section.
- **Priority** – This column contains the FGDS team's opinion on the priority for implementation. Priority is based on the following:
  - ✓ **High** – Implementation of recommendation is urgent for continued success and/or greatest immediate gain
  - ✓ **Medium** – Implementation of recommendation is important and should be implemented as timely as possible
  - ✓ **Low** – Recommendation will result in improvements, but implementation can occur as time allows

TABLE 11 – GLOBAL RECOMMENDATIONS

Rec #	Category	Description	Observation Reference	Priority
1	General	First Data recommends creation of a CalHEERS Strategic Vision. Use of a neutral facilitator will be important to encourage open and communication. Bring together a representative (but small) group of executive decision-makers from the Sponsors, the CalHEERS Project, partner organizations and OSI to discuss individual and mutual goals, and determine an agreed-upon alignment of goals that will be used to frame the strategic vision. Suggested timeframe: begin within 30 days and time box this exercise to no longer than 60 days.	G1, G2, G3, G4, G7, G8, G10	High

Rec #	Category	Description	Observation Reference	Priority
2	General	Create an enterprise-wide Governance Plan to encompass Sponsors, the CalHEERS Project, Stakeholders, and Partners. The plan will address: • Identification of all stakeholders and their roles and responsibilities. • Detail a federated decision-making process and identify decision-making authority for each stakeholder. • Define and document an appropriate escalation process. • Identify a supporting committee structure; create charters to include objectives and participants. This recommendation should commence within 30 days and will require a focused effort by a small cross- organizational team to drive it through to completion, and will also require commitment by the stakeholders to support the effort.	G1	Medium
3	Communication	Create an enterprise-wide Communication Plan that will encompass communication needs for all entities – Sponsors, Partners, CalHEERS Project. A need for comprehensive communication demands this recommendation also begin within 30 days. The plan will need to address the typical communication elements of what, when, who and how and will need to ensure it meets the needs of all stakeholders.	G1, G2, G3, G6, G10	High

Rec #	Category	Description	Observation Reference	Priority
		The effort will require a cross-organizational team to support and manage the recommendation. • Institutionalizing a formal communication plan will facilitate open and consistent sharing information with the team, improve communication, and result in more timely information dissemination and overall project efficiencies.		
4	General	• Review the change and release management processes and determine process improvement opportunities, such as timely sharing of information. • Inform and educate Sponsors and stakeholders of the processes. • Ensure the appropriate representatives are included in the process and invited to the meetings. We recommend this activity be assigned to the Project's PMO and be accomplished in a phased approach.	G9, G10	Medium
5	General	CalHEERS project, Sponsors and Partners re-evaluate the current priority of eHIT enhancements along with known defects to validate which items have a high value impact to County operations and the consumer experience. Based on this effort, plan and schedule the implementation of the priority items.	F4, F6, F7, F13	High

Rec #	Category	Description	Observation Reference	Priority
		This activity could be accomplished by the Program Coordination Committee with defined timeframes and objectives, and facilitation and management by the Office of Systems Integration. Recommend the exercise begin within 60 days.		
6	Functional	Complete deferred, missing and erroneous functionality in a timely manner. Identify if additional resources are needed to address "delivery capacity." Within the next 60 days, First Data recommends that CalHEERS create an improvement plan for the eHIT interface, with input from DHCS, SAWS, and Counties to prioritize the defect and change requests for the next 2-3 release cycles.	G9, F1, F2, F3, F5, F7 – F14, F17	Medium
7	Functional	Create an updated design methodology to ensure the development and design teams are communicating regarding design impacts that occur across the entire system. First Data recommends that Accenture appoint a Solution Architect resource whose primary purpose is to monitor and ensure the cross development teams designs, communication and defect impact trending are occurring.	F6	Medium
8	Business Operations	Comprehensive error handling and reporting was a commonly cited need during interviews to improve Medi-Cal processing. It is recommended that enhanced error handling and alerts be prioritized to help elevate the time to problem	F5, F11, F16, T6, T11, T12	High

Rec #	Category	Description	Observation Reference	Priority
		solve at the Counties and Service Center.		
9	Use Cases	Adopt Use Cases to improve documentation and establish standardized program policy implementation • First Data recommends the use of Use Cases as part of the design process with the eHIT interface. • The functionality flow of how the eHIT interface operates was unclear among all parties. • Improved documentation, with the utilization of Use Cases will allow all parties to reduce the amount of meetings, provide an explanation of how the eHIT interface should or does operate, and improve the effectiveness of communications. • The Use Cases could be used by stakeholders such as DHCS and CDSS Program staff to understand the impact of changes to policy on the automated systems, and would be a step toward uniform design and testing among CalHEERS and SAWS. • Use Cases and sequence diagrams should be generated as part of the effort to develop combined notices for mixed households to address data integration and facilitate an implementation that does not impact county operations.	G6, F1, F2, F4, F7, F12, T1, T3, T15	Medium

Rec #	Category	Description	Observation Reference	Priority
eHIT Stability and Performance				
10	Technical	Replace the eHIT custom queue with an alternate technology • The design quality issues of the custom queue appear to cause delays in the processing of the SAWS transactions. • Java Messaging Service (JMS) with a file store is recommended as alternate architecture to replace the custom queue developed by the CalHEERS team. • Accenture has commenced an initial implementation of this optimization documented in HP ALM item #11939.	T9	Low
11	Technical	Currently, Companion EDRs are not processed until all associated EDRs are received. This is in place to sequence the EDRs. It is recommended that a mechanism be evaluated that will allow VIED processing to commence on receipt of the first EDR. For example create a hash value (e.g., timestamp, sequence number, case, etc.) to re-sequence the EDRs on completion.	T4, T5, T11	Medium
12	Technical	Incorporate Oracle standard functionality and best practices into the eHIT architecture: • Evaluate system tuning for Services Oriented Architecture (SOA) Suite Business Process Execution Language (BPEL) dehydration store available in Oracle Fusion Middleware Performance Tuning Guide.	T9, T10, T11	Medium

Rec #	Category	Description	Observation Reference	Priority
		• Test implementation of Oracle Exadata Write-Back Flashcache if the database supporting the queue and SOA Suite are disk Input Output (I/O) bound.		
13	Testing and Support	Currently, the eHIT and SAWS support teams only have access to their respective system's transaction logs and message payloads. Troubleshooting will be more efficient if both CalHEERS and the SAWS teams have visibility into how all of the systems are handling message generation and translations. For example, the SAWS teams do not have visibility into the transformations CalHEERS makes to their submitted DERS. Having access the final message payloads allows for lower levels of troubleshooting such as "grey box" testing from both the SAWS and CalHEERS teams. It is recommended that some sort of mechanism be put in place in test environments that do not contain PHI/PII data to allow limited read only access to the various support teams.	F4, F5, F6, F7	Medium
14	Availability Reporting	CalHEERS to generate a system availability report: Containing all software and hardware outages, including web servers, application servers, databases, network, storage, monitoring/management servers, and other supporting IT servers, including active directory, file	T1, T17	Low

Rec #	Category	Description	Observation Reference	Priority
		servers, and identity management servers. Such system availability report will improve visibility of system performance to the teams outside of CalHEERS. Also, this report will help the CalHEERS Project establish trends with the components of the system that do not remain available.		
15	Performance Reporting	The CalHEERS project, sponsors, partners, and stakeholders need to define a metric to measure the ACA standard of real time determination.	T1, T3, T4, T17	High
Support of SAWS and CalHEERS Business Needs				
16	Reporting	• In conducting the eHIT interface assessment, the First Data team noticed that the majority of the eHIT interface reporting is based on technical CalHEERS system processing. • The business spends a significant amount of time trying to understand the technology processing rather than the business reality of the eHIT interface. • Business metrics are not easily available. • First Data recommends that the following reports be generated and shared with all parties: ✓ An end-to-end view (SAWS and CalHEERS) of the processing time period for the applications being processed. The average period of time from the initiation of an application	T1, T3, T4, T17	Medium

Rec #	Category	Description	Observation Reference	Priority
		to completion for all access channels. ✓ The total amount of errors that are preventing consumers from completing applications. ✓ The break out of errors by percentages. ✓ The percentage of errors that can be resolved by SAWS and by the County.		
Capacity Plan and System Operations				
17	Capacity Planning	Based on the limited information obtained during the assessment, the following is recommended for the CalHEERS Capacity Plan: Create a standard capacity planning template for use across the SAWS to ensure consistency among the following: • Common assumptions • Clear basis of calculations (e.g., inclusion of Companion EDRs) • Common timeline of information • Inclusion of processing increases once pre-ACA cases are converted to MAGI Medi-Cal • Inclusion of other health programs with potential MAGI Medi-Cal eligible consumers • Inclusion of both monthly and yearly periodic increases in eHIT requests (e.g., Monthly NOA Cut off, COLA) • Inclusion of estimations that	T15, T16, T17, T18, T19, T20	High

Rec #	Category	Description	Observation Reference	Priority
		may impact eHIT/VIED to address changes in DHCS policy which may result in new applications or transition of consumers between programs • Inclusion of transaction projections that may result from DHCS policy updates such as new applications or transition of consumers between programs. Although additional hardware has been purchased, the First Data team recommends developing a global capacity plan that includes these facets in order to better forecast and manage production operations. For example, the capacity plan is critical to the development of a capacity management strategy to allocate processing resources to the SAWS during pre-ACA recovery and renewals. First Data recommends reviewing the CalWIN Capacity Plan as a starting point for a capacity planning template as it contains many of the aspects noted above.		
18	Service Level Agreements	Given that portions of the eHIT processing time are dependent on interface partners' system performance (e.g. FDSH) it is recommended that a service level objective (SLO) instead of a service level agreement (SLA) be defined for monitoring a consumer's end-to-end process and experience. The SLO should correlate to the agreed upon measurement that is required	T24	Low

Rec #	Category	Description	Observation Reference	Priority
		for real time eligibility determination.		
19	Technical Architecture	Once the effective date-based data model is fully implemented within CalHEERS, it is recommended that use of Flashback recovery in Production be evaluated against the project backup and recovery plan. If sufficient backup and recovery capabilities are present through replication to the secondary site and/or through database archive logging, it is recommended that Flashback recovery not be enabled in Production. This will help resolve some of the database level errors that occasionally impact eHIT processing.	T21, T22	Medium
20	Technical	Change Request 9495, which when implemented, will cache FDSH calls will greatly reduce eHIT processing time. In the event the implementation of this change request is in jeopardy by Open Enrollment, the following alternate architecture could be evaluated: • Oracle Service Bus (OSB) provides an out of the box in memory cache service • Results previously retrieved are stored and utilized replacing an external service call (e.g. FDSH) The OSB results caching function can be quickly configured for a proof of concept test. The down side of this implementation over a database store is that without some coding efforts, the results cache is	T21, T22	Medium

Rec #	Category	Description	Observation Reference	Priority
		lost on reboot of the OSB instance.		
21	Operations	Occasionally, eHIT receives a burst of transactions from the SAWS for various reasons (e.g. SAWS side server failures). It is recommended that a procedure be put in place for the SAWS to communicate the release of large amounts of queued transactions to the CalHEERS Production Operations team. This will allow the CalHEERS team to better proactively manage spikes in resource consumption.	T23	Low
22	Operations	The FDSH has nightly scheduled outages that occur during the SAWS batch processing windows. During this period, electronic verification data is not accessible. An effort should be conducted to determine the impact EDR to processing during the FDSH outages such as errors and additional transaction processing from reattempts at electronic verification. CalHEERS should ensure that the SAWS operations teams are aware of the outages. First Data recommends the CalHEERS eHIT team send an email to the SAWS operations teams whenever an FDSH outage occurs that impacts eHIT. Additional measures may be required to queue interfaces to the FDSH during scheduled outages.	T23	Medium
23	Operations	Both the SAWS and CalHEERS have reported that working sessions between CalHEERS and individual SAWS integration teams have been effective at addressing errors. The First Data Team recommends that	F5, F7, F8, F9, F11, F13, T17, T23	High

Rec #	Category	Description	Observation Reference	Priority
		CalHEERS deploy support personnel on site at each of the SAWS project offices to expedite access to information on development specifications and to track production issues. These teams should be deployed until the current eHIT architecture or Options 2 or 3 have been stabilized.		
24	Operations	Due to the significant number of transactions with third party systems, the CalHEERS gateway (Oracle API Gateway) transaction logs are purged. Given the potentially large portion of time integration with the Federal Data Services Hub imposes on eHIT processing, we recommend determining a mechanism to preserve transaction information to support reporting, SLO and general system troubleshooting. In addition, CalHEERS should consider implementing their license for Oracle Business Transaction Monitoring (BTM), which provides data on transaction times between web service calls within the system. This information will help the CalHEERS team identify areas to target for optimization along with the impact of external system calls (e.g. FDSH).	T1, T4	Medium
26	Operations	CalHEERS explore the possibility for an exception to the CMS requirement for a single gateway to verification sources.	F14	Medium
Horizontal Integration				
27	Cross Program	DHCS has created web service	T25	Medium

Rec #	Category	Description	Observation Reference	Priority
	Assets	access to several functions within App Tracking to support the Covered California Portal. The SAWS may benefit from real-time access to App Tracking to support intakes conducted by their service centers. At a future date when resources are available, it is recommended to investigate integrating the App Tracking web services within SAWS such as during the implementation of the system updates required for Options 2 or 3.		
28	Cross Program Assets	At a future date when resources are available, it is recommended that the screening capability within CalHEERS be expanded to be more like that used for "quick sort" for those calling via telephone. This could refer consumers to the SAWS that may be eligible for non-Health programs such as CalWORKs and CalFRESH		Low

5.0 Assessment Observations

This section contains the complete results of the analysis outlined in the Approach / Methodology section. Each subsection addresses the areas evaluated and assessed.

5.1 Technical Observations

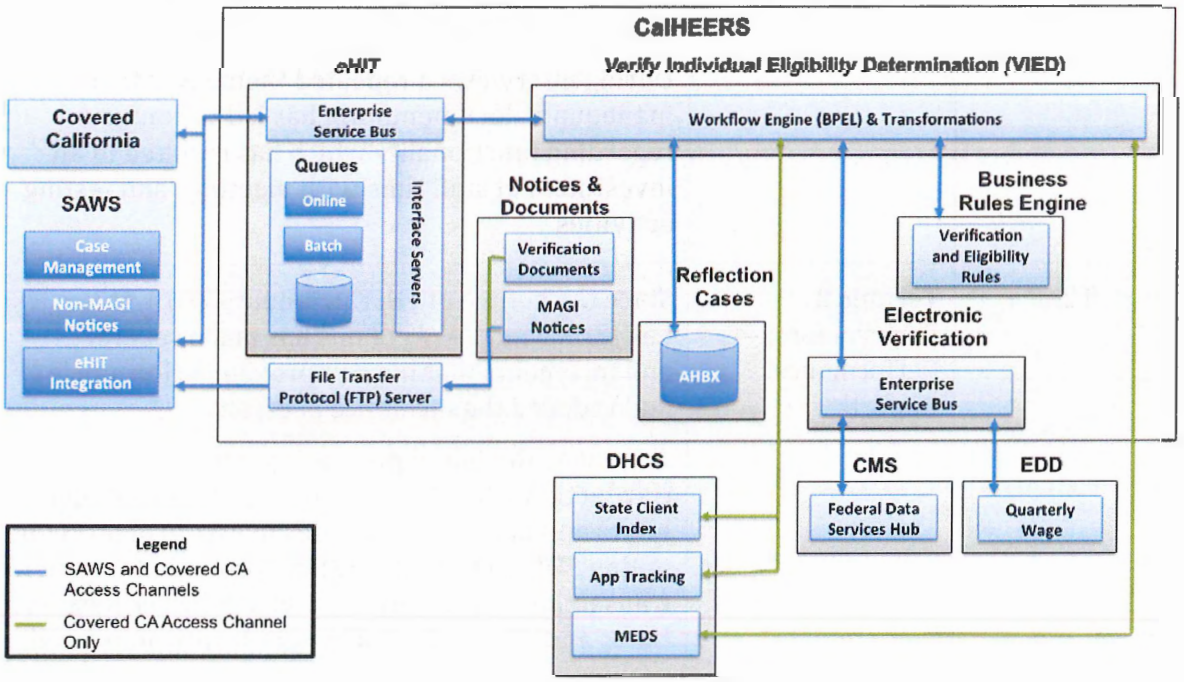
The functionality reviewed in this report covers eHIT along with its backend business services such as VIED and integrations with third party data sources (e.g. Federal Data Services Hub); although the term "eHIT" is frequently used to refer to the overall eligibility process, other CalHEERS components are involved. eHIT and its accompanying services are utilized by both CalHEERS and the SAWS to support a variety of health programs such as MAGI Medi-Cal and APTC/CSR. A high level overview of eHIT and its backend services is provided below:

- eHIT: Serves as the technical integration point to backend business services utilized by both CalHEERS and SAWS. eHIT provides the following technical functions:
    - Provides the data model (XML schema) to transmit case data between CalHEERS and the SAWS.
    - Workflow to track data integration such requests (EDR) and responses (DER), eligibility dispositions and referrals.
    - Handles the varying EDR formats including single and Companion EDRs.
    - Workload management to facilitate consistent performance between consumers (e.g. SAWS) as well as to prioritize online EDR over batch requests.
    - De-duplication of redundant EDR.
    - Transmission of documents such as notices and verification documents provided to CalHEERS.
- VIED: A backend workflow that coordinates the steps of the verification and eligibility process.
    - Enforces current policy to require electronic verification prior to use of paper-based verification.
    - Persists and retrieves case information within the CalHEERS case management system (AHBX).
    - Provides verification services such as access to electronic sources (e.g., FDSH and EDD) and capabilities to support paper based verifications in the event electronic verification is not available.
    - Integrates with the CalHEERS business rules engine for rules related to the State Verification Plan and Eligibility (e.g., MAGI Medi-Cal, APTC/CSR).
    - Applies benefit month and related effective date logic.

  - Provides transformations required to support integration with backend business services and CalHEERS components.
  - Multi-threading verification requests to the FDSH to reduce overall interface time with third party data sources.
- MEDS/DHCS Integration: CalHEERS integrates with MEDS for a variety of functions that primarily support Medi-Cal applications received via the Covered California Access Channels.
  - The interface with the Identify Member service (SCI) is utilized to identify a consumers existing CIN or establish a new CIN for new applicants.
  - CalHEERS interfaces with the App Tracking system to post pending applications.
  - An interface has been established to transmit eligibility transactions to MEDS.
- Electronic Verification: To comply with federal and DHCS requirements, CalHEERS provides the integration to several electronic verification sources.
  - Provides the authentication mechanism to the Federal Data Services Hub (FDSH) through the single Partner Key for the State of California to CMS).
  - Verifies and formulates requests to the FDSH comply with the federal required data model and security standards.
  - Integrates with the EDD for quarterly wage information.

The diagram below provides a conceptual architecture of components evaluated as part of this assessment:

Current State – Application Architecture (MAGI Medi-Cal Functions)



As part of the forthcoming Change Order 9495, eHIT will also provide a local cache within CalHEERS for verification data previously retrieved from the Federal Data Services Hub. This will help reduce eHIT processing times by avoiding repeated calls to the Federal Data Services Hub which can significant processing time to the verification portion of the process. This change may also help address errors created by the Social Security Administration (SSA) verification services contain security controls to block repeated incoming requests for the same Social Security Number (SSN).

Based on our understanding of the technical architecture and components of the eHIT interface, below are our technical observations:

TABLE 12 – TECHNICAL OBSERVATION TABLE

Observation #	Category	Description
eHIT Stability and Performance		
T1	Technical Documentation - General	The CalHEERS team directed First Data to the Deliverable 70 (technical design) series of documents however, they lacked detailed information regarding the technical design of the eHIT interface. Other related facets of CalHEERS such as the VIED and Individual Eligibility Determination documentation are well documented and appear to adhere to applicable best practices. The inconsistent level of detail amongst the eHIT and related documentation makes it difficult to understand how the verification and eligibility functions operate. During interviews a repeated theme was that inadequate documentation has led to confusion regarding functionality which has resulted in an investment of staff time with meetings and testing activities.
T2	Technical Performance – Performance Reports	Since the go-live of eHIT in January 2014, the CalHEERS and SAWS teams has made several enhancements that have improved performance and reduced the incidence of errors. At go-live, the initial processing times for transactions that did not fail validation were over 8 hours and average error rates in excess of 50% for online EDRs. The CalHEERS reported that in general transaction times were around 3 minutes. Response times and error rates have significantly improved

Observation #	Category	Description
		since go-live. • Note: The CalHEERS weekly status reports for the weeks of July 18th and July 21st denote that average response time has further dropped to 1 minute on average with a peak of approximately 5 minutes. In July, the CalHEERS Weekly Status report started including root cause analysis for increases in transaction response time. This information is helpful to create awareness around issues and corresponding corrective measures. Information on batch response times and error rates was not available to the First Data Assessment Team. Through various enhancements such as infrastructure tuning, additional validation and functional updates the response times and errors rates were reduced to the values below for the month of July: • Average Response Time: Approx. 1 Min • Peak Response Time: Approx. 5 Min • Average Cancel/Error Rate by SAWS: ✓ CalWIN – 33% (27% cancelations, 6% errors) ✓ LEADER – 15% (12% cancelations, 3% errors) ✓ C-IV - (0% cancelations, 11% errors) ✓ (Note: A cancelation is when an EDR in the companion set of EDRs reaches the "error" state, the remaining EDR benefit months are cancelled.) • The response times depicted above includes all functions that are a part of VIED (e.g., call the FDSH, California Verification Sources, and Eligibility Determinations) Additional performance graphs are depicted in Appendix C – eHIT Performance Graphs.
T3	Technical Performance –	Performance is measured differently between the

Observation #	Category	Description
	Performance Measurement	CalHEERS Project staff and the Counties. • The CalHEERS Project measures performance based on valid transactions that process through the eHIT interface. • The Counties measure performance as the time period to process an application from start to finish and resolving the eHIT errors, which measures all transactions collectively to complete the consumer experience. • During interviews with County and Consortia staff, eHIT response times were often compared with those from the pre-ACA SAWS EDBC response times. • Performance expectations are increased when a consumer is sitting in the office waiting for an eligibility result from the eHIT interface. Due to the lack of visibility into eHIT processing status, there is very little ability for a CEW to know what is causing the delay. The result is a frustrated CEW and dissatisfied consumer. Several change orders have been identified to improve this process such as CR 10119 to improve reporting automation and CR 7381 for near real-time error reporting. • Due to recent performance improvements, successful transactions have been improving over time; however, continual improvement is still needed to meet the business need of "real-time" determinations.
T4	Technical Performance – Performance Measurement	During the interview with the Accenture eHIT project team, it was stated that the longest portion of processing EDRs is the time required to interface with the FDSH verification services. • The need to interface with the FDSH in the event electronic verifications are required is a constant regardless of the location of the MAGI Medi-Cal business rules due to 42 CFR §435.949. • First Data requested a report from the CalHEERS eHIT team that provides a decomposition of the

Observation #	Category	Description
		percentage of processing time within the various operations performed by eHIT (e.g. FDSH interface, BRE processing). Due to the volume of outgoing requests to the CalHEERS integration Partners, the logs required to generate this report are purged on a regular basis. • Based on experiences with other State exchange systems with the FDSH verification services, interface response times from the FDSH vary greatly during various portions of the day and across the data services provided by CMS. • Response times from the FDSH can vary from a few seconds to upwards of 45 seconds to complete. If the statement that the longest portion of eHIT process is the FDSH requests, processing times for transactions that do not fail business level or data validations should drop dramatically with the implementation of CR 9495 – "Changes to the e-Verification Process (Caching the Values) for the Single Streamlined Application."
T5	Technical Architecture - Case Construct	The First Data Team identified that there are differences in the way the Consortia interact with the eHIT interface. • The design requirement of three or more transactions was described to CalHEERS in the initial eHIT joint application design sessions. However based on our interviews the development of the Companion EDR functionality with eHIT was not initiated until shortly before go-live. • The CalHEERS and SAWS systems application/case constructs are built to handle different benefit rules for each benefit program. For example, household composition and income/asset computation vary across benefit programs. • The CalWIN and LEADER systems process a

Observation #	Category	Description
		group of eHIT transactions based on effective months of eligibility, both retroactive and future (Companion EDR). • C-IV is also sending multiple months of eligibility but as separate transactions for each month. • The Companion EDR-based transactions have a higher potential for failure due to the fact that if any of the benefit month requests fail, the entire EDR will also fail. The single benefit month transactions used by C-IV will continue to process if one of the benefit month requests fail as each month is processed distinctly. • Additionally, it was reported that Change of Circumstances (CoC) entered from other programs with SAWS that occurred after submission of a client's MAGI Medi-Cal application are causing eHIT failures, as all of the data elements in an application must have the same effective date. • Various aspects of the eHIT interface create potential for "cancelations" such as data comparison of the CalHEERS and SAWS case information. CalHEERS is designed to overlay data provided by the SAWS; further analysis is required to understand the specific errors related to data synchronization. • Based on the CalHEERS Processing Reports for the first 15 days of July, 26% of the CalWIN transactions and 12% of the LEADER transactions are cancelled.
T6	Technical Architecture – Companion EDR Processing	Both LEADER and CalWIN transmit a group of EDRs to reflect a set of benefit months related to the consumer. The number of benefit months varies by the operating cycle within a month. For example, CalWIN transmits the Future Month and the Future Future Month after the NOA cut off period. In order to address the benefit month sequencing requirements of CalWIN and LEADER. eHIT is designed to start processing the EDR associated

Observation #	Category	Description
		with a Companion EDR once all of the benefit month requests are received. This design decision has the following impacts: • Response time may be increased while eHIT is waiting for subsequent EDRs associated with a Companion EDR. • Significant delays may be incurred if only a subset of the EDRs are transmitted from SAWS; while eHIT is waiting for remaining EDR transmissions, the Companion EDR is not processed. Case workers have initiated a work-around where they regularly view pending action reports to identify potentially "stuck" EDRs.
T7	Technical Architecture – Data Synchronization	On the daily error report for 6/24/14 provided by CalHEERS, 61% of the 7,341 errors were for validation, person number, primary case individual and other mismatches. This is confirmed by the 7/14/2014 error report provided by CalWIN which showed 73% of the 28,887 errors received were for mismatches, discounting cancellations of prior companion EDRs. • Errors include: primary contact person is changed, CalHEERS Case Person #X not found, Person Counts do not Match, and Combination of CalHEERSCaseNumber : sawsCaseNumber : Consortia : sawsCountyCode is not matching to CalHEERS record. ✓ CalHEERS has stated that the change of the primary contact is outside of the scope of eHIT. The SAWS provide the ability to change the primary contact within their applications. • Counties interviewed reported mismatch errors and the need to change information or cancel applications in CalHEERS in order to make cases synchronize. They are also executing EW20 and EW15 transactions directly into MEDS to force eligibility. • An additional source of errors occurs if a

Observation #	Category	Description
		consumer moves between Counties between the submission of an EDR and receipt of the following DER. Under the current implementation, the DER is returned to the new county servicing the consumer. This results in a processing error as the new county does not have the initial EDR (request) to match with the returned DER.
T8	Technical Architecture – Maintenance and Scalability	The eHIT interface utilizes a custom-built database queue mechanism to manage transactions between SAWS and CalHEERS. Two queues were designed to accommodate online and batch transactions. The development of the custom-built database queue has the following implications: • This custom-built database queue implementation does not utilize standard architecture pattern such as using a Java Message Service (JMS) queue. • The custom queue is used by the CalHEERS team to manage workload and resources for incoming transactions from both the SAWS and CalHEERS. • eHIT utilizes a technology to poll the queues that has additional overhead (XA) over lighter weight data integration protocols. • Accenture has completed development and is currently conducting performance testing on an update to the eHIT architecture that places a JMS queue between the database and the eHIT Interface Servers. This change to the architecture should reduce the amount of database activity and thread contention within the eHIT interface servers. Detailed information on this update to the eHIT architecture is located in HP ALM item #11939.
T9	Technical Architecture – Maintenance and Scalability	The VIED subsystem implements a service oriented architecture (SOA). The VIED architecture has implemented the backend services that compose the verification and eligibility process into distinct services:

Observation #	Category	Description
		• FDSH (specific services are available for each verification service) • Employee Development Department verification • MAGI Medi-Cal eligibility and State Verification Plan rules within the CalHEERS BRE, Oracle Policy Automation (OPA) • Integration with MEDS VIED appropriately uses the various Oracle integration products. Workflow components utilize Oracle Business Process Execution Language (BPEL) as it provides required transaction persistence and technical error handling. Interfaces to third party data sources (e.g. FDSH) and to OPA utilize Oracle Service Bus (OSB), which is optimized for synchronous transactions.
T10	Technical Architecture – Maintenance and Scalability	The Business Rules Engine (BRE) within VIED appears to have implemented the state verification plan, MAGI Medi-Cal and APTC/CSR rules in a single rule base. During interviews with Accenture, it was stated that the rules can be accessed as a service. Based on the information contained within the related design documentation, the verification and eligibility rules can be accessed separately from one another[1]. In order to validate that the actual implementation supports accessing specific rules, analysis of the OPA rule base is required.
Division of System Functionality between CalHEERS and SAWS		
T11	Workflow/Error Handling	The eHIT interface includes a limited workflow function to coordinate the steps of the VIED (e.g. Verification and Eligibility) process along with providing error handling. Based on the CalHEERS VIED Technical Design Document, a larger portion of this workflow appears to be provided via workflows configured with the Oracle SOA Suite. The eHIT and VIED process includes the following

[1] Individual Eligibility Determination Technical Design Document

Observation #	Category	Description
		steps: 1. SAWS initiate and transmit an EDR to CalHEERS. 2. The EDR is stored within the eHIT queue database. 3. As processing resources are available, EDRs are retrieved by the Interface Server database pollers. 4. Case data is stored within the Accenture Health Benefits Exchange (AHBX) application: a. Case data is placed in pre-VIED tables. b. Case data transmitted from the SAWS is compared to CalHEERS records. 5. Electronic verifications are then performed against the FDSH and other integration Partners such as EDD. 6. The CalHEERS BRE (OPA) is called: a. Business rules are assessed for the state verification plan. b. MAGI Medi-Cal eligibility rules are executed. 7. Response (DER) is transmitted to the SAWS from CalHEERS. VIED also contains additional workflows to support applications that are received via the Covered California access channels. For example, VIED also integrates with MEDS to coordinate the steps for File Clearance, App Tracking and Eligibility transaction posting to MEDS. These workflows are not part of the workflow that supports SAWS initiated eligibility (EDR). The overall process contains restart and error handling capability however interviewees have noted that unhandled exceptions exist. It is common for new systems (e.g., VIED) to require a period of stabilization to thoroughly identify and handle exceptions. Additionally, interviewees have reported that SAWS

Observation #	Category	Description
		did not implement conditional eligibility requirements and did not include exception-base user functionality for expedited and approval of cases.
T12	Workflow/Error Handling	The error codes and reporting for failed eHIT transactions is limited. In order for the CEW to be informed of a problem, the Counties must download and distribute reports from the CalHEERS SharePoint. Lack of visibility into eHIT transaction status and errors was one of the most commonly cited issues during interviews with the Counties and Consortia. The error reporting implementation creates the following impacts: • The current process for reporting errors is for CalHEERS to manually post an error report for each SAWS to the CalHEERS file server the day following the occurrence. • The SAWS are required to download these files, parsing them by County and distributing them to the Counties. Counties are manually checking errors against cases that have not received a response. • Distribution of the error reports does not appear to be widespread and in some cases has only been initiated in the last 90 days. • The Counties, which have just recently started receiving these error reports, found them to be difficult to decipher. • Of the 29 reasons for receiving an error, 21 errors cannot be resolved by the Counties. (CalWIN Guide to eHIT Errors) • CR 7381 (eHIT 3.0) will create some functionality to allow for near real time alerts within the SAWS.
Support of SAWS and CalHEERS Business Needs		
T13	System of Record	The VIED design documents are written from the perspective that CalHEERS is the system of record for MAGI Medi-Cal cases. The SAWS operate and have stated in interviews that their systems are the

Observation #	Category	Description
		point of record for MAGI Medi-Cal cases. As per the California Welfare and Institutions Code 10823. These differing design perspectives may be a source of the confusion and functionality misalignment between SAWS and CalHEERS.
T14	Notices	Based on interviews with the SAWS operations teams, the time required to generate and print notices is lengthy due to a complex business process. The following provides the sequence of the "hand offs" that encompass the steps related to the generation of notices 1. SAWS transmits eligibility request to CalHEERS (EDR Transaction #2). 2. CalHEERS processes eligibility and verification functions and returns response (DER Transaction #3). a. Content required to subsequently assemble the notice is populated in the CalHEERS database. 3. CEWs conduct various activities such as reviewing the eligibility determination and potential Non MAGI-eligibility. Once approved, SAWS transmits the disposition (#4 Disposition) to CalHEERS. In addition to the approval, supplemental information such as the CEW contact information is supplied to CalHEERS. 4. CalHEERS receives the case disposition data and associates the DERs authorized by the SAWS with the previously generated notice content (Step 2). 5. CalHEERS batch reads the disposition information and generates the notices requested by the SAWS (Transaction #7) a. C-IV and LEADER receive Portable Document Format (PDF) while CalWIN receives Printer Control Language (PCL) files. b. CalHEERS also transmits any images associated to the consumer received during application intake (e.g.

Observation #	Category	Description
		verification documents). c. The transmission also includes a manifest file denoting the contents of the zip file. 6. SAWS receive the zip files from CalHEERS and prepare a subsequent file transmission to the print vendor. 7. Print vendor receives files and produces mailings. During an interview with one of the SAWS support teams, it was noted that this process could take up to seven days to complete. CalHEERS reports that typically notice generation requests are processed overnight. It is unclear what factor is driving the delay, potential sources are below: • If the eHIT transaction results in an error, the previously mentioned alert and analysis process will also delay notice generation. • If the CEW does not approve of the eligibility result in a timely manner, the subsequent notice is also delayed. • Batch EDRs will have two nights of processing: first night for EDR process and the second night for notice generation. The length of time between the eligibility request and notice mailing has implications for negative actions and timely notifications to consumers. Part of the delay in processing is the requirement to approve the eligibility determination within the SAWS triggering the disposition transaction and subsequent notice generation. This step is necessary under the current process to provide the CEW with an opportunity to view the MAGI Medi-Cal eligibility result and potentially run eligibility within the SAWS for Non-MAGI Medi-Cal. Counties also reported that since notices are sent every time there is an eligibility disposition there has been an increase in postage fees for the SAWS.
Capacity Plan and Infrastructure Architecture		

Observation #	Category	Description
T15	Capacity Plan - Estimates	Deliverable 33- O&M Manual contains a section on Capacity Management Planning. It primarily describes processes and procedures rather than provide a detailed capacity plan for CalHEERS. Deliverable 71 – Performance Test Plan contains pre-implementation volumetric data that indicate expected transactions of 1.9million MAGI Medi-Cal enrollments. Actual Exchange related functions were significantly higher than those projected prior to go-live creating and overall capacity issue which affected eHIT during peak periods during open enrollment.
T16	Capacity Plan – Ongoing Case Processing	The CalHEERS and eHIT operating volumes provide a sound starting point for the development of an ongoing capacity plan. As pre-ACA cases and functionality are currently served by both eHIT and SAWS, development of capacity plans requires development of a model that addresses these factors. The following transaction processing data was provided by the SAWS Consortia during the eHIT assessment: • CalWIN –Peak System volume (Nov. 15, 2013 – Feb. 15, 2014): ✓ EDR in a peak hour (20,625 batch; 10,871 online) ✓ DER transactions in peak hour (20,625 batch; 10,871 online) ✓ DISP in a peak hour (216,395 per Day) ✓ Update Transactions in a peak hour (1,220 inbound per day, 1,330 outbound per day) • LEADER Peak System volume (Nov. 15, 2013 – Feb. 15, 2014): ✓ EDR in a peak hour (13,400) ✓ DER transactions in peak hour (13,800) ✓ DISP in a peak hour (5,000) ✓ Update Transactions in a peak hour (1,000)

Observation #	Category	Description
		• C-IV - Peak System volume (Nov. 15, 2013 – Feb. 15, 2014): ✓ EDR in a peak hour (1,600) ✓ DER transactions in peak hour (3,300) ✓ DISP in a peak hour (3,600) ✓ Update Transactions in a peak hour (C-IV never has received an update transaction/CalHEERS researching) Comparing the volume requirements provided above is error prone due the differing granularity of the data (peak hour versus monthly). A method to collect a standard set of data is required to accurately combine and compare data among the SAWS Consortia and CalHEERS. As CalWIN and LEADER use Companion EDRs and have a nearly equivalent caseload it is expected that their system capacity estimates should not greatly differ from one another. The multipliers referenced above that CalWIN has applied to their capacity model may partially explain the differences in expected transaction projected volumes. Further effort is required to gather consistent metrics across the SAWS. Additionally, the CalWIN capacity plan addresses the additional transaction processing once pre-ACA cases are supported by eHIT by applying a multiplier to their current actuals. Transaction processing reports the First Data Team received from other Consortia do not appear to include a multiplier to reflect additional processing for pre-ACA cases.
T17	Capacity Plan – Pre-ACA Recovery & Renewals	The actual eHIT capacity metrics do not reflect transaction processing to support transition of the Pre-ACA cases to ACA benefit codes. The recovery period will result in an increase in EDR transactions for a period of five months under the CalWIN operations plan. Information is not available on the recovery plans for the other two

Observation #	Category	Description
		Consortia. Based on the CalWIN Capacity Plan, pre-ACA cases will not be verified through the FDSH. Under the current VIED architecture it is not possible to bypass the interface to the FDSH resulting in the following: • Additional transaction process time incurred from FDSH response times. • Potential for verification failures if the data reported by consumers does not match records within the FDSH. For example if the data provided by a consumer is more current than that available through electronic verification, the CEW may have to re-trigger an EDR with an administrative verification. The CalHEERS project team has expressed interest in being able to run separate verification and eligibility processes to support their operations.
T18	Capacity Plan – Renewals	Starting in October 2014, or when renewal functionality is implemented, monthly batch cycles will begin incorporating consumers who enrolled after the initiation of the ACA. The CalWIN capacity plan assumes an increase in activity during the first cycle of renewals. CalWIN has broken down the ACA renewals into four waves across four months that assumes an initial increase in eligibility and verification with a subsequent drop off in activity as regular case maintenance activities commence (e.g. incorporating change of circumstances).
T19	Capacity Plan – Transition of LIHP and Healthy Families	The SAWS are currently in process to incorporate the cases from the Low Income Health Plan (LIHP) and Healthy Families programs into their systems. A portion of the individuals covered under LIHP and Healthy Families are potentially eligible for MAGI Medi-Cal. As these cases are not fully migrated to the SAW, their impact on eHIT processing is not reflected in current eHIT actual processing metrics.
T20	Capacity Plan – Initial ACA Intakes	To date, eHIT processing has been related to new application intakes. Pre-ACA cases are being held by the SAWS while policy and system functionality is

Observation #	Category	Description
		put in place to support ongoing case maintenance. The peak eHIT processing as reported by CalHEERS is 9,986 EDRs in a single hour. It appears that the updated CalHEERS capacity plan was based on historical peak processing and may not include additional processing required to support the inclusion of pre-ACA cases and inclusion of other programs that are still underway such as LIHP and Healthy Families. The updated capacity plan used to develop the configuration of the expanded infrastructure is based on the actual recorded EDR processing peak. According to an Oracle provided report, the infrastructure is designed to support 3 times more than the observed volumes or just under 30,000 EDR per hour. The capacity plan uses actual data and is based on a standard linear extrapolation of the data. This level of processing volume aligns with the aggregated transaction volumes provided in finding T16. An updated capacity planning model is required to validate capacity needs and develop a workload management schedule across the three SAWS. Without a consistent set of metrics, assumptions and working definitions used in the capacity plans across the SAWS, it is not possible to generate an accurate capacity plan for eHIT transactions. Although additional infrastructure has already been purchased to support eHIT and other CalHEERS functions, it is critical that an accurate capacity plan is generated to plan for periodic increases in eHIT capacity via the CalHEERS private cloud and to schedule large workloads across the SAWS to avoid resource contention. This information is required by the CalHEERS Production Support team to proactively manage workload demands throughout the monthly and yearly cycles.
T21	Batch Processing – Federal Data Services Hub	The FDSH has numerous scheduled outages that reflect maintenance on the backend systems (e.g. SSA). As per the CMS published document TDS Availability Document Number 57333, the FDSH is

Observation #	Category	Description
		not available during the following daily scheduled maintenance periods: • Social Security Administration - 8:00 PM to 2:00 AM (PST) • Internal Revenue Service – 9:01 PM to 3:59 AM (PST) CMS did not communicate the scheduled outages to FDSH consumers until late in the summer of 2013. In addition, many of the other FDSH verification services have various weekly scheduled outage periods. The IRS and SSA scheduled outages are particularly impactful as they occur during the initial phases of the SAWS nightly batch processing windows; this is typically the time period when EDBC cycles are run. The results of the EDBC cycle drive numerous downstream batch cycles that occur later in the nightly batch schedule. The FDSH scheduled outages are particularly impactful for nights that have heavy processing requests (e.g., NOA Cut Off) and for future mass update operations such as COLA. eHIT will provide a "not verified" based response if an EDR is processed during FDSH outage windows. Data was not available to the First Data Assessment Team to determine the impact of FDHS outages on increased EDR due to electronic verification re-attempts. As the VIED workflow incorporates both verification (e.g. FDSH) and eligibility, the ability to schedule various batch processing cycles around the CMS scheduled outages is limited. For example, the ability to run verifications during the day while the FDSH is available and then later run eligibility against the eHIT BRE would better accommodate CMS scheduled outages. Based on the interviews with the CalHEERS eHIT team and the SAWS, neither system is queuing EDRs that are transmitted during the FDSH scheduled outages for later processing once the verification services are available. It is unclear what impact the

Observation #	Category	Description
		FDSH has on eHIT errors and batch transaction processing times. The eHIT interface continues to pass through electronic verification requests to the FDSH during the scheduled outage periods. The First Data Team was not able to determine if the SAWS support teams are aware of and manage workload to avoid the outages. The nightly SSA schedule maintenance period occurs during the beginning portion of the SAWS nightly batch cycles. Follow on analysis is required to determine if EDR processing during the scheduled FDSH outage window is contributing to errors and verification failures.
T22	Technical Architecture - Infrastructure	The updated CalHEERS Capacity Plan was developed using actual production data and utilization based on the current eHIT implementation. Several CRs along with some additional identified optimizations will further improve transaction processing throughput in addition to that provided by the infrastructure upgrade. For example, the following modifications are currently planned: • CR 9495 will implement a caching mechanism for FDSH information resulting in a reduction in overall processing time per transactions. • Re-calibrating size of virtual machines to improve performance and manageability. • Adding additional SSL connection capacity; primarily for the portal but may also be used by secure eHIT transactions reducing the possibility of connection timeouts. • Modify the current custom database queue to utilize out of the box Web Logic JMS functionality. • Partition and tune VIED BPEL database repository (SOA repository). • Implement Exadata Write-Back Flash Cache to reduce disk I/O contention.

Observation #	Category	Description
		• Implement Infiniband firewall for low latency communication between the CalHEERS application (Exalogic) and database (Exadata) tiers.
T23	Operations	There are situations in which EDR and other transactions are queued in the SAWS and released in large bursts of requests. Transactions may be queued at the SAWS for a variety of reasons including server failures or other operational issues. The CalHEERS team reported that they do not receive advanced notice that the SAWS will be releasing large bursts of transactions from their systems. For example, CalWIN experienced a significant increase in EDR response times on July 11th and 12th which may be related to a release of a large amount of queued transactions within their systems. Without notice, the CalHEERS Production Support team can only reactively address transaction processing bursts.
T24	Service Level Agreements	The proposed eHIT SLA was developed by the CalHEERS IV&V vendor with a focus on processing transactions through the CalHEERS. The First Data team learned through interviews that a larger concern exists with the consumer experience and the end-to-end processing time of the applications process.
T25	MEDS Impact	Based on a review of the design document BSD2.4.0 – CalHEERS SAWS MEDS Interface, our analysis did not indicate any impacts on MEDS such as changes in transaction volumes or integration with CalHEERS and SAWS. The interface between CalHEERS and MEDS primarily supports MAGI Medi-Cal eligibility initiated under the Covered California access channels; all three of the presented options do not directly change these functions. Changes to the File Clearance process currently under evaluation by DHCS and related stakeholders may impact the Identify Member interface utilized by CalHEERS under all three presented options.

Observation #	Category	Description
		Additionally, DHCS has created several new access points to SCI, App Tracking and MEDS to support CalHEERS that may also be useful to other state systems.

5.2 Functional/Business Observations

The purpose of this section is to describe our observations as to the design and implementation of the eHIT interface from a functional and business perspective. As a general finding, the implementation of the eHIT interface has exceeded projected transaction volumes. The interface is also currently going through a "stabilization" phase, which is to be expected with any new system. However, almost without exception, everyone the First Data team interviewed thought the eHIT interface was overly complex for what needed to be accomplished from a business perspective.

It is also noteworthy to mention that it is difficult to draw a distinction between how the eHIT interface or CalHEERS functionality supports the business. Through our interview process, interviewees provided many examples of areas they felt did not fully support their business processes, and many are due to missing eligibility rules, such as the aid code hierarchy, known Change Requests and defects. General CalHEERS observations unveiled during interviews that are not directly related to eHIT were considered to be out of scope for this assessment and is not included in this report.

Below are our detailed observations in this area. The functional/business observations will begin with the letter "F" to distinguish them from other observation (e.g., F1).

TABLE 13 – FUNCTIONAL/BUSINESS OBSERVATIONS TABLE

Observation #	Category	Description
F1	Functional Design	During the development of the eHIT interface, a design decision was made to leverage the eICT (electronic Inter-County Transfer) interface jointly developed and deployed by the SAWS as a design starting point for the eHIT interface. • The eICT process is a point in time transfer of data from one SAWS system to another. • The eICT design does not include ongoing temporal data regarding history or future eligibility. This paradigm was carried into the eHIT design and is inconsistent with the highly time-based nature of eligibility processes. • Evolving a time-oriented data model and

Observation #	Category	Description
		ability to handle data changes within cases has negatively impacted County business operations and has initiated numerous changes to the eHIT schema.
F2	Functional Design	Interviewees repeatedly commented on an overarching theme: the eHIT interface is overly complex. Many believed that eHIT does more than ever envisioned. Interviewees also stated that functions such as Notices of Action, and Consumer Protection Programs should have remained in the SAWS systems.
F3	Functional Design	CEWs have very limited visibility into the eligibility determination and budgeting factors, which limits their ability to troubleshoot potential determination errors or discuss specific case issues with their clients.
F4	Functional Design	The need to coordinate and gain consensus of proposed design changes slows the Project's and Consortia's ability to adapt their systems. Additionally, the need to have eHIT releases deployed to all SAWS and CalHEERS/eHIT simultaneously requires coordination across all four systems and delays can occur if any one of the four systems is not able to incorporate needed design changes on the same time frame as the others. All Consortia commented that the overall coordination of design, testing and deployment activities is much greater than anticipated.
F5	Functional Design Gaps	Design decisions resulted in a focus on the yearlong eligibility cycle of APTC versus the monthly ongoing eligibility and case management processes needed to support MAGI Medi-Cal. These design decisions have resulted in the following challenges: • There are few temporal data elements with beginning and ending dates. (Note: Change Request #9202 went into production August 1, 2014, to address income dates.)

Observation #	Category	Description
		• Since historical information is not currently displayed, it is difficult to track account changes. The transaction history log shows all data that was generated by the interface, not just the changes. • The requirement to send and process Companion EDRs serially was not included within the initial design. SAWS and CalHEERS report the need to process eHIT transactions time sequentially in order to ensure the most recent transaction is the "current" transaction. • CalHEERS eHIT interface currently has multiple issues with processing changing data elements such as previous County of residence or primary contact person, as indicated by error reports, identified defects, enhancements and County reports. For example: ✓ A change in residency (between Counties) sends case information and subsequent transactions to the new County as an update versus utilizing the ICT process, and without giving the original County a chance to properly transfer the case. This issue becomes a reporting issue for the County, which can only be resolved through a manual workaround. • During interviews with county staff, it was reported they have encountered data synchronization problems with the eHIT interface and MEDS. SAWS and counties describe scenarios where if one individual on a case is incorrect, the entire transaction fails including all other individuals associated with the case. For example, the workers reported that if the address is not specified for all individuals (including children), the EDR will fail.

Observation #	Category	Description
		✓ A complete set of information on the individuals in an application is required to determine the tax filer household, which is required for both MAGI Medi-Cal and APTC/CSR eligibility determination. As such some of the failures are based on required business level validations. ✓ Both the SAWS and CalHEERS are individual based for data tracking. Currently, the CalHEERS schema does create multiple records of an individual associated with multiple cases. • The design requires that all data elements be sent with every eHIT transaction. Transactions that change data, rather than identifying only the changed data elements with a begin/end date, must include all case data with every transaction. These additional data elements impact the performance of the interface. ✓ Month by month income records are required if an individual within an application is not found eligible for MAGI Medi-Cal and eligibility needs to be determined for APTC/CSR.
F6	Functional Design Process Issue	CalHEERS project interviewees suggested that a major reason for design issues and defects associated with the development of eHIT was related to development teams working independently and not thoroughly discussing functional design impacts. A cross team understanding of how functionality changes impact other parts of the CalHEERS system is not occurring on a consistent basis.
F7	Additional Functionality	In addition to the progress made over the past several months with stabilizing and improving the performance of the eHIT interface, several Change Requests are in various states of

Observation #	Category	Description
		implementation that should provide significant improvements to eHIT. However, additional functionality is still required.
F8	Business Operations	The complexity of the implementation of ACA has consumed resources (CEWs, technical resources, management) at an unanticipated rate. Many interviewees felt that the impact on County operations was not fully considered or understood during the design, development and deployment of CalHEERS. • County Welfare Directors stated that the implementation of the eHIT interface has taken more time by all levels of staff, including management and executives, than any other initiative in the past, including welfare reform (Personal Responsibility and Work Opportunity Reconciliation Act of 1996).
F9	Business Operations	Counties and the State are performing manual intervention as a result of CalHEERS missing or incorrect functionality. For example: • At the initial implementation of eHIT, the CalHEERS case management system had limited ability to track time based data. CalHEERS is incrementally adding a temporal based data model. • Limited ability to detect and resolve errors within the EDR process.
F10	Business Operations	Change DER (Determined Eligibility Result) eHIT transactions do not identify specific data that is being changed at a granular level. • This requires workers to compare, element by element, information currently in the system to that provided in the change DER. • For example, if a customer's email address changes, a worker must compare the information provided in the DER to the SAWS systems' 30 elements that constitute the

Observation #	Category	Description
		demographics node to determine what the change was. • The data comparison process is very time consuming for CEWs and is a source of eligibility processing errors.
F11	Business Operations	• Interviewees reported that CalHEERS does not produce a confirmation message after a CEW submits a transaction for eligibility. Based on our review of the eHIT design documentation an acknowledgement is transmitted to the SAWS on receipt of the EDR. • After requesting the EDR, the CEWs do not receive any subsequent alert advising of failure. There is no visibility into the CalHEERS queue, so there is no way to know if a transaction has errored out until the manual error report is reviewed or is pending processing. This has resulted in "hitting the enter key multiple time syndrome". • CEWs must periodically go back into CalHEERS to check status, which could range from hours to days to be received.
F12	Business Operations	Some Counties have implemented what they call the "mirror mirror" method. CEWs review every window in both systems -- CalHEERS and SAWS -- side by side. This business practice has been implemented because: • The CEW is not always aware of the default value behavior of SAWS and CalHEERS. This creates confusion to the CEW as to the validity of the information.
F13	Cross Program Impacts	As with CalHEERS, the SAWS are also evolving their systems to address the impacts of ACA. It does not appear that SAWS have completed updates in their system to avoid data collision between programs, such as, tracking the different types of household compositions (e.g. tax filer. vs. the rules for CalFresh) across the various

Observation #	Category	Description
		programs.
F14	Consumer Experience	The ability for the CEW to process an application with a consumer in one sitting is limited to the eHIT interface's ability to process information in a timely manner and retrieve verification data with the FDSH. For example, county operations staff expressed the desire to utilize paper-based verifications when available to help expedite the verification process. The FDSH has daily scheduled outages and occasional unscheduled outages that can create delays in obtaining electronic verification information. The CalHEERS system was built in conformance with the Code of Federal Regulations (CFR), which requires the use of electronic verification sources proper to any subsequent manual verification.
F15	Change Requests	The line between CRs and defects are often blurred and the eHIT interface is no exception. Over the past few months, the CalHEERS project has introduced additional monitoring and controls to assist clarifying expectations and delineating CRs as warranty, defect mitigation, clarification of policy and/or true enhancements to functionality. The project has also implemented a process that brings CRs back to the CalHEERS Change Control Board (CCB) for review as they mature through the process. The CCB evaluates the decision to move forward initially with the approval to Assess Impact, again by approving a portion of the costs presented in the impact analysis for design, and finally, the cost associated with the implementation once design has been confirmed and approved. As this review process matures, the state continues to verbalize and reinforce the expectation of end-to-end functionality delivered with the base product, defect mitigation and functionality enhancement. Specifics on each are as follows:

Observation #	Category	Description
		• The eHIT schema definition and Interface Design Document were approved by the state and implemented. Each time the CalHEERS functionality matures and the information needs to be shared, the schema and corresponding data structures and contents are modified. The baseline eHIT architecture should have been designed in such a fashion that could easily accept changes to data without complicated increases to file formats/sizes that result in considerable testing and validation efforts. CR7381 (eHIT Schema Changes has been approved for design and costs of implementation are scheduled to be presented and approved by mid-August to make an R9 implementation date. • Beginning and ending effective dates has been a requirement from the start of the project and was discussed during the initial CalHEERS JADs (CR 4180). During Change Evaluation, it was determined that a portion of the CR was refinement of baseline scope. The change request has been approved. • CR7900 Negative Action: This CR was considered to be a full function enhancement and the CR was approved through implementation prior to the process providing for interim review. However, the CR and level of effort and requirements have been through Change Control three different times based on re-evaluation of requirements and design. Cost variances are being tracked and approved as functionality and expectations are realigned with each iteration of impact to the SAWS organization and DHCS policies. • Comprehensive error handling should be considered baseline functionality (TR177 and CR10119) and will be evaluated as such when the baseline requirement and CR enter the

Observation #	Category	Description
		Change Evaluation and Control Process. The eHIT Assessment Team did not re-evaluate the cost estimates for those CRs that have been evaluated since the implementation of the current change control process.
F16	Notices	Functionality is not currently in place to support combined notices for various forms of mixed households. Notices are currently being generated on a program level basis, however, mixed households receive multiple notice packets (e.g. one for MAGI Medi-Cal and one for APTC/CSR). According to the January 22, 2013, Centers for Medicare and Medicaid Services (CMS) proposed rules (Federal Register, Vol. 78, No. 14), Covered California and DHCS are to phase in a coordinated system for notifications of eligibility determinations by January 2015.

5.3 General Observations

This section provides general First Data's observations regarding the project's processes derived from interviews and documentation reviews.

Detailed observations are documented in the following table. The General observations will begin with the letter "G" to distinguish them from other observations (e.g., G1).

TABLE 14 – GENERAL OBSERVATIONS TABLE

Observation #	Category	Description
G1	General	First Data recognizes that CalHEERS is a complex project and exists in a complicated governance environment. The CalHEERS Governance Plan depicts decision-making to support development of the CalHEERS application. • The Governance Plan was developed to frame the project during its Design, Development and Implementation phase, and has not been updated to reflect the maintenance and operations activities. • The governance model, its roles and responsibilities are not widely understood

Observation #	Category	Description
		resulting in different opinions around who has or should have decision-making authority.
G2	General	Sponsor, project and partner involvement varies, and several interviewees noted that all players are not consistently at the table at the right time for key discussions and decision-making. This relates communication gaps and a lack of clarity of when and where topics are discussed and with whom.
G3	General	Interviewees observed that executive sponsors may be involved in too many low-level meetings, and responsibility for managing project activities and desired business outcomes should rest with mid managers and staff.
G4	General	Policy decision-making is a complex process and must take into consideration impact to Sponsors, Stakeholders and the Project, as well as business operations. Communication channels need better alignment to support this complexity.
G5	General	There is no one entity that has knowledge of, or is responsible for successful "end-to-end" transaction processing among SAWS, CalHEERS and MEDS. There are organizational boundaries that impede a holistic approach to understanding and addressing eHIT issues.
G6	General	There is a perception that there is need for additional state SME participation during JADs and other meetings given complexities with the eligibility policy and differences with some requirements between MAGI Medi-Cal and APTC.
G7	General	There has been a long-standing governance process between DHCS and the Counties that supports the State supervised, County administered arrangement. With the implementation of ACA, the arrangement is transitioning to reflect the CalHEERS and ACA environment. • Pre-ACA, DHCS made policies and issued direction and guidance to Counties.

Observation #	Category	Description
		• Counties and SAWS would determine how to implement and determined their respective automation strategy; DHCS was not required to be active participant at that level. • With the onset of ACA, DHCS assumed a changed role given its sponsorship of CalHEERS, and its programmatic responsibility for ensuring that MAGI Medi-Cal is correctly programmed in CalHEERS. DHCS has become an active participant in determining automation decisions. • Efforts are underway to continue to change and mature processes to support changing responsibilities.
G8	General	The Change Control Board (CCB) and Release Management Processes are improving, however, additional improvements are needed. • Many interviewees demonstrated a lack of understanding of the processes, attendees and decision-making of the CCB and Release Management. • A comment from the majority of the interviewees is the belief that the Release Management and Change Control processes do not consistently or timely engage the right representatives.
G9	General	Interviewees identified thematic issues about the Change Control Process: • There is not enough information shared in advance of the CCB meeting to allow for understanding and analysis of the change. • CCB does not allow Partner input into decision-making. Decisions are made by the Project and Sponsors, and Partners are informed. • Counties want a voice to communicate operational perspectives when changes are

Observation #	Category	Description
		being discussed. • CCB discusses items are processes that have already been prioritized or designed. There is a need for a forum to guide work efforts based on strategic direction.
G10	General	Interviewees identified thematic issues about the Release Management process: • Counties/Consortia believe that the contents of releases are prioritized without sufficient consideration of County/Consortia business needs. • There is a need to decouple design/enhancement releases from maintenance releases, and provide for an emergency release process. • Communication around release content is sometimes inconsistent, unclear or not timely. • There have been instances of information (e.g. Release Notes) being shared after the release is in production.

6.0 Deliverable Roles and Responsibilities

This section identifies the First Data and OSI roles and responsibilities associated with the development, maintenance, review, and approval of the CalHEERS Assessment Report.

TABLE 15 – DELIVERABLE ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITIES
First Data Engagement Manager	• Provide executive oversight to First Data Team. • Work directly with stakeholders and Sponsors.
First Data Project Manager	• Manage the daily work of the First Data Team. • Coordinate work with and provide status to OSI Project Manager, stakeholders, and Sponsors. • Internally approve and formally submit deliverables to stakeholders and Sponsors. • Escalate issues and risks to OSI Project Manager and First Data Engagement Manager.
OSI Project Manager	• Oversee assessment activities. • Coordinate efforts with First Data Project Manager. • Review and provide direction on draft and final deliverables.
First Data Team Members	• Conduct assessment activities, including interviews and documentation assessment. • Prepare deliverables. • Participate in deliverable reviews with stakeholders/Sponsors.
Deliverable Approver	• Review and approve deliverables. • Participate in deliverable walkthroughs.
Deliverable Reviewers	• Review deliverables and provide comments to First Data Team. • Participate in deliverable walkthroughs. **NOTE:** One person from each organization will collect, consolidate, and submit comments from their reviewers via a single comment matrix.

ROLE	RESPONSIBILITIES
Subject Matter Experts	• Participate in interviews. • Provide documentation, as requested. • Provide clarifications, as needed.

7.0 Deliverable Schedule

This section contains start and completion dates for the CalHEERS eHIT Assessment Report.

TABLE 16 – DELIVERABLE DEVELOPMENT, REVIEW, AND APPROVAL SCHEDULE

WBS#	TASK	START DATE	COMPLETION DATE
1.1	Initiate Project	06/16/14	06/26/14
2.1	Conduct Interviews	06/18/14	07/09/14
2.2	Request, Review and Analyze Documentation	06/18/14	07/15/14
2.3.1	**Prepare/Submit DED for the CalHEERS Assessment Report**	**06/20/14**	**06/30/14**
2.3.1.6	Stakeholders/Sponsors Review and Approve DED	07/01/14	07/03/14
2.3.2	Prepare Draft CalHEERS Assessment Report	07/10/14	08/11/14
2.3.2.5	Conduct Walkthrough of Report with Stakeholders/Sponsors	08/12/14	08/12/14
2.3.2.6	State Stakeholders/Sponsors Reviews Draft Report	08/12/14	08/22/14
2.3.3.1	First Data incorporates stakeholder and partner feedback	08/25/14	09/2/14
2.3.3.2	Conduct Walkthrough with State PM Team	09/3/14	09/3/14
2.3.3.3	State Stakeholders/Sponsors Reviews Draft Report 2nd Review	09/3/14	09/11/14
2.3.3.5	Incorporate Draft 2nd Review feedback and submit Final Report	9/112/14	09/19/14
2.3.3.6	State Stakeholders/Sponsors Reviews Final Report	9/19/14	9/24/14
2.3.3.7	**Incorporate feedback and submit Final Report**	**9/24/14**	**9/26/14**

8.0 Deliverable Assumptions

First Data assumes that:

- During the development of the eHIT assessment, status on CR, defection, application design and interview perspectives were in change with the continue maintenance and operations of the CalHEERS system. First Data assumes the observations, deliverables, documents, interview status were accurate at the point of time these items were presented to First Data.

9.0 Appendix A – List of Documents Reviewed

The following is a list of the documentation reviewed to complete the assessment.

- Accenture Proposal to HBEX4, Section 2.4.2 Baseline System (Alternative Case Management Approach)
- Alternative Approach Analysis
- CalHEERS and CalWIN Action Items log, CalWIN, June 24-30, 2014
- CalHEERS Architecture Diagrams
- CalHEERS Architecture Overview
- CalHEERS Batch Summary, Level 1, and Level 2 Reports
- CalHEERS BSD2 - CalHEERS-SAWS-MEDS Interface Business Services Definition, Version 2.4.0, CalHEERS, June 7, 2013
- CalHEERS Case Management Vision, August 17, 2012 (unofficial project document)
- CalHEERS Change Request 10021 - Add Business Validation to SAWS eHIT Interface to Prevent Data Overlay at Primary Contact Level, May 30, 2014
- CalHEERS Change Request 5254 - Lump Sum Income / Deduction & Income Type Resolution, October 29, 2013
- CalHEERS Change Request 7381 - SAWS eHIT Interface: Near Real Time Error Communication, Citizenship Information and additional updates, Conditional, Approval May 30, 2014
- CalHEERS Change Request 8772 - CalHEERS Integration to MEDS, Approved May 16, 2014
- CalHEERS Communication Plan
- CalHEERS Daily Error Reports, CalHEERS, June 24 and June 29, 2014
- CalHEERS Deliverable 12 – Technical Architecture Diagrams, Accenture, December 20, 2012
- CalHEERS Deliverable 17c – Database Design and Data Management Plan – Release 3, 4 and 5, Accenture, August 5, 2013
- CalHEERS Deliverable 23a – Final Interface Control Document, Accenture, March 29, 2013
- CalHEERS Deliverable 70a – Application Technical Design Specifications – Group 1, Accenture, March 29, 2013
- CalHEERS Deliverable 70b – Application Technical Design Specifications – Group 2, Accenture, May 2, 2013
- CalHEERS Deliverable 70c – Application Technical Design Specifications – Group 3, Accenture, July 8, 2013

- CalHEERS Deliverable 70d – Application Technical Design Specifications – Group 4, Accenture, September 4, 2013
- CalHEERS Deliverable 70e – Application Technical Design Specifications – Group 5, Accenture, November 6, 2013
- CalHEERS Deliverable 70f – Application Technical Design Specifications – Group 6, Accenture, March 25, 2014
- CalHEERS eHIT Processing Outages June 2014, CalHEERS, July 1, 2014
- CalHEERS Electronic Health Information Transfer, Interface Design Document, Version 2.8, CalHEERS, December 5, 2013
- CalHEERS Governance Plan
- CalHEERS MAGI Medi-Cal NOA Approach Options, Accenture, November 20, 2012.
- CalHEERS Monthly IV&V Report Draft (October 3 - November 9), Visionary Integration Professionals, November 15, 2012
- CalHEERS Outage Notification, CalWIN, June 2014
- CalHEERS Performance Summit materials, OSI, April 28, 2014
- CalHEERS Preliminary Draft IV&V Review Report - April 2013, Visionary Integration Professionals, May 15, 2013
- CalHEERS Preliminary Draft IV&V Review Report - August 2013, Visionary Integration Professionals, September 15, 2013
- CalHEERS Preliminary Draft IV&V Review Report - December 2012, Visionary Integration Professionals, January 15, 2013
- CalHEERS Preliminary Draft IV&V Review Report - February 2014 Visionary Integration Professionals, March 15, 2014
- CalHEERS Preliminary Draft IV&V Review Report - January 2014, Visionary Integration Professionals, February 15, 2014
- CalHEERS Preliminary Draft IV&V Review Report - May 2014, Visionary Integration Professionals, June 15, 2014
- CalHEERS Preliminary Draft IV&V Review Report - November 2013, Visionary Integration Professionals, December 15, 2013
- CalHEERS Production Defect Log – June 23, 2014 and July 7, 2014
- CalHEERS Project: IV&V Technical Assessment Version 1.18, Visionary Integration Professionals
- CalHEERS Site Feedback - Fresno
- CalHEERS Site Feedback - Sacramento
- CalHEERS Site Feedback - San Francisco

- CalHEERS Site Feedback - Stanislaus
- CalHEERS Technical Committee Discussion, CalHEERS, May 9, 2014
- CalHEERS Throughput Report, Volume Reports, CalHEERS, March 13 - June 15, 2014
- CalWIN EDR/DER Processing Return Rates, CalWIN, June 2014
- CalWIN eHIT Transaction Capacity Plan
- CalWIN Guide to eHIT Errors, CalWIN
- CalWIN Rejected Error Tracking Log, CalWIN, June 2014
- CalWIN Responsiveness Data, CalHEERS, March 3 - July 3, 2014
- CR 10102 - CR 10102 - Suspend California Residency Verification as condition of eligibility for MAGI Medi-Cal, Approved May 30, 2014
- CR 6340CR 6340 - Electronic Health Information Transfer (eHIT) IDD 2.8 Updates, Approved June 18, 2014
- CWDA Analysis of SAWS Statutory Language (no date)
- DHCS Impact Analysis for the Proposed Changes to CIN Return Rules for Identify Member Service, DHCS, May 1, 2013
- DHCS Site Visit To San Francisco Human Services Agency, Issue 1 - Homeless Issue- no DER, San Francisco HSA, June 26, 2014
- DHCS Site Visit To San Francisco Human Services Agency, Issue 2 - Solicited DERs not returning when information is sent to BRE, San Francisco HSA, June 26, 2014
- DHCS Site Visit To San Francisco Human Services Agency, Issue 3 - M1 eligibility for Medicare active applicants/ MSP issue, San Francisco HSA, June 26, 2014
- DHCS Site Visit To San Francisco Human Services Agency, Issue 4 – Multiple CINs, San Francisco HSA, June 26, 2014
- DHCS Site Visit To San Francisco Human Services Agency, Issue 5 - CalHEERS cases not found in the External Referral Data, San Francisco HSA, June 26, 2014
- DHCS Site Visit To San Francisco Human Services Agency, Issue 6 - Minor Primary Applicant. San Francisco HSA, June 26, 2014
- DHCS Site Visit To San Francisco Human Services Agency, Issue 7 - Former Foster Care Child (FFCC) wrong eligibility, San Francisco HSA, June 26, 2014
- DHCS Site Visit To San Francisco Human Services Agency, Issue 8 - Difficulty in establishing communication with the CalHEERS "helpdesk", San Francisco HSA, June 26, 2014
- eHIT SAWS NIEM Schema version 2.1
- eHIT SAWS NIEM Schema version 2.8
- eHIT SLA IV&V Analysis, Visionary Integration Professionals, June 13, 2014

- Executive Steering Committee, eHIT Initiatives Status Update, CalHEERS, June 12, 2014
- Federal Data Services Hub TDS Availability schedule, CalHEERS
- Fresno County–DHCS ACA Review, CalHEERS Processing Issues, Clients showing multiple applications approved in CalHEERS requiring attention, Fresno County, May 21, 2014
- Fresno County–DHCS ACA Review, CalHEERS System Issues for Eligibility Concerning Income, Fresno County, May 21, 2014
- Fresno County–DHCS ACA Review, CalHEERS Tickets Passwords and Accounts, Fresno County, May 21, 2014
- Fresno County–DHCS ACA Review, Client Correspondence Needs, Fresno County, May 21, 2014
- Fresno County–DHCS ACA Review, MAGI Medi-Cal Applicant, Fresno County, May 21, 2014
- Infrastructure Expansion Options ROM, Business Case Focus, Oracle, May 21, 2014
- Medi-Cal Eligibility Division Information Letter No.: I 14-02, Affordable Care Act Guidance, DHCS, January 9, 2014
- Medi-Cal Eligibility Division Information Letter No.: I 14-03, Processing Health Coverage-Only Applications Received at the County January 13-20, 2014, DHCS, January 13, 2014
- Medi-Cal Eligibility Division Information Letter NO.: I 14-11, System Workarounds and Overrides, DHCS, January 31, 2014.
- Medi-Cal Eligibility Division Information Letter No.: I 14-14, Application Processing Priorities, Performance Standards, and Inter-County Transfers of California Work Opportunity and Responsibility to Kids (CalWORKs) and CalFresh Cases, DHCS, February 18, 2014
- Medi-Cal Eligibility Division Information Letter No.: I 14-22, Informational Update and Guidance on Medi-Cal Notices of Action (NOA) Generation, DHCS, April 14, 2014
- Medi-Cal Eligibility Division Information Letter No.: I 14-31, Pregnancy Changes In Circumstance Workaround, DHCS, June 4, 2014
- Medi-Cal Eligibility Informational Letter: I 14-08, E-HIT Workarounds - January 21, 2014, DHCS, January 21, 2014.
- MEDS WEB Services and Batch Processes CalHEERS SAWS MEDS Interface, Interface Design Description (IDD) for Business Service Definition – CalHEERS v.05, April 2, 2013
- Negative Actions: Assessment of Options, DHCS, June 10, 2014
- Oracle 11gR2 High Availability Best Practices
- Oracle Database High Availability Overview 11g Release 2 (11.2) E17157-09, Oracle, July 201.

- Oracle eHIT SOA Current and Recommended, Oracle
- Oracle Fusion Middleware - Developing JMS Applications for Oracle WebLogic Server
- OSI Best Practices
- Proposed Board Resolution – CalHEERS Options, May 15, 2012
- Real-Time EDR Processing Daily Activity Based on Created Date Time, Oracle, June 24, 2014
- SAWS EDR Processing Day Summary, CalHEERS, June 30 - July 23, 2014
- SAWS EDR Processing Weekly Summary, CalHEERS, July 6 - July 13, 2014
- SAWS eHIT Consolidated IV&V Findings (November 15, 2012 – June 2, 2014)
- SAWS Governance Plan Status, July 12, 2012
- SAWS Traffic Report, CalHEERS, June 25, 2014
- SAWS Traffic Summary, CalHEERS, June 25 and June 26, 2014
- Section 10823 of Welfare and Institutions Code
- Senate Bill 1341
- Solicitation HBEX4 - Request for CalHEERS Development and Operations Services, Section 4.3.2 Baseline System Functionality (Case Data Management Alternative Approach), February 22, 2012
- Stanislaus County eHIT Troubleshooting Guide
- Statewide Automated Welfare System (SAWS) Project Executive Steering Committee Charter, October 21, 2011

Appendix B – List of Interview Participants by Organization

The following is a list of participants interviewed by organization name.

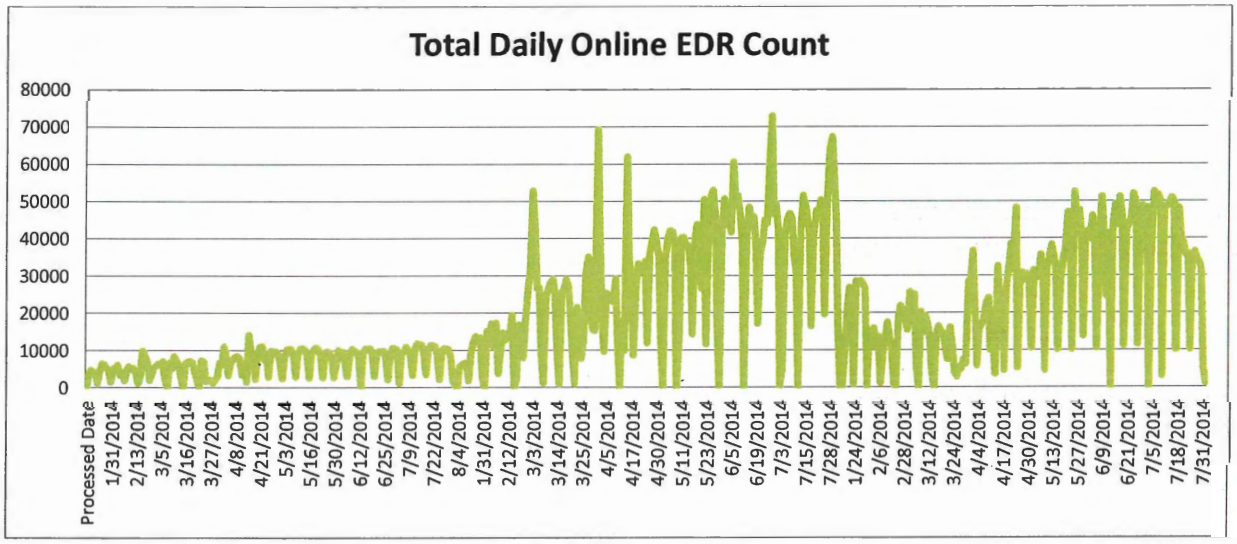
Name	Organization	Title/Role
James Kane	Accenture	CalHEERS Interface Lead
Raymond Martin	Accenture	CalHEERS Eligibility Functional Lead
Keith Salas	Accenture	eHIT Lead / SAWS Liaison
Peter Fotopoulos	Accenture	eHIT Interface Technical Lead
Jon Seltzer	Accenture	Application Architect
Dan Boxwell	Accenture	CalHEERS Technical Manager
Jon Seltzer	Accenture	CalHEERS Application Architect
Karen Ruiz	CalHEERS	Project Director, CalHEERS
Cynthia Hayden	CalHEERS	Assistant Project Director, CalHEERS
Dale Paolucci	CalHEERS	Acting System Development Chief, CalHEERS
Rachel Hernandez	CalHEERS	CalHEERS UAT Lead
Mary Ogden	CalHEERS	CalHEERS Functional Lead
Carol Huot	CalHEERS	CalHEERS Business Analyst
Karen Roach	CalHEERS	CalHEERS Business Analyst
Kay Kha	CalHEERS	CalHEERS Business Analyst
Hali Reyes	CalWIN	Executive Director, CalWIN
Christi Hendren	CalWIN	HP Project Manager Covered California Changes
Melissa Diamond	CalWIN	WCDS Portfolio Manager for CalHEERS Changes
Jim Hollister	CC - Service Center	Manager, Back Office
Liz Glogowski	CC - Service Center	QA Manager, Back Office
Jocelyn Paradise	CC - Service Center	Manager Customer Resolution Team
Jennifer Reed	CC - Service Center	Supervisor, Customer Resolution Team
Adam Dondro	CDSS	Assistant Director, CDSS

Name	Organization	Title/Role
Will Lightborne	CDSS	Director
Karen Rapponotti	C-IV	Acting Director, C-IV
Jason Horton	C-IV	Operations Manager
Jennifer Hobbs	C-IV	Medi-Cal Business Analyst
Yolanda Richardson	Covered CA	Covered California Chief Deputy Executive Director of Strategy, Marketing and Product Development
Juli Baker	Covered CA	Covered California Chief Technology Officer
Thien Lam	Covered CA	Covered California Deputy Director, Eligibility and Enrollment
Jim Hollister	Covered CA	Manager, CC Service Center Back Office
Liz Glogowski	Covered CA	QA Manager, CC Service Center Back Office
Jocelyn Paradise	Covered CA	Manager, CC Service Center, Customer Resolutions Team
Jennifer Reed	Covered CA	Supervisor, CC Service Center, Customer Resolutions Team
Frank Mecca	CWDA	CWDA Director
Christiana Smith	CWDA	IT Associate
Meg Sheldon	CWDA	Retired, CWDA
Toby Douglas	DHCS	Department of Health Care Services Director
Chris Cruz	DHCS	Department of Health Care Services CIO
Rene Mollow	DHCS	DHCS Deputy Director
Anastasia Dodson	DHCS	DHCS Associate Director
Maria Delk	DHCS	Policy Analyst, Medi-Cal Application Unit
Lance Jackson	DHCS	Consultant, DHCS
Ken Buehler	DHCS	Assistant Director
Lorenza Pennington	DHCS	HEMI Project Director, DHCS
Sharon Silvas	DHCS	Project Lead/Analyst

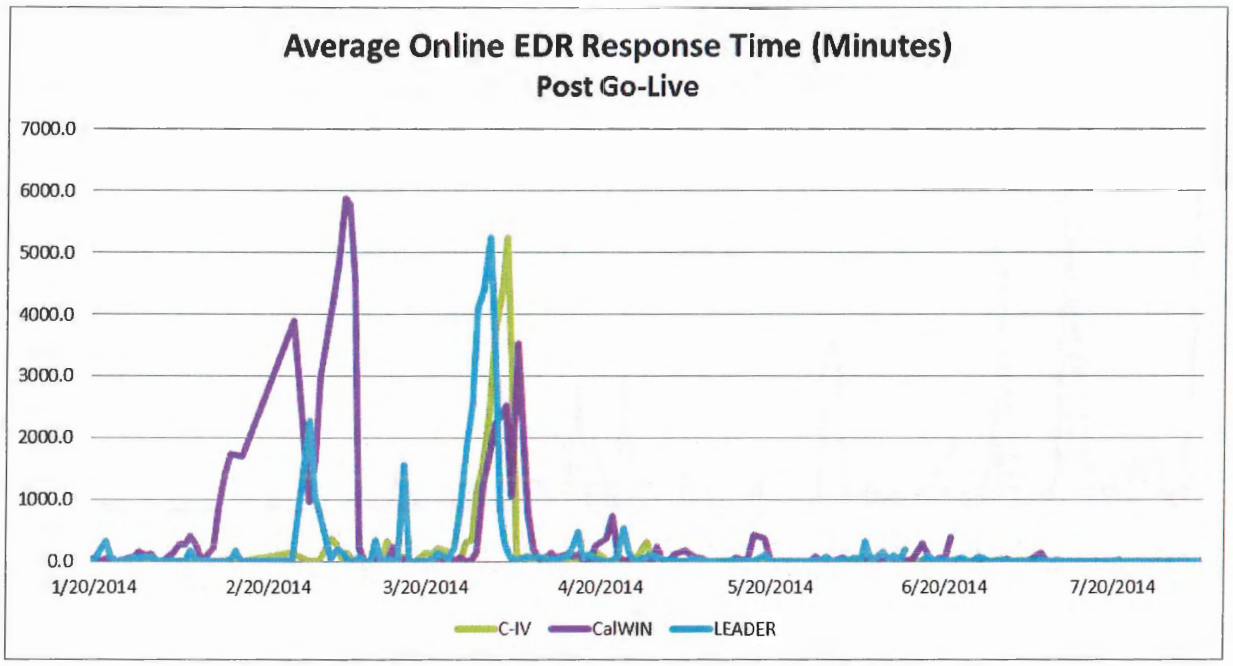
Name	Organization	Title/Role
John Gunnufsen	IV&V	IV&V Lead
Anna Chia	LEADER	Information Systems Supervisor
Laura Chavez	LEADER	Information Technology Manager II
Hayward Gee	LEADER	Senior Information Technology Manager
Christian Festa	LEADER	Unisys - Consultant
Martin Pieters	LEADER	LEADER - Consultant
Phil Ansel	Los Angeles County - LEADER	Director, DPSS
Eric Sanchez	Oracle	CalHEERS Liaison / Oracle Pre-Sales Representative
Mark Fellows	Oracle	Oracle Sales Manager
Ashish Krishna	Oracle	Oracle Consultant
Robin Geddes	Oracle	Oracle Consultant
Todd Olmeda	Oracle	Oracle Consultant
John Boule	OSI	OSI Director
Melody Hayes	OSI	OSI Deputy Director, SAWS
Kristine Dudley	OSI	OSI Assistant Deputy Director, SAWS
Bill Obernesser	PCG	OSI Consultant
Susan vonZabern	Riverside County - C-IV	Director
Yvonne Pielenz	Sacramento County	Program Specialist
Buryakov Vitaliy	Sacramento County	Eligibility Specialist
Elaine Nuval	Sacramento County	Eligibility Specialist
Andrea Ancic	Sacramento County	Eligibility Specialist
Sharon Chao	Sacramento County	Eligibility Supervisor
Lisa Pierce-Sharp	Sacramento County	Eligibility Supervisor
Heidi Kerhulas	Sacramento County	Program Specialist
Various	Stanislaus County	Various staff (18)

Name	Organization	Title/Role
Barry Zimmerman	Ventura County - CalWIN	Director

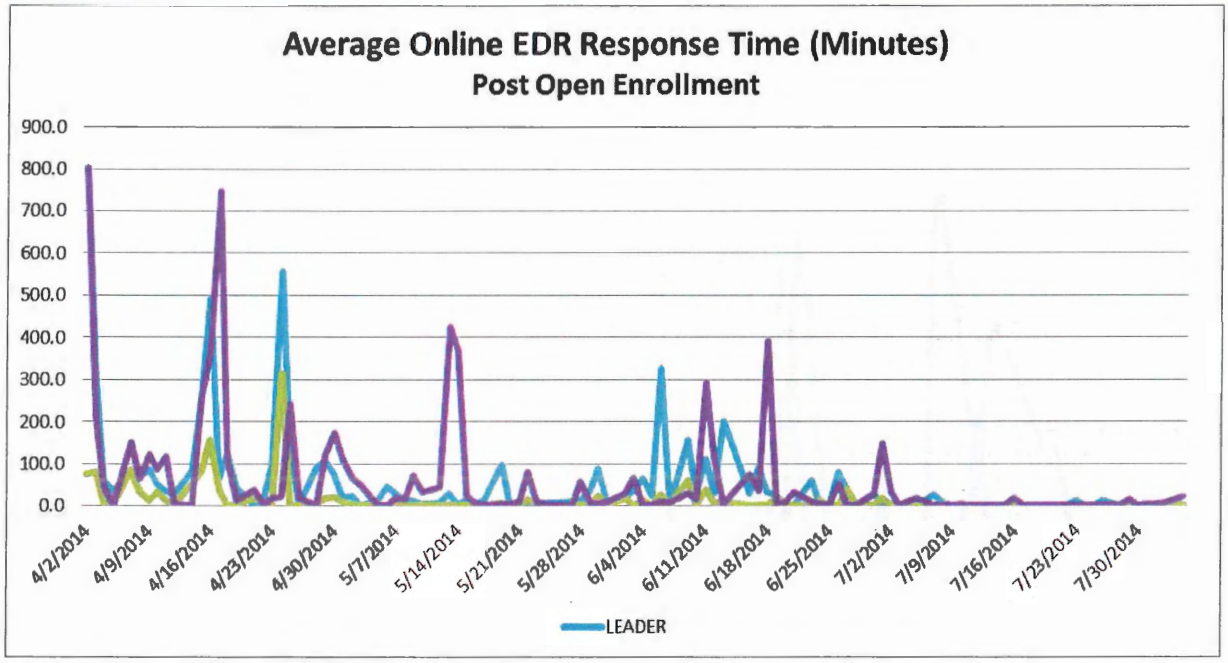
Appendix C – eHIT Performance Graphs



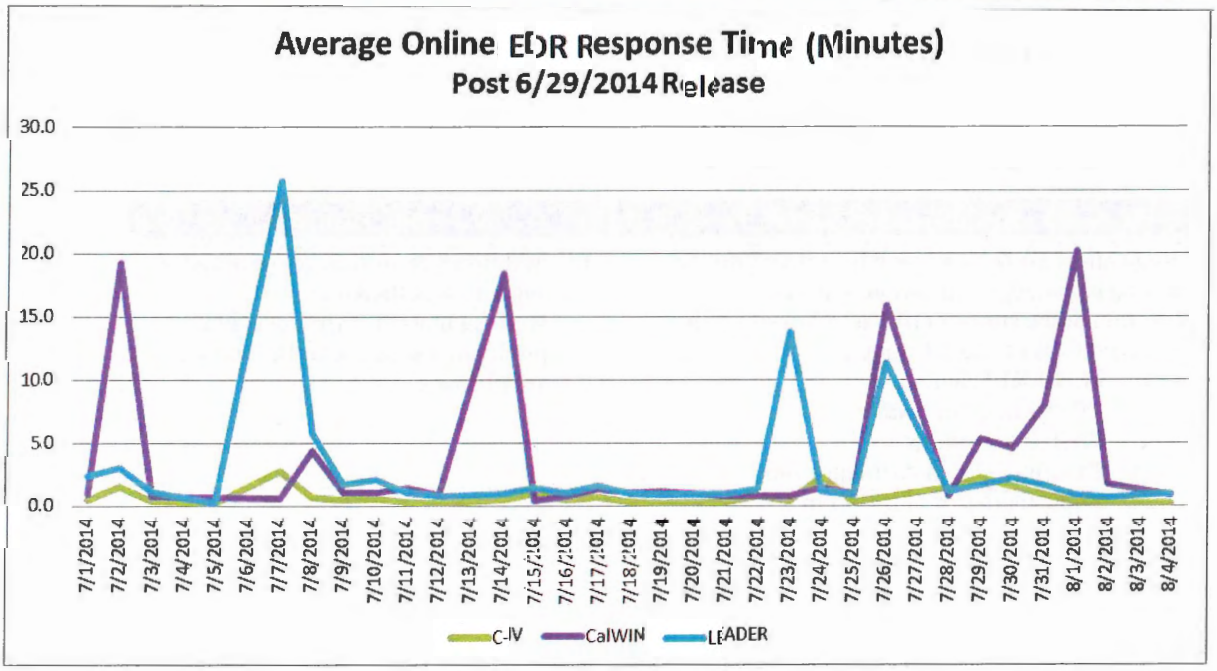
GRAPH C-1 – TOTAL DAILY ONLINE EDR COUNT



GRAPH C-2 – AVERAGE DAILY RESPONSE SINCE POST GO-LIVE



GRAPH C-3 – AVERAGE DAILY RESPONSE SINCE POST OPEN ENROLLMENT



GRAPH C-4 – AVERAGE DAILY RESPONSE SINCE 6/29/2014 RELEASE

Appendix D – eHIT MAGI Medi-Cal Rules Options Assumptions

Option 1 Assumptions and Constraints

Assumptions	Constraints
1. The global recommendations within the eHIT Assessment are implemented 2. Development continues on eHIT to support CalHEERS functions	

Option 2 Assumptions and Constraints

Assumptions	Constraints
1. Design effort for Option 2 will be reduced due to existing knowledge and lessons learned 2. A portion of the current eHIT assessment can be leveraged to implement Option 2: a. eHIT XML Schemas b. VIED SOA Composite c. FDSH integrations d. Existing SAWS data integration implementations for Option 1 3. SAWS are able to update pre-ACA Medi-Cal workflows for compliance and integration with the distinct CalHEERS verification and eligibility services 4. Simplification of eHIT allows for improved access to testing environments by SAWS 5. Data integration skillsets required for Option 2 are already in place due to current eHIT implementation 6. The State Verification Plan rules will remain with CalHEERS 7. Development continues on eHIT to support CalHEERS functions 8. Efforts to update and correct CalHEERs MAGI Medi-Cal rules proceed in parallel with Option 2	1. Additional resources are required to support simultaneous implementation of Option 2 and production support for the current architecture

Potential Option 3	
1. Design effort for potential Option 3 will be reduced due to implementation of Option 2 2. Development efforts will re-use workflows and data validations created through implementation of Option 2 3. CalHEERS will provide SAWS with VIED SOA Composites to shorten development 4. SAWS will provide sufficient environments to support eligibility business rules implementation 5. Required rules engine skillsets will be in place through existing staff or system updates (e.g. CalWIN re-compete, LRS implementation) 6. In addition to the eligibility rules, implementation of Option 3 will localize the State Verification Plan rules within SAWS 7. Development continues on eHIT to support CalHEERS functions 8. Incorporation of the C-IV counties into the LRS based system will occur after the noted implementation timeline	

Option 3 Assumptions and Constraints

Assumptions	Considerations
1. Design will be reduced due to experience from experience supporting county operations with current eHIT architecture 2. Business rules engines are available to all three SAWS; note rules engines are currently in place or part of system update efforts (e.g. LRS) 3. SAWS will provide sufficient environments to support eligibility business rules implementation 4. In addition to the eligibility rules, implementation of Option 3 will localize the State Verification Plan rules within SAWS 5. The point at which CalHEERS enhancements are frozen may be longer than Option 2 due to the longer implementation time for Option 3 and the need to prepare for 2016 Open Enrollment 6. Development continues on eHIT to support CalHEERS functions 7. Incorporation of the C-IV counties into the LRS based system will occur after the noted implementation timeline	1. SAWS may not implement the local business rules simultaneously

Appendix 5

CalWIN
Risk Assessment

Prepared by: GovConnect

TABLE OF CONTENTS

SECTION 1. EXECUTIVE SUMMARY **1**

1.1 INTRODUCTION 1
1.2 ASSESSMENT FINDINGS 1
1.3 RECOMMENDATIONS 2

SECTION 2. PURPOSE, SCOPE, AND APPROACH **3**

2.1 PURPOSE 3
2.2 SCOPE 3
2.3 APPROACH 3
2.3.1 Approach to Analysis of Outstanding Change Requests *4*
2.3.2 Approach to Analysis of County Knowledge Gaps *4*
2.3.3 Approach to Analysis of the Adequacy of the Current Training Approach *4*

SECTION 3. ANALYSIS **6**

3.1 ANALYSIS OF OUTSTANDING CHANGE REQUESTS 6
3.1.1 ACL & Change Assessment *6*
3.1.2 Results of the Analysis *7*
3.1.3 Potential Impact Of Future Changes *8*
3.2 ANALYSIS OF COUNTY KNOWLEDGE GAPS 10
3.2.1 Application Infrastructure/Reference Tables *11*
3.2.2 Client Correspondence *12*
3.2.3 Management Reporting *14*
3.2.4 County Information Server (CIS) Downloads *14*
3.3 ANALYSIS OF TRAINING APPROACH 15

SECTION 4. FINDINGS AND RECOMMENDATIONS **19**

4.1 FINDINGS 19
4.1.1 New Regulatory Changes To The Application *19*
4.1.2 County Knowledge Gaps *19*
4.1.3 Training Challenges *21*
4.2 CONCLUSION 22
4.3 RECOMMENDATIONS 23
4.3.1 Assumptions *24*
4.4 ADDITIONAL BENEFITS 24
4.4.1 NumaQ Technology Migration *24*
4.4.2 Mission Critical Interfaces *25*
4.4.3 Evaluation of UAT Rolling Wave *25*
4.4.4 Transitioning to Joint Maintenance Procedures *26*
4.5 NEXT STEPS 26

APPENDIX A. ACL AND CHANGE ASSESSMENT MATRIX 28

A.1 ACL CHANGES 28
A.2 OTHER APPLICATION CHANGES 42

APPENDIX B. ASSUMPTIONS APPROACH 62

B.1 INTRODUCTION 62
B.2 SAMPLING EXISTING CHANGE REQUESTS TO DETERMINE CRITICAL PATH 62
B.3 ESTIMATING HOURS TO COMPLETE REQUIRED CHANGE REQUESTS 62
B.4 ESTIMATING EDS RESOURCE AVAILABILITY 63
B.5 ASSUMED EDS RESOURCE UTILIZATION OF 200 HOURS PER PERSON, PER MONTH 63
B.6 CALCULATE TOTAL MONTHS TO COMPLETE REQUIRED CHANGE REQUESTS THROUGH SYSTEM TEST 63

Section 1. Executive Summary

1.1 Introduction

The CalWORKs Information Network (CalWIN) Project began design, development and implementation activities on February 28, 2000. The Requirements Validation, General System Design (GSD), Detailed System Design (DSD), Code and Unit Test, and System Test phases have been completed. The project schedule has been adjusted twice; once to allow for an additional month during DSD to conduct a series of structured design walkthroughs and once to add four months in order to accommodate a significant budget reduction imposed by the legislature.

The CalWIN Project is now approaching a milestone event in its development cycle. The User Acceptance Test (UAT) phase is nearing its scheduled completion date. In February 2003, Placer County is scheduled to commence Pilot Test of the CalWIN system; Sacramento County is scheduled to commence Pilot Test in April 2003. The decision to proceed from the UAT phase to the Pilot Test phase is one that requires careful assessment. Transition into the Pilot phase might undermine user trust, weaken stakeholder support, stall a project's momentum, adversely impact public assistance recipients, and directly or indirectly cause benefit issuance errors.

In October 2002, the CalWIN Project Manager was informed by Health and Human Services Data Center (HHSDC) that the Project's executive sponsor, the California Department of Social Services (CDSS) considered CalWIN's implementation to be a major factor in the State's Food Stamp error rate. The State stakeholders are increasingly concerned that lessons learned from the Los Angeles Eligibility Automated Determination Evaluation and Reporting System (LEADER) implementation be applied to CalWIN's implementation in order to reduce the risk of an excessive spike in the Food Stamp error rate. During the same period of time, the CalWIN development/implementation vendor informed the WCDS Project Management that several change requests were at risk for not being included in the Application prior to its release to the first Pilot County.

These factors coupled with the overall concern of the progress of the current UAT efforts contributed to a heightened sense of urgency to determine the risk of moving forward under the current set of circumstances. GovConnect, the WCDS Quality Assurance (QA) vendor, was asked by the WCDS Welfare Directors' Conference to provide a formal assessment of CalWIN's readiness for Pilot. In the process of developing the approach to the assessment, WCDS Project Management and GovConnect identified three areas of concern that merited immediate, point-in-time assessment and, dependent on the results, early advisement to all County and State stakeholders. The areas of concern are listed below:

- Significant new rule and regulation changes;
- Complexity in several areas of the Application where there are known "County knowledge gaps"; and
- Adequacy of the training approach that was modified to accommodate an increase in user population.

1.2 Assessment Findings

WCDS CalWIN Project and Pilot County staff, led by GovConnect, completed an assessment of the overall readiness of the CalWIN Application, from a workaround and training perspective. Findings of this risk assessment are summarized below.

The number and significance of new changes to the Application pose risk of Food Stamp error rate increases and other consequential system user problems.
Major outstanding changes to the Application, including some All County Letters (ACLs), have not yet been included in the CalWIN Change Management Process. Sufficient resources and time are not available to incorporate these changes into the Application within the current project schedule prior to Pilot. The alternative is to develop manual workarounds as a means of remaining in compliance with policy. The workarounds must be viable, organized in a documented guide, and accompanied by training and regular oversight by supervisory/management staff. Even with these conditions satisfied, based on LEADER lessons-learned, manual workarounds increase the potential for user morale problems, productivity losses and Food Stamp error rate increases.

The complexity in several areas of the Application poses risk to completion of a sufficiently functional system.
There are complex areas of the Application where there is a gap in County knowledge. If that gap is not addressed, there is risk that the County expectations will not be met. These complex areas include management reporting, reference tables, client correspondence, and ad hoc downloads. Based on LEADER lessons learned, incomplete or inconsistent functioning of key areas of the Application will invariably create statistical reporting problems, fiscal management problems, benefit issuance problems, client reporting problems and, of course, executive management and administrative problems.

Training challenges pose risk to successful system implementation.
Based on feedback from UAT testers and County staff who attended CalWIN training to-date, the approach, training methods and time allotted for classroom training do not assure understanding and competent use of the CalWIN system. Based on LEADER lessons learned, under-trained staff lose productivity, make deleterious errors including Food Stamp issuance errors, and undermine office morale and user acceptance of the system. Decisions regarding training methods were made early in the Project based on budget constraints that may not otherwise have been made if the focus of attention had been on error rate reduction strategies.

1.3 Recommendations

GovConnect recommends that the project schedule be adjusted to include the time and resources necessary to incorporate the impending policy changes, including Quarterly Reporting/Prospective Budgeting (QR/PB), prior to deploying the Application to the Pilot Counties for use in a production mode for service delivery.

The recommended schedule adjustment would provide additional benefits to the Project by allowing more time to successfully mitigate *other* project risks already identified in the CalWIN Risk Management Plan. These risks include:

- Technology Migration;
- Mission Critical Interfaces;
- Implementation of Rolling Wave Approach; and
- Transitioning to Joint Maintenance Procedures.

Section 2. Purpose, Scope, and Approach

2.1 Purpose

In October 2002, the WCDS CalWIN Project Manager presented a discussion paper to the WCDS Welfare Director's Conference entitled Discussion of Project Management Priorities and Three Considerations. The discussion focused on the project management priorities that have been set for CalWIN at the onset of the Project six years ago and the evolution of the Project since that time which have impacted the scope, budget and schedule. The following three considerations were presented:

1. Should the CalWIN Project reevaluate the Rolling Wave/Stagger approach to completing UAT for County-specific functions?
2. Should the CalWIN Project reevaluate the impact of regulation change? Will the Application be current enough to avoid implementation problems? Should any adjustments be made to schedule, budget or scope/expectations to address current concerns?
3. Should the CalWIN Project look at training in light of LEADER lessons learned and make any adjustments to schedule, budget or scope?

The purpose of this assessment is to provide an analysis of these considerations, focusing particularly on items #2 and #3 above, due to their direct connection to a worker's ability to provide accurate and timely benefits. The primary drivers of this assessment are the risk of experiencing significant increases in the Food Stamp error rate and having users adequately prepared to use an application requiring extensive workarounds.

This risk assessment assumes project management processes are in place to determine if CalWIN is ready to go to Pilot based on the original scope of work. GovConnect is confident that a separate Go/No Go decision strategy will be employed to determine the readiness of the Pilot Counties', the readiness of the Application as tested in UAT, and the effectiveness of project resources to support a successful transition of CalWIN into production. GovConnect will participate with the State and County stakeholders in the Go/No Go decision process through its involvement on the Project and if requested, can provide a separate risk analysis. The purpose of *this* assessment is to determine that, if the Application successfully passed UAT, would the users be adequately prepared to use an application that requires workarounds to implement policy changes in order to provide accurate benefits and services.

2.2 Scope

As the WCDS QA vendor, GovConnect's role includes assisting in the identification of areas of concern, development of recommended solutions and improvements, and documentation of the decision process that leads to implementation of chosen alternatives. This risk assessment focuses on three areas of concern: the currency of regulation changes, the County knowledge gap in key areas of the Application, and the adequacy of training in light of lessons learned from the LEADER implementation. For each of these areas of concern, the assessment provides a list of mitigation opportunities to be considered. Finally, a recommendation is made based on a project management priority assumption that sets quality as the focus in order to avoid a significant onset of error rate problems as experienced on other automation projects where schedule was the driving factor.

2.3 Approach

This section outlines the approach taken by GovConnect in facilitating and documenting this risk assessment. GovConnect leveraged existing CalWIN Project documentation, WCDS project team

members, Pilot County staff, UAT testers and the first hand expertise of the on-site GovConnect consultants to perform this assessment. Supplementing the on-site staff was former LEADER Project Manager, Rene Camou and other GovConnect resources with significant knowledge of the LEADER implementation. This LEADER experience and expertise brought an understanding of the similarities and differences between the two projects allowing true risks and viable recommendations to be developed and documented.

The standard approach employed by the GovConnect Team included:

- Information gathering and analysis;
- Risk identification/categorization;
- Formulation of risk mitigation opportunities; and
- Assessment recommendation.

2.3.1 Approach to Analysis of Outstanding Change Requests

Section 3.1 of this Assessment summarizes the results of the analysis of outstanding change requests. GovConnect reviewed all regulatory changes associated with existing CalWIN change requests as well as regulatory changes that have been issued but have *not* yet made it into the CalWIN Change Management Process.

Pilot County staff and representatives from HHSDC were asked to participate in a review of each change to validate the initial assessment work that had been done. An estimate was then made as to the number of hours necessary to complete the design, code and system testing of the changes determined to pose the highest risk. The purpose of this analysis was to identify those changes which pose the greatest risk of increasing the food stamp error rate if: 1) the change is not implemented and 2) the workaround would significantly increase the likelihood of worker confusion and misuse of the new system. In addition, this process highlighted several areas for risk mitigation including the planned discussions with both CDSS and Department of Health Services (DHS) regarding the impact of going to Pilot with some changes not implemented, specifically in the area of Notices of Action (NOAs) and forms.

2.3.2 Approach to Analysis of County Knowledge Gaps

During the course of the CalWIN Project, GovConnect consultants have been working side-by-side with the WCDS and EDS project teams. This involvement and access has provided the consultants with direct insight into the complexities inherent with the functionally rich yet flexible design of CalWIN. Using this knowledge and experience in addition to the insight that has been gained from UAT, the GovConnect consultants assessed known areas of complexity that result in increased risk due to knowledge gaps. Section 3.2, Analysis of County Knowledge Gaps, summarizes four specific knowledge gaps and risk mitigation opportunities aimed at transferring critical knowledge to the Counties prior to Pilot.

2.3.3 Approach to Analysis of the Adequacy of the Current Training Approach

In order to determine the adequacy of the current CalWIN training approach, GovConnect consultants gleaned information by:

- Working closely with the WCDS and EDS CalWIN Training Teams throughout all phases of the CalWIN Project;
- Participating in assessments of Sacramento County Train-the-Trainer (T4T) training;
- Attending CalWIN Application Training in October 2002;

- Reviewing documented feedback from the County UAT testers who completed application training in July 2002 and who have been challenged to apply the knowledge gained to their current UAT responsibilities; and
- Reviewing documented feedback from the Pilot Counties who completed vendor-led T4T* and System Administrator/System Coordinator training.

***Note**: The Sacramento County CalWIN T4T Debriefing document and the After Action Review that was distributed at the CalWIN Training Subcommittee meeting on October 11, 2002 was also provided for review in this analysis.

Section 3. Analysis

3.1 Analysis of Outstanding Change Requests

This section of the Risk Assessment summarizes the results of the analysis of outstanding change requests. GovConnect developed the ACL & Change Assessment Matrix (Appendix A) as the key assessment tool to conduct the analysis. The matrix identifies two categories of changes; ACL or regulatory changes, and Other Application Changes that are not mandated by regulation, but impact the worker's ability to use the system effectively.

Using the draft assessment matrix as a discussion tool, a meeting was held on November 1, 2002 with Pilot County and HHSDC Representatives to complete, validate and correct the initial assessment work that had been done. The Pilot County and HHSDC Representatives brought valuable insight into the process in determining potential impact and priority. Due to the limited amount of time to conduct the assessment, the discussion on November 1st focused on the regulatory changes and specifically on whether a workaround was a viable alternative to having the actual change made prior to Pilot Test. The Pilot Counties and HHSDC agreed that the assessment of the Other Application Changes could go forward without their direct input.

Many of the regulatory changes were related to revisions of forms, NOAs, and reports. HHSDC agreed to assist in facilitating discussions with CDSS and DHS to request potential relief from implementing these changes and to get approval for going to Pilot, for a limited time, with outdated versions. While the Pilot Counties felt that the workaround for any one change related to forms, NOA's, and reports was tolerable, the number and volume of these changes and the amount of correspondence involved may make this prohibitive; thus impeding the ability to provide accurate and timely benefits.

3.1.1 ACL & Change Assessment

The ACL & Change Assessment Matrix lists each required change and the estimated EDS CalWIN Team hours needed to make the change in the Application. If there were no documented hours for the change from the EDS CalWIN Team in the CalWIN Change Management Database, then estimates were derived based upon the following methods (see Appendix B for details on the hours estimation approach):

- For ACL Changes, the estimates were based on the CalWIN subsystems impacted and the anticipated complexity of the change in comparison to existing change estimates of a similar nature and complexity.
- For Other Application Changes, the estimates were calculated based on the average number of hours of the Other Application Changes that had assigned hours.

In addition, each item on the matrix was reviewed to determine:

- Whether a workaround was required if the change was not implemented prior to Pilot Test;
- Whether payment errors could result if the change was not implemented prior to Pilot Test; and
- Potential impact on end-user training.

The ACL & Change Assessment Matrix in Appendix A includes only those changes identified in this assessment as being needed for Pilot Test. This was based upon the input received from

the Pilot Counties regarding the degree of difficulty of the associated workaround. Appendix A does not include the format changes from which HHSDC is seeking relief.

3.1.2 Results of the Analysis

As of November 4, 2002 there were seventy-six change requests targeted for Release 3 of the Application. Only thirty-seven of those change requests were approved for design and coding. The remaining change requests are in various stages of approval and are at risk of not being incorporated into Release 3. The anticipated date for promoting Release 3 into the UAT environment for testing is mid-December 2002. Given the number and critical nature of the changes, adequate user acceptance testing is at risk. The WCDS CalWIN team is attempting to mitigate this risk by gaining access to system test scripts for use in preparation for retesting associated with the new release. There is still a risk that even if the testing is conducted in an expeditious manner, there may not be sufficient time to correct the critical or high priority defects prior to Pilot Test. It should be noted that important changes to the Electronic Fund Transfer (EFT) functionality are part of Release 3. This change involves multiple stakeholders and must be tested and accepted as fully functional prior to Pilot Test.

Even if the UAT of Release 3 is achievable, there clearly is no time to complete that testing prior to the start of the Pilot County end-user training. Training will be forced to be conducted using the older release of the Application. Users will not be exposed to a Release 3 version of the Application until the go-live date. This dynamic will occur throughout the CalWIN implementation. The difficulty faced by the Consortium here is that in an attempt to keep up with the regulatory changes introduced through two prior CalWIN releases, there has not been sufficient time and resources to analyze the impact of the new release and prepare supplemental training tools to bridge the gap between releases.

In addition to the changes in Release 3, the review of the change requests conducted with the Pilot Counties and HHSDC staff made it very clear that there are more change requests that must be incorporated into the Application that are critical for a successful Pilot implementation. Based on that review, the number of workarounds and their collective impact represent significantly high risk of the CalWIN system being inadvertently misused by line staff. Detailed information on workarounds associated with each change is provided in Appendix A, the ACL & Change Assessment Matrix. Given the number and extensive nature of the workarounds, the ability to adequately provide the vendor and County resources to provide viable, organized, documented, and monitored workarounds is highly unlikely within the current timeframes. Lessons learned from the LEADER implementation clearly identify manual workarounds as a potential for user morale problems, productivity losses and Food Stamp error rate increases. **The inability to incorporate the backlog of regulatory changes into the CalWIN Application prior to Pilot County implementation will likely result in a significant increase in error rates.**

Appendix B contains details on the assumptions and approaches used to estimate change hours, available man-hours, and time required to complete all changes identified in Appendix A, the ACL & Change Assessment Matrix. Based on the calculations in Appendix B the development/implementation vendor will require approximately four calendar months to implement and System Test all changes identified in Appendix A. Based on the amount and complexity of change, a reasonable estimate would be at least two calendar months to complete UAT of the changed functionality, bringing the total number of calendar months to complete all identified changes, through UAT, to approximately six months.

3.1.3 Potential Impact Of Future Changes

When assessing risk associated with pending changes it is important to evaluate current changes that are required, however, in assessing the impact of current changes, timelines, and resources it is important to look at the potential impact of future changes as well. The future changes evaluated for this purpose were:

- Change Request 909 (Electronic Benefit Transfer);
- Change Request 1513 (Quarterly Reporting/Prospective Budgeting); and
- NumaQ Technology Change.

These three changes are scheduled for implementation either right at Pilot implementation or shortly after Pilot begins, and during a time when users are just getting familiar with the CalWIN Application. These changes are significant enough to warrant their own individual project plans to track progress and timelines and in reality will have their own mini project development lifecycle.

3.1.3.1 Change Request 909, Electronic Benefit Transfer (EBT)

A significant mandatory change to be incorporated into CalWIN immediately following the Pilot Test of Placer and Sacramento Counties is Host-to-Host Electronic Benefit Transfer (EBT) functionality. This enhancement to CalWIN is being tracked under Change Request 909.

In order to provide context for this change it is important to understand that the Statewide EBT Project and CalWIN had development schedules that were out of sync. As a result the CalWIN Project started the Code and Unit Test Phase prior to the design of the Statewide EBT solution being complete or approved. To ensure CalWIN included the required EBT functionality and in an effort to reduce costs associated with the eventual CalWIN implementation of EBT, a decision was made to code CalWIN to draft EBT specifications. Following the completion of the CalWIN Code and Unit Test Phase, the Statewide EBT Project completed contract negotiations with their vendor and started requirements validation and design. As a result of the completion of the Requirements Validation and Design phases of the EBT Project, the original EBT design has significant modifications in comparison with the draft. Change Request 909 reflects the finalized specifications.

Both Placer and Sacramento Counties plan to go live on CalWIN prior to their County implementation of Statewide EBT. However, every County following these Pilots must have CalWIN functionality that supports Statewide EBT. The EDS CalWIN Team has completed a preliminary estimate of resources for the implementation of EBT in CalWIN including hours associated with design, code, testing and modifications to existing training materials. The preliminary estimate is 20,675 hours. This represents significant designing, coding and testing of a mission critical function.

3.1.3.2 Change Request 1513, Quarterly Reporting/Prospective Budgeting (QR/PB)

QR/PB is a major change to the Counties' business processes as well as to the CalWIN Application and will require a significant amount of user training on the regulation changes themselves as well as training on the CalWIN Application Changes.

This change will require several phases:

1. Requirements Phase. JAD sessions to define requirements and to design the changes needed for CalWIN. JAD sessions are anticipated for:
   - Eligibility Determination and Benefit Calculation (EDBC). How eligibility is determined, when individuals are added or removed, when benefits can be reduced or increased and how that impacts the Food Stamp portion of the case. Authorization and Benefit Recovery will need to be included here.
   - Data Collection. The information required to be captured and the effective date that EDBC should use the data will impact window designs for CalWIN as well as Alerts.
   - Client Correspondence. JAD sessions will be needed to determine what correspondence is new, changed, or no longer required. Business conditions will need to be defined and any triggers that EDBC needs to send.
   - Training. Revisions to training materials, on-line help, and eLearning will need to be defined.
   - Conversion. For those Counties that will be converting after QR/PB has been implemented, new elements and mapping will need to be defined.
2. Code and Unit test phase:
   - At a minimum, twelve subsystems are impacted by this change, five of which have been identified as large and all of which will require code and unit testing.
3. System test phase:
   - Because this change is so extensive, not only the change itself will need to be tested, but also a significant amount of regression testing will be required.
4. UAT phase:
   - This change will require a significant UAT effort heavily dependent on regression testing.
5. Training phase:
   - The timeframe that changes will be available in the County and classroom training environments will impact when or how end-users will be trained and when Counties will be able to customize and validate their training materials.
   - Training of end-users will be needed for the policy change as well as for the CalWIN Application Changes.

In order to meet the current implementation date of July 2003, several concurrent activities will be taking place given the current schedule:

- The design phase of Change Request 1513 will have commenced;
- Release 3 changes will be in UAT;
- Placer and Sacramento Counties will be preparing for and beginning Pilot Test; and
- Project resources will be supporting the Pilot Test effort.

This change will require resource intensive design activity, significant code and retesting of core functionality, comprehensive user acceptance testing, and extensive end-user application and policy re-training.

3.1.3.3 Migration from NumaQ to P690 Architecture for the CalWIN Enterprise Server

The enterprise server platform for CalWIN was proposed and is currently operating on Sequent's NumaQ Enterprise Server architecture. IBM Corporation acquired Sequent after the CalWIN Project started. IBM has recently announced that they will stop supporting the NumaQ architecture in the fourth quarter of 2006 and would be replacing that product line with their pSeries P690. In response to that announcement EDS scheduled a migration from the NumaQ Enterprise Server to the P690 Enterprise Server to occur prior to Pilot Test.

IBM has provided to EDS the services of Sector7, a company that specializes in testing application compatibilities when moving from one hardware and system software platform to another. Sector7 has conducted tests using the current CalWIN Application and has identified changes that must be made for both the CalWIN Application and configuration parameters of other CalWIN system software products. EDS also plans to do the CalWIN Full Load Benchmark Test on the new platform.

With the current migration schedule, CalWIN would go live in Placer on the new P690 platform on February 3, 2003. The EDS CalWIN Application Services team, as well as the WCDS UAT team would not have their first opportunity to test on the new platform until mid-December 2002. This is the same timeframe that Release 3 is scheduled for UAT. Many of the CalWIN deliverables, work products, and processes and procedures will need to be updated because of the new platform.

There are risks associated with introducing a technology change of this magnitude given the current accelerated schedule for testing, gaining experience, and revising processes and procedures associated with this architecture migration.

3.2 Analysis of County Knowledge Gaps

The CalWIN system is rich in functionality and will provide the Counties with a tool that will serve them well for many years. In order to meet eighteen Counties' varying business needs, the CalWIN system is also replete with flexibility and County options. Any system that is this function rich and flexible is also very complex and requires a significant amount of knowledge transfer from the development project to the end-users, including those who will participate in County administration and maintenance of the system.

This section of the risk assessment addresses several areas of the Application where, due to the complexity of the subsystem or other factors, the Counties' knowledge gaps are the greatest. These include:

- Application Infrastructure/Reference Tables;
- Client Correspondence;
- Management Reporting; and
- County Information Server (CIS) Downloads used for County-specific interfaces and ad hoc reporting

The discussion of each area includes a synopsis of activities the Project and Counties have undertaken to increase the Counties' knowledge base and an assessment of the risk involved if

CalWIN is implemented without closing the knowledge gaps. Particular attention is given to the potential risk of increased error rates.

3.2.1 Application Infrastructure/Reference Tables

The internal structure design of CalWIN relies heavily on a fairly complex infrastructure that uses numerous reference tables containing the following kinds of data:

- List of values. These data elements (values) are used primarily for displays in CalWIN window drop-down fields.
- County-specific Process Controls. These controls allow the County flexibility to implement functional areas of CalWIN according to specific County policies and procedures. This would include items such as office information, worker information, automatic/non-automatic case assignment, etc.
- Program-specific Controls. These controls define programmatic standards needed for eligibility determination. This would include items such as minimum wage standards, participation status, and policy tables.

CalWIN Reference Tables currently number about 670, and are classified into four different categories:

- System tables. These tables are used by the system internally to determine eligibility and initiate batch processes. Counties cannot update these tables.
- Consortium maintained. These tables are system related, defined by regulation and standard across all Counties. The Counties cannot update these tables.
- Consortium-County maintained tables. The Consortium maintains the values in these tables that are standard, but the Counties will be allowed to add/maintain values that are specific for them.
- County maintained tables. These tables are controlled entirely by Counties.

The structure of Reference Tables is complex and maintaining them will require a great deal of involvement from Counties both pre- and post-implementation. Reference Tables, perhaps more than any other single concern, are the most critical to the successful implementation of CalWIN.

The Project and the Counties have already exerted a great deal of effort related to reference tables, including:

- UAT Infrastructure set-ups (using the County Process Control Tables);
- Gathering and validation of reference table values; and
- Preparation of the Application Infrastructure Workbook.

Pre-implementation infrastructure set-up activities will involve decision-making at several levels of County Management and will consume a great deal of manpower. Correct completion of this infrastructure set-up will be absolutely critical to CalWIN, particularly in the areas of Appointment Scheduling, Hearings, Benefit Issuances, Security, business process controls, provider information, Client Correspondence, Client Referral, Error Prone case processing, Foster Care, and Management Reporting. In addition, all County-Consortium and County-maintained tables must be reviewed immediately prior to implementation to assure the data is current and accurately reflects County policy and/or procedures.

Post-implementation infrastructure maintenance activities will involve assigning employees permanently to the "care and maintenance" of the items identified above. This activity will be critical for on-going CalWIN functionality for the same processes identified above and for assuring overall system performance is meeting County, State, and Federal requirements. Counties will need to assign permanent staff to the review and maintenance of Reference Tables.

Although multiple attempts were made to communicate the magnitude of the CalWIN infrastructure to the Counties, it is almost a certainty that Counties still lack sufficient knowledge to make the right decisions regarding the implementation of their business choices in the Application. The **Application Infrastructure, in particular Reference Tables, remains a high risk** for a Counties' successful utilization of the flexibility available in CalWIN.

3.2.2 Client Correspondence

The Client Correspondence subsystem of the CalWIN Application dynamically produces Notices of Action (NOAs) and other correspondence, as well as generates forms. A considerable portion of the correspondence is automatically generated, based on actions completed within the system. Variable data, such as client name, address, effective dates and benefit amounts are populated by the system. Additionally, all correspondence may be user-initiated. In addition to English, correspondence will be produced in eight other languages.

The CalWIN Client Correspondence Tracking Database (Tracking Database) is the tool used to manage and develop correspondence that will populate the Client Correspondence Master Database in the CalWIN system. The Tracking Database contains approximately 7,600 items of correspondence, consisting of over 7,100 County-specific items and about 500 State correspondences. Through an extensive process of Project and County review and feedback, this number is down from the original 27,000 NOAs components, forms and other correspondence originally entered.

Early in the planning process for development of the CalWIN system, the ability to produce accurate and timely NOAs, forms and other correspondence was recognized as an important requirement of the system. Also identified was the need to include County-specific correspondence, particularly in the areas of Foster Care and General Assistance/General Relief. Both the volume of correspondence and the complexity involved in appropriately populating the Tracking Database with components of correspondence to be dynamically generated, continues to require considerable reliance upon County resources and Subject Matter Experts (SMEs).

Throughout the life of the Project, the technical and functional aspects of the Client Correspondence subsystem have undergone considerable changes. Many of these were driven by the Counties' and the Project's increasing understanding of the intricacies of the system and its functionality, as well as continuing clarification of the Counties' business needs. These changes, while necessary, have added an increased level of difficulty to the Project's ability to provide the Counties with accurate, timely and detailed information about the functionality of the subsystem and the output it will generate.

While many issues and concerns have been resolved, several resolutions remain in progress. Areas that may impact Pilot Test and continue to present complexity that must be addressed or result in incorrect/incomplete or non-issued correspondence include:

- Testing the solution for generating correspondence in nine languages;
- The time commitment necessary from County and Project staff to complete the translation efforts and incorporate the correspondence components once the translations are complete;
- Technical considerations for producing and printing correspondence that continues to be subject to modifications;
- The current volume of County-specific correspondence, while substantial, still appears to lack necessary correspondence. For example, a necessary approval or denial NOA is identified as not included in the database and must be added; and
- The pre- and post-implementation and on-going maintenance activities that will require significant time and resource commitments by the Counties, and the complexity of those activities.

The Project has been fortunate to have numerous County resources working with both Project and other County staff to accomplish what is needed, but it is clear the effort and resources required are much greater than anticipated when the Project began. The County resources not only need to have an in-depth understanding of the rules and regulations that apply to correspondence and what is required for each Program (for example, CalWORKs, Medi-Cal, Food Stamps), but also need to understand the fine points of deconstructing correspondence into components according to complex instructions, for use in CalWIN. Changes in approach that have been made in response to the Counties' difficulties with completing the required tasks, as well as the complexity of the tasks themselves have often resulted in incomplete or inaccurate input from the Counties. In attempts to complete tasks related to Client Correspondence and increase the Counties' knowledge and understanding of this multifaceted subsystem, the Project and County resources have:

- Made County visits to work with staff;
- Convened a number of workgroups and taskforces;
- Produced and delivered numerous presentations, walk-throughs and updates;
- Produced a Client Correspondence Workbook and Process and Procedures documents;
- Designed and included some standard forms that are available for use by all Counties;
- Communicated through various County Information Transmittals and County Requests for Information; and
- Issued a monthly Client Correspondence Status Report and made monthly reports to the CalWIN Joint Committee.

Even with these concerted efforts and County involvement, **Client Correspondence remains a high-risk area** of the CalWIN system. Lack of notification to clients, as well as incomplete or incorrect notification, will result in payment errors. The potential for increased error rates remains high.

3.2.3 Management Reporting

As with any large system implementation, Management Reporting (MR) has been on the "concerns" list for CalWIN implementation from the earliest days of the Project. The concerns relating to MR have generally focused in the following areas:

- The large numbers of reports CalWIN will be producing;
- The time commitment necessary from County and WCDS staff to complete design of cover sheets and report formats;
- The knowledge of the application infrastructure and reference tables needed in order to establish the correct parameters from which data will be provided on the reports;
- The time commitment for review and sign-off once reports were completed in the accepted design format; and
- Technical considerations for producing reports, including a longer than expected time commitment to finding the best solution.

As of October 2002, CalWIN will be producing more than 670 reports, with a very real possibility of additional reports being needed. This volume of reports has contributed extensively to the extended time considerations identified in the bullets. The Project has been fortunate to have a group of development/implementation vendor and County staff working in concert to create these reports, but the task has been much larger and consumed much more time than anticipated when the Project first started. Early in the Project, a decision was made to use CalWIN development as an opportunity for Counties to identify the kinds of reports that would best serve their needs. This decision ultimately resulted in a complete overhaul of reports. While there is no question of the validity of this decision, it has contributed to extensive time commitments for design and review of reports.

Technical discussions were begun early in the Project, and several solutions were developed, discussed, and modified before a final recommendation was made. The recommendation includes having a separate Management Reporting server in each County, and using Business Objects and Content-on-Demand software for producing reports. Since several options were proposed before a final was adopted, it is likely neither the Counties nor the Project thoroughly understand this solution, and indeed, the Project is still in the throes of trying to find an acceptable solution for report retention.

Understanding programmatic and technical management reporting functionality is vital for the Counties as they implement CalWIN. Key management reporting staffs at the County-level have not had the opportunity to gain this understanding, and this **gap in County knowledge of Management Reporting creates a high level of risk**. Counties will use reports for a variety of critical tasks including fiscal reporting, State and Federal claiming and caseload management. Correct and accurate reports are vital to the Counties at any time. This becomes more critical with current budget reductions concerns and increasing emphasis on reducing error rates.

3.2.4 County Information Server (CIS) Downloads

CIS data downloads are used by Counties for their ad hoc reporting and their County Optional Interfaces. During GSD and DSD it was determined that it would be almost impossible to identify specific data elements within CalWIN that were necessary for the ad hoc downloads. Therefore, it was decided that Counties would receive a full CalWIN database download when they go live, then nightly update downloads with an option to also receive monthly refresh downloads. These

monthly refresh downloads would again be a full CalWIN database download as of that particular date. Downloads include a schema file and a data file.

The need to download a full CalWIN County database to the CIS and then upload it into a database on the CIS has created some technical problems that still have not been completely resolved. Some steps have been taken to alleviate some of these problems, such as changing the configuration of the CIS, which has just recently occurred. Several methods including using DVDs have been discussed as being an efficient method for the initial downloads as well as the monthly refresh downloads based on the size of the data that would need to be downloaded to the Counties.

Counties have received downloads of the CalWIN CIS schema and some data. The amounts of data Counties receive have been dependant upon the data that is currently in the UAT environment. Counties have not yet received a full conversion CIS download. The database design of CalWIN is complex and the Counties are just now receiving information that helps them understand the complexities to be able to use the downloaded data in a database of their own on the CIS. Counties are now gaining knowledge of the data relationships within the CIS downloads. They are also in the early stages of developing methods to upload that data into their CIS database. These methods may have to change once they get the opportunity to test them with data that reflect the sizes of initial and monthly refresh downloads. Developing the CIS database is critical to a County for ad hoc reports as well as their County Optional Interfaces. Gaining the knowledge needed to get the CIS database design, download and upload procedure to a level needed for Production will take time.

Project resources are now addressing the technical challenges for downloading a full County database from the CalWIN Enterprise Server and the subsequent uploading of that data to the County CIS. To promote County awareness of what they will be receiving and how they will be able to use the data they receive, the CalWIN Technical Implementation Workgroup (TIWG) created a County CalWIN CIS Subcommittee in September of 2002. The County CIS Subcommittee now meets monthly following the TIWG meeting. Both the TIWG and CIS Subcommittee are chaired and run by the Counties, with participation from the WCDS CalWIN Project team as well as participation from the development/implementation vendor. There is a concern that Counties may not have gained enough knowledge of the CalWIN database to build their CIS databases to satisfy their County needs. This presents a **high risk of not fully utilizing the CIS data** for use in the County to provide ad hoc reporting or County-specific interface flexibility.

3.3 Analysis of Training Approach

With an automated system the size and scope of CalWIN, training of end-users has been the focus of intensive effort by both the Counties and the development/implementation vendor since the early days of the Project. The current training design uses a blended approach to delivering training, which includes:

- Instructor-led training using a classroom (ILT);
- Web-based training (eLearning);
- Supplemental, reinforcement, enhancement, and refresher training; and
- On-line help.

CalWIN training's technical design uses the Learning Management System (LMS). LMS is the web-enabled, technical support structure designed to support all training activities from design through user training, and user support after implementation. In addition to LMS, technical support for training will be accommodated by the creation of separate training environments or regions that are intended to support all phases of training.

Instructor Led Training (ILT) utilizes two methods of delivery:

- Vendor-led training (VLT)--the EDS CalWIN Training Team will be responsible for the delivery of all CalWIN system-based user training.
- Train-the-Trainer (T4T)--WCDS County Trainers will deliver the CalWIN end-user training.

Regardless of the training approach that the Counties have selected, T4T or VLT, the same classroom training approach will apply. CalWIN end-user training will be delivered to each target group of end-users through a series of modules contained in an end-user-specific CalWIN training course.

In addition to initial Consortium-level training, each CalWIN County has the flexibility to develop supplemental training for County-specific needs. Counties will also have access to desktop training materials intended to reinforce, enhance and refresh end-user training skills.

No matter how intuitive the design of the CalWIN Application, the end-user will have questions about its functionality and interfaces, so on-line help functionality was developed to be an integral component of overall training requirements. On-line help is available from any area in the Application and contains three basic elements: a procedural user manual, window-level help and field-level help. The Help system should be the first place users turn for assistance as they work with the Application.

A great deal of attention and effort has gone into the design and development of training for CalWIN. There was recognition that the training needed to be detailed, focused and robust, as reflected by the following deliverables that have already been developed and approved:

- Instructor Guides (Hard Copy);
- Student Guides (Hard Copy);
- Module Quizzes (On-Line);
- Training Games (On-Line);
- CalWIN User's Manual (On-Line);
- Window- & Field-Level Help (On-Line);
- eLearning (On-Line);
- Quick Reference Guides (Hard Copy);
- Module Presentations (On-line); and
- User Activity Guides (Hard Copy).

However, as in all areas of project development, budget and time constraints were limiting factors. From the start of the Project through the approval of the training plan, the number of end-users to be trained grew by 40%. Driven by budget constraints, a decision was made to accommodate this increase with an alternative delivery approach for some areas of the Application. eLearning was determined to be an appropriate method for part of the classroom curriculum thereby minimizing the impact of bringing the additional trainees into the regional training site classrooms. eLearning is intended to be a robust, self-directed product that would

enable end-users to learn basic CalWIN navigation and functionality as a pre-requisite to their instructor-led training. While this adjustment in the training approach allowed for the increase in trainees, it has reduced the amount of "in-class" time for the average eligibility worker from five days to three days.

The original length and approach to CalWIN training was patterned after that done by prior system development efforts, such as LEADER. The LEADER system lessons learned has identified training as a contributing factor to the increased error rates experienced after the implementation of that system. Due to the need to address an increase in the training population, the WCDS Consortium made a decision to further reduce the length of classroom training and modify the training delivery method. If the emphasis had been on error rate reduction and the lessons learned from the LEADER implementation had been apparent at the time, that decision may have been vastly different. It has now become apparent that significant enhancements to the LEADER training model for both pre and post implementation training would have increased the ability of the workers to use the new system to its full potential.

Based on feedback from the initial CalWIN training that has been provided to the UAT testers and Pilot County trainers, the eLearning delivery method is a viable alternative for some aspects of the training curriculum. The eLearning modules provide a broad overview of CalWIN functionality that, if provided in the classroom setting, take up valuable instructor time that could otherwise be used for more difficult subsystems or practice opportunities. Also, it was noted that some eLearning modules may not be sufficiently comprehensive for users who receive only eLearning.

Another challenge posed by the current training approach is in meeting the expectation that training will teach the user everything they need to know to do their job using CalWIN. Based on identified issues and problems experienced during preparation and presentation of the initial CalWIN training, the following specific concerns were identified:

- There is insufficient time to cover the necessary material, practice using the Application and, participate in independent hands-on activities.
- The training for mixed audiences such as T4T and Help Desk only offers single program examples. Students from other programs may not relate to the examples and as a result miss out on critical experiential learning.
- Trainers do not provide context to the training by explaining why information is gathered, why it is important, and how errors can occur. Trainers do not have time to explain the impact of entering or not entering data on particular screens. Sufficient time to cover the essential functionality used to determine eligibility and calculate benefits is not available. When programs "fail" in CalWIN, there is inadequate troubleshooting time to determine why. When the benefits automatically calculated by CalWIN differ from expected results there is not enough time to determine the reasons for the discrepancy, which could help users understand the 'connection' between what data is entered (or omitted) and the end result.
- For T4T Counties, there is a significant work effort involved in both customizing the training material and uploading that material to the LMS in order to use it in the classroom. The current schedule was based on an estimate of the time required to complete these tasks before the magnitude of the effort was clearly recognized. Based on more detailed information now available, there is concern that there will be insufficient time and resources for the T4T Counties to complete these required tasks.

- A specific course for County Coaches has not been developed. The Coaches have a key role in troubleshooting the end-user's issues during the hands-on activities. They are also expected to help students understand how CalWIN relates to program policy, County-specific procedures, and County business processes. They may not be adequately prepared without instruction specifically tailored to their responsibilities in the classroom.

Other automation projects have faced the same challenges. The length of time it takes to ensure the end-user is comfortable with the system is in direct conflict with the time a County can afford to have a trainee away from their job during the resource-intensive pre-implementation period. The use of vendor trainers can compound the problem of understanding the policy behind the system, however it should be noted that County trainers will also have difficulty "fitting it all in".

In summary, CalWIN training is the critical path to ensuring that end-users understand and can effectively use the system. **The risks inherent in the CalWIN training approach, content and tools (to both conduct and reinforce training) are significantly high.** If these risks are not successfully mitigated, the results will be costly.

Section 4. Findings and Recommendations

4.1 Findings

Accurate benefits and timely delivery of services are the primary objectives of the CalWIN system. Under the current set of circumstances, as described in Section 3, the Pilot Counties are at risk of failing to meet those objectives. The following risks were identified as a result of this risk assessment:

- The number and significance of new changes to the Application poses risk of Food Stamp error rate increases and other consequential system user problems.
- The complexity in several areas of the Application and related County knowledge gaps poses risk to completion of a sufficiently functional and usable system.
- Training challenges pose risk to successful system implementation.

For each risk GovConnect has identified associated mitigation opportunities (see sections 4.1.1 through 4.1.3), which collectively mitigate the identified risks.

4.1.1 New Regulatory Changes To The Application

There are major outstanding changes to the Application, including some regulatory changes that have not yet been included in the CalWIN Change Management Process. Sufficient resources and time are not available to incorporate these changes into the Application within the current project schedule prior to Pilot. The alternative is to develop manual workarounds as a means of remaining in compliance with policy. The workarounds must be viable, organized in a documented guide, and accompanied by training and regular oversight by supervisory/management staff. Even with these conditions satisfied, based on LEADER "lessons-learned", manual workarounds increase the potential for user morale problems, productivity losses and Food Stamp error rate increases.

ID	Description of Mitigation Opportunities
1.	Enhance the current policy/regulation evaluation process and develop a strategy and process for evaluating ongoing regulation changes for impact, urgency, and possible workarounds.
2.	Develop a process for communicating to the Pilot Counties, the strategy and process described in item # 1 above, so they may assess the impact to their workload and/or training areas.
3.	Transition to a process that provides for County feedback and prioritization related to regulation changes.

Table 4-1. Risk Mitigation Opportunities Associated with Pending Changes

4.1.2 County Knowledge Gaps

There are complex areas of the Application where there is a gap in County knowledge. If that gap is not addressed, there is risk that the County expectations will not be met. These complex areas include Application Infrastructure/Reference Tables, Client Correspondence, Management Reporting, and County Information Server Downloads/Ad Hoc Reporting. Based on LEADER lessons learned, incomplete or inconsistent functioning of key areas of the Application will invariably create statistical reporting problems, fiscal management problems, benefit issuance

problems, client reporting problems and, of course, executive management and administrative problems.

ID	Description of Mitigation Opportunities
1.	Attempt to increase communication regarding County Knowledge Gaps via CIT and CWJC discussions.
2.	Offer additional training to the implementation teams currently in each County and rely on them to assist in getting the County ready.
3.	Prepare an extensive training session or series of workshops for each County prior to and during their pre-implementation window.
4.	Designate a CalWIN project resource that will work on-site with each County as they prepare their Application Infrastructure and County Reference Table Maintenance Plan. This option could be used in conjunction with any of the strategies described in items #1, #2 or, #3.
5.	Reduce the volume of County-specific correspondence and the corresponding County maintenance commitment by using State correspondence when possible.
6.	Reduce the volume of County-specific correspondence and the corresponding County maintenance commitment by using CalWIN Standard Forms.
7.	Continue efforts to standardize correspondence where possible and encourage Counties to select the standard items rather than County specific NOAs, forms and other correspondence.
8.	Charge the newly implemented Client Correspondence Workgroup with spearheading the standardization efforts, as well as efforts to increase Counties knowledge base through communication and education in their Counties.
9.	Designate a Client Correspondence Coordinator in each County and charge the resource with educating others in the County who will be involved in development and maintenance of correspondence.
10.	Increase communications with the County regarding the reporting environment via CIT process and continuing meetings with the MR workgroup.
11.	Prepare an informational/training packet regarding the reporting environment and explore with the MR workgroup how to disseminate it to the Counties.
12.	Prepare an extensive training opportunity on MR and offer it to at least one person from each County.
13.	Create a workbook similar to Client Correspondence and Application Infrastructure that would document the technical solution for reporting and the final format for reports.
14.	As part of the full load conversion effort, an initial download for the CIS can be created. This can be used to verify that the procedures for uploading the County CIS database are sufficient.
15.	Offer additional support to the CIS Subcommittee to ensure their success in creating a database that will be the appropriate structure and size for the initial CIS download.
16.	Determine what kind of system documentation, if any, can be developed for use by the County to better understand the schema file.
17.	Use the CIS Subcommittee to share information from the Counties in the best positions to test and validate the data file and any accompanying documentation

Table 4-2. Risk Mitigation Opportunities Associated with County Knowledge Gaps

4.1.3 Training Challenges

Based on feedback from UAT testers and County staff who attended CalWIN training to-date, the approach, training methods and time allotted for classroom training do not assure understanding and competent use of the CalWIN system. Based on LEADER lessons learned, under-trained staff lose productivity, make deleterious errors including Food Stamp issuance errors, and undermine office morale and user acceptance of the system. Decisions regarding training methods were made early in the Project based on budget constraints that may not otherwise have been made if the focus of attention had been on error rate reduction strategies.

ID	Description of Mitigation Opportunities
1.	Increase the duration of several Instructor-Led course sessions. This increase in classroom days would mainly target two groups: eligibility staff and clerical staff. • Some of the additional time should be used to discuss how CalWIN uses the data entered to determine eligibility and calculate benefits; • Recommend changing the existing Medi-Cal case from a "vanilla" to a more complex case to enable more thorough and comprehensive learning; • More exercises should be included to teach students how to troubleshoot, when a program "fails" or the expected results differ from CalWIN's eligibility determination; and • Other programs, in addition to CalWORKs, should be used in case examples in T4T, Help Desk Staff Development and Generic Eligibility training.
2.	Enhance the On-line Help system to include more helpful and specific information. These include: • CalWIN terminology, particularly terms used in current Welfare environment but with different meaning in CalWIN, must be more clearly defined. These include terms in the glossary, but more importantly, names of fields and group boxes need to be further explained in window- and field-level help; and • Procedures should be more detailed, specifically on how to enter income, expenses, resources, and ownership. These should also include more detail on how to enter program-specific data.
3.	Enhance eLearning by adding audio content to all eLearning course modules.
4.	Develop an Inquiry module for web inquiry-only users as a part of eLearning and/or make the eLearning Core Course available to inquiry-only end-users.
5.	Customize the Instructor-Led Training Environment to support multiple County environments so Counties will be working in their own County environment during classroom training.
6.	Provide more training materials focused on troubleshooting errors: • Enhance the Quick Reference Guide to include more troubleshooting procedures as they relate to each end-user group; and • Create an eLearning module that focuses on error-prone areas (household composition, income, expenses, resources) and provides a connection between policy and the CalWIN Application.
7.	Add another course to the Training Plan for County Coaches. Develop a curriculum for training coaches that include troubleshooting when a program "fails" or the expected results differ from CalWIN's determination. Furthermore, the coaches should be prepared to answer County-specific questions on how CalWIN will affect end-users in their job functions. This may mean extending the time available for coaches to become more familiar with the system.

ID	Description of Mitigation Opportunities
8.	Make the regional training sites available to County CalWIN Trainers so they can practice their training in the same training environment as will be available during their end-user training.
9.	Add operational support to allow Counties to run batch in the County Training Environment.
10.	Consider one of the following changes to the current training delivery methods: • Move the T4T training course up in the training schedule, increasing the amount of time they will have to customize their training material; or • Design and implement a blended ILT training approach, which combines the VLT and T4T methodologies. All training would then be provided by Vendor Trainers who have months of working and training experience in the CalWIN system. County CalWIN Trainers would still attend the three-week Train-the-Trainer course to learn how to customize their training material to be used during post-implementation.
11.	Provide post Go-Live refresher training. This may be something that can be covered by the existing training requirements, or may be in addition to what is covered by the approved CalWIN Training Plan. The strategy would be to provide refresher training during the month following system implementation. Depending on Consortium preference, this refresher training could involve the following activities: • The Consortium could take a system-focused approach. At a Consortium-level, the Counties would identify functional areas, processes or tasks about which a majority of users have questions or on which additional training is required. The Project would develop a Consortium-level set of refresher training materials. Vendor or County trainers would then deliver this refresher training to County users. • The Consortium could take a user-focused approach. Each County would be responsible for identifying those users experiencing the greatest amount of difficulty with the system. Identified users would then be sent to an additional round of classroom training. Vendor or County trainers would deliver this refresher training.

Table 4-3. Risk Mitigation Opportunities Associated with Training Challenges

4.2 Conclusion

To go to Pilot without mitigating the risks identified in Section 4.1 Findings, would be a disservice to stakeholders who have invested their time, staff, and financial resources to support this Project.

Based on the results of the change-backlog analysis, the time estimated to develop and System Test the necessary changes is approximately four months. Given that some design work is in progress, the four months could be applied starting with the month of November 2002. This means that the Application, with all required changes, would be ready for UAT at the beginning of March 2003.

A minimum of two months would be required to successfully UAT the Application given the volume of changes. This presumably could lead to a May "go-live" date for Placer. However, since Placer must begin end-user training with an application that a) reflects the incorporated changes and b) is adequately tested to ensure a productive learning environment, a more reasonable date for Placer to "go-live" would be June 2003.

Adjusting the schedule to incorporate the above timeframes would *not* be prudent without also looking at QR/PB as the driving force. QR/PB must be implemented in July 2003. This is precisely the time when, according to the current project schedule, 100% of CalWIN resources must be devoted to a) supporting two Pilot Counties; b) making numerous application changes identified in Pilot; and c) preparing for implementation in the other sixteen Counties. Consequently, there will be neither time nor resources to implement QR/PB.

Ignoring the issues noted in the previous paragraph, if the schedule *is* adjusted to have Placer "go-live" in the May/June 2003 timeframe, the risk to implementing a successful system would be greatly increased because users already new to the CalWIN Application would be first trained on the use of CalWIN's *retrospective* budgeting system, then shortly thereafter be *retrained* on a new *prospective* budgeting methodology. Also previously converted data would have to be re-converted to accommodate the change in budgeting methodology.

Deferment of QR/PB implementation is one alternative; but obtaining the necessary waivers could prove difficult and would delay statewide implementation of a change that is designed to improve Food Stamp performance. Another alternative is overriding or disabling much of the CalWIN functionality for eligibility determination/benefit calculation (EDBC) and devising, if possible, a viable manual workaround. However, this workaround will have more severe problems than other workarounds because the loss of so much existing functionality will require considerable manual processing. A sufficient extension of the schedule will have the advantage of providing the necessary time to implement the QR/PB change while enjoying the maximum intended-benefits of the change.

4.3 Recommendations

GovConnect recommends that the project schedule be adjusted to include the time and resources necessary to incorporate the impending policy changes, including QR/PB, prior to deploying the Application to the Pilot Counties for use in a production mode for service delivery.

The Project stakeholders and the development/implementation vendor must re-evaluate the project schedule to include the implementation of QR/PB into the Application. Several factors must be considered before an anticipated date for Pilot implementation can be determined. Some of those factors are:

- Change Request 1513 (QR/PB) must be approved. The final ACL must be available before the design sessions and the Detailed Impact Analysis can be completed and approved.
- QR/PB must be incorporated into CDS regardless of CalWIN timelines.
- The impact to conversion must be clearly understood and fully tested. This may include an additional full load conversion test prior to go-live using prospectively budgeted data.
- The UAT of this change is significant. Most, if not all, components of CalWIN must be retested to ensure that they are functioning as originally scoped if no change was made, or as newly designed if impacted by QR/PB.
- The impact to training of implementing QR/PB is significant. Training materials must be revised. Trainers and Pilot staff who have attended training must be re-trained. The training environment must reflect an adequately tested Application. UAT and end-user training cannot be concurrent activities.

Given the complexity and impact that this major policy change will have, a significant effort to re-scope the Project must occur and it must be completed in the most expeditious manner.

In addition to providing the necessary time to implement the QR/PB change, this extension would provide the Project with additional time to pursue risk mitigation opportunities in *other* areas of the Project including Conversion, Interfaces, and Training. Areas identified as having a County knowledge gap could be addressed as well. These areas include Application Architecture/Reference Tables, Client Correspondence, Management Reporting, and County Information Server/Ad Hoc Reports.

4.3.1 Assumptions

The following assumptions are associated with the above recommendations:

- The development/implementation vendor will be available, on short notice, to re-evaluate the project schedule.
- The WCDS Director's Conference will approve the required changes to scope, schedule, and cost.
- A change to the CalWIN Technology Agreement will be made to increase the term of the Agreement.
- The current UAT efforts will immediately be reevaluated to determine the components that are not impacted by the scope changes and those activities will be completed within the existing UAT phase.
- The concerns regarding the current UAT efforts will be addressed in order to ensure that improvements to communication, project reporting and decision-making processes are discussed, incorporated and refined.

4.4 Additional Benefits

The schedule adjustment recommended in section 4.3, Recommendations, would provide additional benefits to the Project by allowing more time to successfully mitigate other project risks already identified in the CalWIN Risk Management Plan. These risks include:

- Technology Migration;
- Mission Critical Interfaces;
- Implementation of Rolling Wave Approach; and
- Transitioning to Joint Maintenance Procedures.

4.4.1 NumaQ Technology Migration

Delaying the project schedule would provide the following benefits to the Project, in relation to the risk associated with NumaQ Technology Migration:

- Allows for developing a Detailed Migration Plan that takes into consideration possible delays due to technical problems;
- Allows the EDS Development and System Test team adequate time to test the CalWIN Application on the new platform;
- Allows the WCDS CalWIN UAT team adequate time to test the CalWIN Application on the new platform;
- Allows the EDS Systems Support Team adequate time to gain experience on the new architecture and to thoroughly System Test the processes and procedures for managing the new system. It also allows the WCDS CalWIN UAT team to test these processes and procedures to ensure they are at an acceptable maturity level for Pilot; and

- Allows time to update CalWIN deliverables, work products, and processes and procedures affected by the new platform.

4.4.2 Mission Critical Interfaces

With the complexity and number of State and County Interfaces being implemented in CalWIN, it is imperative for the CalWIN Project, as well as State and County Interface Partners, to have a clear understanding of the interface functionality. To-date many steps have been taken to establish clear communication and information exchange. However with the large number of changes implemented in CalWIN since Detailed System Design, some of which directly impacts the Interface Partners, neither the Application nor Interface designs have stabilized.

In particular, the lack of stability in the Interface design has been a challenge for the CalWIN Project and especially the CalWIN Interface Track and Interface Partners. Even though Interface changes are reviewed by Interface Partners and approved by the Counties, they tend to create funding, procurement and timing issues. These kinds of issues can increase the risk that the interface will not be thoroughly tested.

A benefit that would be realized from a schedule extension would be the ability to stabilize the interface design, increase communication with interface partners and ensure each interface is thoroughly tested prior to Pilot implementation. An additional step that would be recommended during a delay would be to do completed interface testing using a full load of conversion data from each of the Pilot Counties. Full load conversion interface testing would ensure that as many data and software issues are discovered and resolved as possible. A full load conversion interface test is currently being planned for Placer County; however, with the current schedule constraints and a major system release scheduled to be in CalWIN UAT in mid-December 2002, concerns exist regarding the amount of focus that can be directed to the full-load interface testing prior to the currently scheduled Placer County Pilot implementation date.

4.4.3 Evaluation of UAT Rolling Wave

An outstanding Change Request that should be reviewed and included in any type of re-scope of the project timeline is Change Request 417 "Rolling Test Wave". Change Request 417 calls for the review of the UAT approach and timing for County-specific functionality such as GA/GR, County-specific Interfaces, County data conversion logic, County-specific client correspondence as well as County-specific process controls.

The current schedule requires all testing for all Counties to be completed prior to the beginning of consortium-wide implementation. A Rolling Wave approach would move County-specific UAT and Conversion Tests closer to their respective Go-Live dates. This approach could mitigate a number of risks identified in the CalWIN Risk Plan, specifically in the areas of external agency interface readiness; potential changes to County data and County systems between the current test window and Go-Live; and County-specific test needs.

The Rolling Wave approach should be revisited during the re-scope of the project timeline. There may be an opportunity to test some of the County-specific functionality for the early implementing Counties. There also will be an opportunity to better understand the ongoing County UAT environment and develop processes and procedures regarding future releases of the Application at the same time other Counties are testing for their implementation.

4.4.4 Transitioning to Joint Maintenance Procedures

As CalWIN transitions from the Development to the Maintenance Phase of the Project, it is imperative that WCDS Consortium Facilities Maintenance and Operations (FM&O) procedures be established. The FM&O Workgroup has proposed a model for ensuring that regulatory changes and enhancements are implemented in a timely manor in the CalWIN Application. Requests for system enhancements will increase from the current CDS/WICAR environments, due to the fact that a highly automated system such as CalWIN will require additional changes as a result of modifications to regulations.

Under the Maintenance organizational structure proposed by the FM&O Workgroup, CalWIN Managers would provide direction on, and priority of, issues referred to subcommittees. The new proposal calls for the election of Chairs and Vice-Chairs of each subcommittee and the designation of Oversight Managers to support the Chairs in managing assignments. It also recommends that each subcommittee have Action Teams appointed to complete the assignments given to the subcommittee. Each Action Team will select a leader and be comprised of various Counties to ensure balance.

The FM&O Workgroup has made strides in preparing the Consortium for CalWIN maintenance. A project schedule extension would allow time for the FM&O structure to be put in place and stabilized prior to Pilot implementation. This would provide direct influence by Counties on the CalWIN change and release processes. An extension would also provide time for the interaction between the Subcommittees and the Project to be institutionalized.

4.5 Next Steps

It is imperative that a consensus on the desired direction of the Project be quickly reached by the CalWIN stakeholders in light of this Risk Assessment Report. If the CalWIN stakeholders choose to follow the GovConnect recommendation (which includes a schedule adjustment) or implement any other option that includes a schedule adjustment, a number of activities must be initiated immediately:

- Examination of current Project and Stakeholder activities/priorities;
- Re-scope of the project timeline; and
- Preparation and submittal of an Implementation Advanced Planning Document Update (IAPDU).

All resources including development/implementation vendor, WCDS CalWIN Team, and Pilot Counties are focused on activities required for Placer County to "go-live" on February 3, 2003. If a schedule adjustment is to be implemented the timing of these activities must be quickly reassessed. In addition, any risk mitigation opportunities being considered must be reanalyzed based on the current resource plans and activities.

An example of the review that needs to take place is in regard to current project actions to test, clarify, modify or correct CalWIN logic that is going to be impacted, revised or replaced due to the implementation of QR/PB or other regulatory changes. If there is a schedule adjustment many of these resources should be refocused on the analysis, design, test and eventual implementation of QR/PB and the other required regulatory changes.

It is imperative that a policy and process be established to allow for freezing the Application design at a reasonable point-in-time prior to a County's "go-live" date. This will ensure that the *adjusted* project timeline does not encounter the same level of risk due to the volume and magnitude of regulatory changes. The Policy must include a process to unfreeze and refreeze as

appropriate, based on the various County "go-live" dates and their required functionality. In addition the *adjusted* project timeline must engage the FM&O transition plans. By fully engaging these plans, the CalWIN Joint Committee and County staffs will be fully involved and have first-hand knowledge and control over the Release Management Process prior to implementation.

As mentioned above, timing of any project schedule adjustment must be done quickly. A schedule adjustment will impact current and future State fiscal year budgets and activities, thus requiring the preparation of an IAPDU. In order to prepare the IAPDU for adjustments to the 2003/2004 fiscal year budget, agreement on the re-scoped project timeline, as well as it's fiscal impact, must be documented and in-place by January 2003.

Appendix A. ACL and Change Assessment Matrix

A.1 ACL Changes

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
241		IHSS (Eligibility for PCSP individuals	4871			Yes	High.	Yes for Medi-Cal	Yes	Yes	Not ACL driven, however CalWIN will be non-compliant with current regulation.
560	ACWDL 01-40	CEC Program Revisions in CEC period and CEC guarantee period.	471			Yes	Low. When a child is eligible to CEC, then the aid code and SOC will need to be overridden in CalWIN. NOA's will be manual and the CEC periods will have to be tracked outside of CalWIN.	Yes. Medi-Cal SOC could be incorrect.	Potential	No	

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
982	ACWDL 01-59	Retroactive Medi-Cal applications for SSI/SSP PD recipients in appeal	88			Yes	Medium. Users will need to override the Retro-Medi-Cal determinations to pending until the final SSI/SSP appeals determination is made. When the final determination is made, if they are denied the appeal, then EDBC will need to be reran for those retro months and approved or denied based upon EDBC determination.	Yes if the Retro Medi-Cal SOC is incorrect.	Potential	Yes	
997	ACL 01-57	Safe at Home (ACL 01-57)	200			No	Low	No	Potential	Yes	Counties can implement a business process to accommodate this change.
1010	ACWDL 00-56	Medi-Cal Personal Care Services Ded	897	135		Yes	Medium. Individuals in a Board & Care facility and eligible to a Personal Care Services deduction for Medi-Cal will need to have a manual budget completed and the results overridden in CalWIN. All NOA's will be manual.	Yes	Potential	Yes	

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
1128	CFL 01/02-01	Revision of CA800 EA (FED), DFA881 (FED) and CA800FC (non-fed) forms per CFL N0. 01/02-01 Supplemental Clothing Allowance changes to claim forms.	307			Yes	Medium. Report will be formatted incorrect and will not contain all the information required. Perhaps an ad hoc report would need to be run to gather the new elements for this report and a manual report could be created using the new format.	No	No	No	
1129	CFL 01/02-52	Change to State Report CA 800KG (FED) CFL N0. 01/ 02-52	231			Yes	Medium. For CalWIN this requires a change to the extract, a format change and a change to the county process control table. Report will be formatted incorrect and will not contain all the information required. A manual report could be created using the new format.	No	No	No	

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
1137		Medi-Cal Hunt v Kizer Adjustments to Sneede v Kizer MBU's			200	Yes	Medium. When a person has Hunt v Kizer adjustments to make and there are multiple Sneede MBUs with SOCs where that person is either a member or a responsible relative, the person may use the Hunt v Kizer adjustment to reduce the SOCs of any of those MBUs. Currently CalWIN only applies the Hunt v Kizer adjustment to the MBU where that person is a member. Overrides will be required in this situation as well as manual NOA's.	Yes for Medi-Cal SOC	Potential	No	This is not ACL driven, however CalWIN may be out of compliance without this change.
1355	ACL 02-51	Revision of STAT 46 per ACL NO. 02-51			250	Yes	Medium. Report and data will be incorrect. The new report will need to be manually completed using the actual expenditures.	No	No	No	The counties considered this to be a showstopper No Go item.

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
1367	MEM 264	No resource test for TMC or 4 month continuing	475	95		Yes	Medium. If a TMC or 4 month continuing case fails for excess resource, this determination will need to be overridden in EDBC and manual NOA's will be required.	Yes if cases are discontinued in error.	No	No	The counties considered this to be a showstopper No Go item.
1407	ACL 02-62	ACL 02-62 FS COLA & Standard Deduction change	300	75		Yes	High. The majority of FS HH will have incorrect benefits and will require a manual budget and override. HH's with 4 or more will also be impacted for the Standard Deduction. Manual NOA's will be required.	Yes	Yes	No	
1434	ACL 02-33 & 02-70	ACL 02-33 & 02-70 California Work Opportunity and Responsibility to Kids (Cal WORKS) Regulations for 60-Month Time Limit Procedures.			1000	Yes	Medium. New Forms will need to be shelf stock. New NOA's will need to be manual. EDBC will not be able to set the triggers required by Client Correspondence so the user will need to set their own alerts for when to issue the NOA or Form.	No	No	No	This is important for Sacramento to have these triggers in place. Initially there will be approx. 6000 cases impacted and then 600 - 1000 monthly thereafter. This is a No Go item.

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
1437	ACL 02-17	ACL 02-17 Non-Citizen Eligibility and Certification Provisions			350	Yes	Low. New DFA 386 & 387 forms will need to be shelf stock. The revised NOA will need to be manually generated.	No	No	No	
1443	ACL 02-36	Periodic Reporting Change for CalWORKs when child is receiving Out-of-Home care for CalWORKs reunification cases.			2000	Yes	High. For CalWORKs, the grant needs to be overridden to $0 if no other children are in the home or if financial eligibility fails due to income of remaining AU members. The child will be entered as temporarily out of the home so eligibility passes. Periodic reports will continue to go out and be tracked in CalWIN and will need to be logged in as received, even though they are not required for reunification CalWORKs Services only cases. WTW Sanctioned individuals are able to participate immediately and the time counts towards the sanction period so the sanction will need to be	Yes.	Potential	Yes	CalWORKs services only need to be provided. This is a No Go item.

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
							lifted in order for CalWORKs services to be entered into CalWIN. The 18/24 and 60 month clocks will probably need to be overridden. Budget will need to be manually calculated the overridden. FS will need to be overridden based upon the CW budget. NOA's will be manual				
1459	ACL 02-66, 02-69, CFL 02/03-29	ACL 02-66 & 02-69 Safety Net program in CalWORKs	692	133		Yes	**High**. An override will need to be performed for the new aid codes. NOA will be manual. There are additional changes anticipated for the treatment of income. There are changes to the CA 237 CW report that will need to be manually entered.	Yes	Yes	Yes	

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
1477	ACL 02-45	Change to AFDC-FC Property limit to $10,000	250	30		Yes	Medium. If the FC determination fails due to over property limit and the child has property less than $10,000 then an override will be required to pass the case. NOA will be manual if required.	Yes	No	Yes	
1480	ACL 02-63	ACL 02-63 Sponsor Deeming Changes in CAPI			500	Yes	High. Any income or resources being deemed inappropriately for CAPI would need to be overridden in EDBC as well as any related FS that the CAPI grant is used in. NOA's would be manual.	Yes	No	Yes	This will be an issue for Sacramento, who processes CAPI cases for Placer and many other counties.

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
1481	ACWDL 02-37	ACWDL 02-37: CalWORKs and Medi-Cal DA Cooperation			700	Yes	High. Eligibility determination for Medi-Cal when an individual does not cooperate with DA Family support for CalWORKs will need to be overridden to an "IE" status. A MEDS on-line translation would need to be done to report the appropriate restriction code to identify individuals subject to the CalWORKs 25%penalty and a manual NOA will need to be sent.	Yes	Potential	Yes	
1486	ACWDL 02-44	ACWDL 02-44 $240 Disability income deduction for Medi-Cal 1931b. CR#1064 was combined with this change for the impact to conversion.	600	70		Yes	High. For 1931b (Alternative B) determinations, a manual budget will need to be done and the MC SOC overridden if needed. NOA's will be manual. This ACWDL applies also to Sneede cases.	Yes	Yes	Yes	

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
1487	ACL 02-58 & 01-85	Additional FC Placement Type	800	70		Yes	Medium. Without the new Foster Care placement type, the Non-relative Extended Family Member would need to be entered as a Foster Home used only if the approval documents have been received. If the approval documents have not been received, then another action would need to be taken to fail the Fed/State determination and authorize County funds.	Yes.	Yes	Yes	This impacts County Funds for Foster Care and is considered critical.
1495	ACWDL 02-40	ACWDL 02-40: Disability evaluations under SB87			400	Yes	Medium. For those cases which do not roll into a "38" aid code for Medi-Cal, an Override will need to be done on the eligibility result and aid code. NOA's will be manual.	Yes	No	No	
1496	ACL 01-71, 01-89, 02-44, 02-71	Changes to WTW25, WTW25A and WTW30 (ACL 01-71, ACL 01-89, ACL 02-44 and 02-71)			200	Yes	Medium. Without the changes to the extract, the reports will be incorrect. An ad hoc may need to be run to capture the elements needed and the reports completed manually.	No	No	No	

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
1502	CFL 02/03-16	Changes to State reports AD 800A (MRS002R) and CA 800FC (FED) (MRS022R) per CFL 02/03-16			200	Yes	Low. These reports will be incorrect due to the decrease in the FMAP rate. A manual calculation and manual completion of the report will be required.	No	No	No	County funding involved.
1516	ACL 02-74	Tracking Child Support Collections and Overpayments for CalWORKs 60 month Time Limit.			2000	Yes	High. The user will need to manually determine if there is an O/P to apply the recoupment amount prior to applying the recoupment to the aid payment and manually untick the clock as appropriate.	No	Potential	Yes	WDTIP does not have this information, there are a large number of cases impacted and the interface with child support will not function.
1523	ACWDL 02-22 & 02-22E & ACWDL 02-38	Cost of IHSS deduction for A&D FPL program. Questions & Answers about the A&D FPL program.			650	Yes	High. Overrides will be necessary in EDBC so that the deductions are applied appropriately for Medi-Cal. NOA's will be manual.	Yes	No	Yes	

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
1526	ACL 02-22 & 02-67	ACL 02-22 eliminates the sunset date for CFAP. ACL 02-67 is part of FS reauthorization and restores Federal benefits to Legal Non-citizens and increases resource level to $3000 for HH with disabled members.			800	Yes	High. Overrides will be necessary in EDBC for Food Stamp resources for certain disabled members & for funding for State/Federal Food Stamps tracking.	Yes.	No	No	
	MEM 266	Article 8G Medi-Cal Family Budget Unit Determinations for 1931b program.			500	Yes	Medium. Worker would need to determine if Parents and Minor Parents should be included in same case or not and override as needed. Manual NOA's will be needed.	Yes for Medi-Cal	No	No	
	MEM 267	Article 8G Medi-Cal Family Budget Unit Determinations for 1931b program.			0	Yes	This will be included with MEM 266.	No	No	No	

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
	ACIN 1-39-02	Wraparound and CalWORKs Eligibility.			50	Yes	Medium. This is an income type and if the income type is not in the table, then the income amount used to determine the CalWORKs grant will need to be overridden, or another income can be used that will be budgeted correctly for CalWORKs & FS. If overridden, manual NOA's will be required.	Yes.	No	No	
	ACIN 1-56-02	Food Stamp Reauthorization Act of 2002.			750	Yes	High. There are two portions that have not been addressed in other changes. 1. Federal benefits for legal non-citizens who have been in the US for 5 or more years will be restored to federal benefits effective 4/1/03. 2. Legal non-citizen children will be restored effective 10/1/03. For the 4/1/03 effective date, EDBC non-financial determinations for CFAP individuals may need to be overridden. NOA's will be manual.	Yes. Due to mixed HH and pro-rations for FS.	Potential	No	

CR #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Work-around	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Materials Impact	Notes
	ACL 02-55	Budgeting Policy changes in the Food Stamp program regarding the SUA and offsets to SSA Benefits. Effective 10/02			250	Yes	High. In cases where SUA proration is incorrect, the FS budget will need to be overridden. NOA's will be manual.	Yes	Potential	No	
	ACIN 1-70-02	Treatment of Americorps and Volunteer Service to America (Vista) payment in CalWORKs.			50	Yes	Medium. For this type of income, the user will need to select the Vista payment for it to be treated correctly, or an override will need be done and NOA's will be manual.	Yes.	No	No	Possible RT impact.

A.2 Other Application Changes

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
888		WDTIP Reports	70			No		Yes	No	Yes	If an individual is exceeding their time limit and is not discontinued, an O/P could result.
1044		Sponsor Deeming for Income & Resources for FS, Resources for CalWORKs, and Resources for some GA/GR programs.	1892			Yes	High. In deeming situations, EDBC will need to be overridden and NOA's will be manual.	Yes for CalWORKs & FS	Possibly	Yes	
1078		Mass Updates of DC Records	382			Yes	Each time there is a COLA increase, the user will need to update the income records for cases impacted.	Yes	No	No	
1086		Immediate Need Reasons - verification fields	827			Yes	Low. For immediate need a valid verification source needs to be entered for immediate need to pass.	Yes	No	Yes	

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1096		Overpayment Alert/Notification	258			No		No	No	No	
1097		Time Limits for Foster Care Voluntary Placements	50			Yes	High. If the time limit has exceeded, EDBC will need to be overridden and County funds authorized. NOA's will be manual.	Yes	No	No	
1119		30 State Budgets that need to be coded.			300	Yes	Medium. NOA's would need to be manual.	No	No	No	
1136		CMIPS ability to process the Conversion Cross Reference file. Add CIN to CMIPS	915			No		No	Yes	No	
1138		Medi-Cal SSA Cola Disregard for certain Medi-Cal programs	108			Yes	Medium. For certain Medi-Cal programs, EDBC results will need to be overridden for a certain months. NOA's will be manual.	Yes	Possibly	No	

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1143		FS POI durations	60			Yes	Medium. For transfer of resource POI's, the EDBC POI period will incorrect and need to be calculated and tracked manually and the NOA indicating the period of the POI will need to be manually issued.	Yes	No	No	
1144		FS Income prorations for ineligible aliens	40			Yes	Medium. EDBC results will need to be overridden and NOA's will be manual.	Yes	No	No	
1149		EFT CalWIN Direct Deposit for CDS Counties	9272	696		Yes	High	No	Yes	No	

Change Request# (CR) #	ACL	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1159		Foster Care Correspondence Address				Yes	High. In fact there may not be a workaround. FC payments, Notices and correspondence will be addressed to the child and not the provider.	No	Yes	No	Fast Track
1180		Higher MAP Amounts				No		No	No	No	The current grant table will accommodate Placer & Sacramento, however the structure needs to be done to complete UAT. Fast Track

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1188		Viewing of amount Authorized as County Funds for FC				Yes	Medium. When the County wishes to issue an amount for County Funded FC that is different than what the State/Fed amount would have been, the user will need to override the grant amount and issue manual NOA's.	No	No	Yes	Medium. When the County Funds authorized amount is different than what the State/Fed amount would have been, the County authorized amount does not display to the user and could cause confusion and misinformation to the provider. Fast Track
1193		Search Hearings by Case Number				Yes	Low. Users will need to search for an individual instead of a case.	No	No	No	Fast Track

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1197		1931b Recipient Evaluation Test				Yes	High. When a case contains Sneede class members and has excess income. Manual 1931b recipient tests would need to be computed to determine if EDBC results are correct and if not the results will need to be overridden and manual NOA's used.	Yes for Medi-Cal	No	No	Fast Track
1198		System Generated Appointments standard durations.			412	No		No	No	No	
1199		Granted Diversion with Medi-Cal and Food stamps			425	Yes	Medium. The Medi-Cal Aid Code will need to be overridden in EDBC and the NOA will be manual.	No	No	No	

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1208		RRR Duration for Non-monthly ES FS households				Yes	RRR duration will need to be manually tracked and NOA will need to be manual.	Yes	No	No	Non-monthly reporting ES HH could receive additional months of FS. Fast Track
1209		SFIS Compliance			75	No		Yes	No	Yes	
1210		Minor Parent CA25	105			Yes	Low. When there is a minor parent the user will need to indicate the CA 25 has been received when the minor parent is the applicant.	No	No	No	
1211		Pregnancy Special Needs				Yes	Medium. When an individual is pregnant, the user will need to request special needs instead of automatically receiving them if eligible.	Yes	No	Yes	Fast Track
1214		Confidentiality Concerns when parents of Minor Consent are given a CWIN				No		No	No	No	Confidentiality issues and recommend as needed prior to pilot. Fast Track

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1217		Assigning Multiple Workers for a CalWORKS, PA Food Stamp, and Cash-linked MediCal case				Yes	Medium. Counties will need to manually reassign cases to the same worker.	No	Yes	No	Fast Track
1222		NA 960 X NOA for Food Stamps				Yes	High. For food stamps, each 960X NOA will need to be manually generated.	Yes	No	No	The payment error will be in the client not receiving adequate notice Fast Track
1225		Special Needs RT structure change				Yes	High. Non-recurring special needs will need to be manually budgeted for each person and the grant then overridden and manual NOA's sent.	Yes	No	No	Fast Track

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1226		Field Label On Absent Parent & Pregnancy Window				No		No	No	Yes	In order for these fields to be clearer for the user and to ensure that the CA2.1 is populated correctly and the high usage of these fields, this should be included for pilot. Fast Track
1257		9.4.1 CVESD0R Report Change. Display of old CDS aid-type on this conversion report.				No		No	Yes	No	Fast Track
1268		SMART Conversion X-REF file	153			No		No	Yes	No	
1279		APS 15.6.17--New Window for BV to capture and report summary and detail level information for referral tracking.				Yes	Medium. Counties will need to run an ad hoc query to receive this report.	No	No	Yes	Fast Track

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1280		18/24 Month Time Clock for WTW				Yes	High. The user will need to manually adjust the 18/24-month clock.	No	No	No	Fast Track
1283		Additional Fields to Collection Send File Layout	322			No		No	No	No	Additional elements for VACS, CUBS & Sacramento
1288		Treatment of unverified Income and Resources			412	Yes	High. Unverified income & resources need to be used for prospective eligibility tests and budgeting during the initial determination. EDBC results if incorrect in this situation will need to be overridden and manual NOA's issued.	Yes	No	No	
1306		DPR RD 2 Changes Requested by Placer Co.			412	No		No	Yes	No	

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1335		Employment services integration	278			Yes	Medium. If the user knows the case # but not the SSN# they will need to go to inquiry to get the SSN of the individual they wish to access ES information for.	No	No	Yes	
1337		GA/GR NOA Backs and County Name of Program	221			Yes	High. This would require all NOA's and letters that do not have the correct backs be manual.	No	No	No	The workaround is not acceptable for the pilot counties. This is too much of a workload impact.
1342		Conversion PC Merge Logic change	175			Yes	High. Cases would need to be identified at conversion to be evaluated for this situation.	Yes	Yes	No	
1350		Multiple Mileage Rates	152			Yes	High. Mileage rates will not be computed correctly and will need to be overridden.	Yes	No	No	This requires an update to the reference table structure

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1353		Testing Client Correspondence in Maintenance			946	Yes	High. There is currently no workaround other than to test the new or revised forms in production.	No	No	Yes	This has a high risk and should be implemented before pilot.
1377		Reconciling Regional Market Rates for Child Care categories and reporting requirements				No		No	No	No	The need for duplicate entries and the fact that this table is a large and complex table that requires updating annually, it is recommended to have this change for pilot. Fast Track
1379	PUAT 20	Multiple payment types for supportive services	298	72		Yes	Minor. Additional RT values to identify multiple issuance types for a service type. E.g., Child Care-Voucher, Child Care-Warrant, etc.	No	No	No	

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1390		AR1010N Collect Application Information			412	No		No	No	Yes	The location of the Special Circumstances question is being relocated from the immediate need group box to it's own groups box.
1397		SMART Interface - Minor Consent	90			No		No	No	No	This is a modification to the interface file to include a Special Indicator on minor consent records in the SMART Interface file.
1402		Child Support Full load Conversion Request for Sacramento	818			No		No	No	No	This impacts Sacramento Co. only.

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1403		Program Status Indicator on Claim Cross Reference Conversion File & Case/Program/Person Status to the Child support conversion Cross-Reference file.	223			Yes	High. Manual analysis will be needed to determine the status of the claim for collection systems and the status of individuals for child support systems.	No	Yes	No	
1410		Manual conversion of non converted cases			412	Yes	High. Converted cases that are in retrospective budgeting will be changed to prospective budgeting, which could cause incorrect determinations. In addition, when a case is manually converted, a new application must be registered in CalWIN and currently that	Yes	Yes	Yes	

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
							application will be counted as a new application and should not be. The original application date should be used, however if it is used, EDBC will begin running from the first month of conversion in the County. This could be incorrect and cause duplicate benefits to be issued. EDBC should begin running with the future month for converted cases.				
1412		Conversion - Placer DPR 3 Changes	448			No		No	Yes	No	
1413		Conversion - Modify Exception Reports-All County	794			No		No	Yes	No	

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1421		Inclusion of Agency/Provider name in CR search results				No		No	No	Yes	There is currently no way to view the provider name when doing a search in client referral. Fast Track
1431		CDS Conversion - change in data validation rules	936			No		No	Yes	No	
1454		WDTIP Exception Messages that Require Caseworker Attention			412	Yes	Low. Users will need to check the WDTIP exception window for error messages on a regular basis.	No	No	Yes	
1465		Inquiry Only Web: New Requirements	415	101		No		No	No	No	This is important for certain partners to view needed information.
1467		Notices of Action for Approval through Future Month			412	No		No	No	No	Without this change, NOA's will be confusing and misleading to the client.

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1471		Changes in the Application Registration Process	1071			Yes	High. Clerical staff would need to be trained to ask all the questions up front before the SAWS1 is signed.	No	No	Yes	The issue with the workaround is that an individual can request emergency services for CalWORKs anytime during the application period.
1485		Alerts for cases with multiple workers			412	Yes	High. When a worker runs EDBC, they will need to send an alert to the other workers on the case. If the case runs in batch, the only worker notified is the worker that made the change.	Yes	No	Yes	

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1490	PUAT 248	BDOA - Program request date				Yes	High. When EDBC is run on-line the worker will need to adjust the EDBC run date on the Run EDBC window. When the case is run in batch and the incorrect BDOA date is used, results will need to be overridden and manual NOA's issued.	Yes	No	Yes	Fast Track
1491		Registry Entries for SQL Server				No		No	No	No	Fast Track
1497		Foster Care Expenditures/Two New Reports			412	Yes	Medium. The two new reports can be manually completed using the current report being generated.	No	No	No	This has to do with claiming and the pilot counties feel this should be included.
1499		Placer Baseline Changes				No		No	No	No	Fast Track
1500		Sacramento Baseline Changes			412	No		No	No	No	

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1501		Medi-Cal property disregard applications	1133	209		Yes	Medium. For cases that should have been evaluated for Medi-Cal property disregard, an override may be required.	Yes	No	No	
1514		Unable to Clear User ID			412	Yes	High. If the user is locked out, the help desk needs to be notified and the database table cleared out.	No	No	No	
1517		Worker Table Conversion Schedule	54			No		No	Yes	No	
1522		Placer GA/GR NOA Budget				Yes	Medium. GA/GR NOA's & budget calculations will need to be manual.	No	No	No	Fast Track

Change Request (CR) #	ACL #	Title/Description	Change Hours	DIA Hours	Est. Hours	Requires Workaround	Degree of Difficulty	Potential Payment Errors	Conversion Impact	Training Impact	Notes
1528	PUAT 1476	Allow provider to be non-mandatory and freeform on the Medical Expense Detail window.				Yes	High. Any medical expense will need to have the provider information entered via the provider windows in CalWIN so it appears in the dropdown.	No	No	No	Fast Track
1530		Conversion. Sacramento Co. has requested changes for DPR3			412	No		No	Yes	No	

Appendix B. Assumptions Approach

B.1 Introduction

To determine the number of months required to complete the change requests related to ACLs as well as the other changes needed by Placer County Pilot, GovConnect performed the following tasks:

- Sampled Detailed Impact Analysis (DIA) of existing change requests to determine critical path;
- Estimated vendor hours to complete all required change requests (including analysis, design, code, unit test, and system test);
- Estimated vendor resource availability;
- Assumed vendor resource utilization of 200 hours per person, per month; and
- Calculated total months to complete required change requests through System Test.

The following paragraphs describe each of the above tasks in detail.

B.2 Sampling Existing Change Requests to Determine Critical Path

GovConnect sampled the DIAs of twelve significant change requests (i.e., hours greater than 150) to determine the distribution of hours across the various EDS resources. This exercise showed that the vast majority of hours (77%) were associated with the positions of Programmer Analyst and Tester. Thus the design, coding, and testing activities were identified as the critical path.

B.3 Estimating Hours to Complete Required Change Requests

GovConnect estimated the total vendor hours to complete all required change requests (including analysis, design, code, unit test, and system test) using the approach described below.

When available, GovConnect used the Impact Analysis (IAs), Preliminary Impact Analysis (PIAs) and DIAs of the required change requests to retrieve total estimated hours to complete the associated change requests.

For each ACL change without an associated IA, PIA, or DIA, GovConnect estimated the total hours based on existing estimates of similar changes as well as our experience and familiarity with the CalWIN Application and its requirements.

For each non-ACL change without an associated IA, PIA, or DIA, GovConnect used an average number of hours based on the sampling performed in the previous paragraph. "Fast Track" changes were not assigned any hours for the purposes of these calculations.

All hours were accumulated in a spreadsheet and totaled by the type of change request:

ACL	21,640 hours
Other Application	29,328 hours
Total	50,968 hours

Because the change request sampling described earlier indicated that 77% of the total hours are associated with the critical path activities of design, coding, and testing, the total hours calculated above was reduced by 23%:

Total hours	50,968 hours
Non-critical path hours (23%)	-11,723 hours
Critical path hours	39,245 hours

The total critical path hours above include EDS hours associated with UAT and Training Support. To account for critical path hours through System Test only, GovConnect reduced the total critical path hours based on the assumptions that 15% are associated with UAT Support and 5% are associated with Training Support:

Critical path hours	39,245 hours
UAT support (15%)	- 5,887 hours
Training support (5%)	- 1,962 hours
Critical path hours through System Test	31,396 hours

B.4 Estimating EDS Resource Availability

GovConnect used the EDS Staffing Chart, dated 6/18/02, to estimate monthly staffing based on the availability for the month of December 2002. Since the positions of Programmer Analyst and Tester are the key resources associated with the critical path activities of design, coding, and testing, the December 2002 resource availability for those positions (i.e., 33 Programmer Analysts and 4 Testers for a total of 37 resources) was used for the EDS resource availability estimate and was assumed to be constant.

B.5 Assumed EDS Resource Utilization of 200 Hours per Person, per Month

Based on EDS estimates, GovConnect used a resource utilization (i.e., burn-rate) of 200 hours per person, per calendar month.

B.6 Calculate Total Months To Complete Required Change Requests Through System Test

Based on the fact that the critical path activities are design, coding, and testing, the following calculations use only the design, coding, and testing resources (i.e., 33 Programmer Analysts and 4 Testers for a total of 37 resources):

Num_Resources/Month * Burn_Rate = Total_Hrs_Burned/Month

37 * 200 = 7,400

Critical_Path_Hrs_Thru_ST / Total_Hrs_Burned/Month = Total_ Months

31,396 / 7,400 = 4.2

Deliverable #28

Final Assessment of Conversion Plan Tasks Complete Wave 1

December 2, 2009

TABLE OF CONTENTS

1. RECORD OF CHANGES 1
2. INTRODUCTION 2
3. Related Documentation 2
4. Quality Assurance Review Activities 3
5. Deliverable Assessment Methodology 3
5.1. REVIEW OF VENDOR DED 5
5.1.1. Requirements Analysis 5
5.1.2. Comments and Feedback 5
5.1.3. Recommendations 5
5.2. REVIEW OF VENDOR DRAFT DELIVERABLE 5
5.2.1. Adherence to DED 6
5.2.2. Requirements Analysis 6
5.2.3. Deficiencies Analysis 6
5.2.4. Recommendations 6
5.3. REVIEW OF VENDOR FINAL DELIVERABLE 6
5.3.1. Adherence to DED 7
5.3.2. Requirements Analysis 7
5.3.3. Deficiencies Analysis 7
5.3.4. Recommendations 7
6. Deliverable Assessment Findings 7
6.1. REVIEW OF VENDOR DED 7
6.1.1. Requirements Analysis 7
6.1.2. Comments and Feedback 11
6.1.3. Deficiencies Analysis 11
6.1.4. Recommendations 11
6.2. REVIEW OF VENDOR DRAFT DELIVERABLE 11
6.2.1. Adherence to DED 11
6.2.2. Requirements Analysis 13
6.2.3. Deficiencies Analysis 16
6.2.4. Recommendations 16
6.3. REVIEW OF VENDOR FINAL DELIVERABLE 16
6.3.1. Adherence to DED 16
6.3.2. Requirements Analysis 18
6.3.3. Deficiencies Analysis 21
6.3.4. Recommendations 21
7. Acceptance Recommendation 21
8. Deliverable Roles and Responsibilities 22
9. Deliverable Schedule 23
10. Deliverable Requirements 24
11. Deliverable Assumptions 25
12. Appendix A – Material and Cosmetic Deficiencies A-1

1. RECORD OF CHANGES

REVISION DATE	AUTHOR	SUMMARY OF CHANGES (INCLUDING SECTION/PAGE NUMBERS)
11/19/2009	Kristin Summers	Initial Draft
12/02/09	Kristin Summers	Final Draft

2. INTRODUCTION

This Deliverable, Assessment of Wave 1 Conversion Plan Tasks Complete – Deliverable #28, documents the approach and deliverable review and assessment activities that were performed by FDGS over the course of the Wave 1 Conversion Plan Tasks Complete development lifecycle. The target audience of the Assessment of Wave 1 Conversion Plan Tasks Complete Deliverable is all stakeholders (Application Vendor, Consortium Management, Business Analysts, County Project Managers, and QA Team) that will be impacted by the assessment.

3. RELATED DOCUMENTATION

The following documents were used and/or referenced in completion of this review:

- Accenture Deliverable #77 – Final Wave 1 Conversion Plan Tasks Completed, dated November 30, 2009
- Accenture Deliverable #77 – Draft Wave 1 Conversion Plan Tasks Completed, dated September 14, 2009
- Accenture Deliverable #77, 87 & 95 – DED for Wave 1, 2 &3 Conversion Plans, dated August 19, 2009
- Accenture Deliverable #64 – Draft Wave 3 Conversion Plan, dated January 28, 2009
- Accenture Deliverable #64 – Final Wave 3 Conversion Plan, February 26, 2009
- Accenture Deliverable #53 – Draft Wave 2 Conversion Plan, dated October 24, 2008
- Accenture Deliverable #53 – Final Wave 2 Conversion Plan, November 24, 2008
- Accenture Deliverable #43, 53 & 64 – DED for Wave 1, 2 &3 Conversion Plans, dated June 27, 2008
- Accenture Deliverable #43 – Draft Wave 1 Conversion Plan, dated July 18, 2008
- Accenture Deliverable #43 – Final Wave 1 Conversion Plan, August 15, 2008
- Accenture Deliverable #17 – DED for Overall Conversion Plan, dated December 5, 2007
- Accenture Deliverable #17– Draft Overall Conversion Plan, dated December 12, 2007
- Accenture Deliverable #17 – Final Overall Conversion Plan, dated January 14, 2007
- ANSI/IEEE Standard 730-2002, IEEE Standard for Software Quality Assurance Plans
- ANSI/IEEE Standard 1012-2004, IEEE Standard for Software Verification and Validation
- FDGS' Deliverable Review and Assessment Plan
- FDGS'QA Deliverable Development, Production, and Acceptance Plan
- FDGS' Migration Project QA Services Proposal dated August 15, 2007

The following table contains a list of acronyms and terms that are used within this document:

ACRONYM/TERM	DESCRIPTION
C-IV	Consortium IV
D&I	Development and Implementation
DED	Deliverable Expectation Document
FDGS	First Data Government Solutions
ANSI/IEEE	American National Standards Institute/Institute of Electrical and Electronics Engineers
ISAWS	Interim Statewide Automated Welfare System
M&O	Maintenance and Operations
QA	Quality Assurance
WDTIP	Welfare Data Tracking Implementation Project

4. QUALITY ASSURANCE REVIEW ACTIVITIES

In accordance with the Deliverable # 8 – FDGS Deliverable Review and Assessment Plan the FDGS activities associated with this deliverable include the following:

- Actively participate in structured walkthroughs and reviews.
- Attend Conversion Workgroup meetings between C-IV and ISAWS Projects.
- Attend Mock Conversion Workgroup Meetings between C-IV and ISAWS Projects.
- Participate in each Mock Conversion including schedule monitoring, data validation and an application click-thrus.
- Participate in cutover activities including schedule monitoring, data validation and application click-thrus.
- Review draft deliverables and provide feedback and comments to the Consortium and Vendor teams.
- Review final deliverables to document the completeness, comprehensiveness and accuracy of the deliverable based on requirements and project standards.
- Produce an FDGS DED for Assessment of the Wave Conversion Plans Tasks Complete.
- Produce Assessments of the Wave 1 Conversion Plans Task to document the QA findings, material and cosmetic deficiencies and provided a recommendation for acceptance.

5. DELIVERABLE ASSESSMENT METHODOLOGY

The FDGS Deliverable Review and Assessment Plan outlines the approach used for deliverable evaluation. The methodology contained in the plan describes how FDGS completes the assessments and consists of the following tasks and activities:

- Review Vendor's Draft and Final DED and complete a Deficiency Log.
- Produce FDGS Assessment DED and submit to Consortium for review and approval.
- Actively participate in Vendor deliverable development meetings and workgroup sessions.
- Actively participate in structured walkthroughs and reviews of Vendor deliverables.
- Review Vendor Deliverables and compare to cutover specific requirements from Change Order 27 and identify deficiencies.
- Review Vendor Draft Deliverable and provide feedback and comments to the Consortium and Vendor teams.
- Review Vendor Final Deliverables to document the completeness, comprehensiveness and accuracy of the deliverable based on requirements and project standards.
- Develop Draft Deliverable Assessment Report which documents the QA findings, material and cosmetic deficiencies and recommendation for acceptance and submit to Consortium for review and comment.
- Incorporate changes (as needed) into Final Deliverable Assessment Report, including confirming recommendation for acceptance.

The FDGS Deliverable Review and Assessment approach has been further tailored to the unique characteristics of the Wave 1 Conversion Plan Tasks Complete deliverable. FDGS assessed each component of the Wave 1 Conversion Plan Tasks Complete and validated all requirements were met or identified to be met in the Wave 1 Conversion Plan, or appropriate recommendations were provided. FDGS' assessment methodology for Wave 1 Conversion Plan Tasks Complete included taking into account any distinct characteristics of the Wave 1 Migration Counties.

The review of the Wave 1 Conversion Plan Tasks Complete Deliverable included:

- Validating that the work plan for Wave 1 Conversion was adhered to.
- Evaluating of the measurements to determine conversion readiness.
- Analyzing the outstanding conversion SIRs for criticality and post conversion impact.
- Reviewing the progress of Converted Data Testing.
- Reviewing the outcomes for each mock conversion including the detailed timings and issues encountered.
- Reviewing of the Data Validation reports at each milestone.
- Reviewing of the Critical Fallout report output from mock conversions through cutover.
- Validating that the roles and responsibilities for the C-IV Project, ISAWS Project, WDTIP Project and Migration Counties were clearly followed.
- Reviewing of Conversion Data related reports.

For FDGS, the Deliverable Assessment and Review process for the Wave 1 Conversion Plan Tasks Complete did not start upon formal delivery of the Wave 1 Conversion Plan Tasks

Complete deliverable; feedback was provided through multiple iterations of informal review and the draft deliverable based upon mock conversion data. A key component of the FDGS methodology is proactive involvement of staff throughout the development effort.

5.1. Review of Vendor DED

The Vendor DED outlines deliverable components and provides a brief overview of the contents of each of the sections included in the deliverable. Review of the DED allows FDGS to assess the quality of the future deliverable based on the outline and provide comments and recommendations early in the process, so that the changes can be incorporated in the most efficient manner.

In its review of the Vendor DED, FDGS assessed the structure of the deliverable, adherence to quality and standards, coverage of requirements, completeness and accuracy. The DED review process included review of the Draft DED and Final DED. The majority of the comments were provided based on the review of the Draft DED via the deficiency logs. This review helped facilitate that a more accurate and complete version of the document was prepared for the final submission. Review of the Final DED included validation of the Vendor's responses to the deficiency log items documented by FDGS and ensuring that all material comments were adequately addressed.

5.1.1. Requirements Analysis

FDGS conducts requirements analysis to validate that all appropriate requirements are identified in the DED and that all requirements were met.

5.1.2. Comments and Feedback

FDGS provides comments to the Vendor throughout the DED process. Any comments not addressed were documented in the Wave 1 Conversion Plan Tasks Complete DED deficiency logs and provided to the Consortium. Additionally, FDGS reviews all Vendor responses on the Draft and Final Deficiency logs and will discuss with the Consortium and Vendor any discrepancies identified.

5.1.3. Recommendations

FDGS uses the assessment results from the review of the DED to develop informal recommendations regarding the structure, contents and overall quality of the Wave 1 Conversion Plan Tasks Complete deliverable so that corrective actions could be taken. FDGS reviews the requirements from Change Order 27 and identifies which ones were applicable to cutover processes or conversion tasks complete. FDGS provides the list of recommended requirements to be included in the deliverable in addition to the requirement for a Conversion Tasks Complete deliverable.

5.2. Review of Vendor Draft Deliverable

The Draft Deliverable review allows FDGS to assess the validity of the approach applied to the development of the deliverable, its logical organizational structure, adherence to requirements and standards, readability, completeness and accuracy. As a result, the Vendor will have the opportunity to recommend or take corrective action before additional time and resources are

expended in the final development phase of the deliverable. This approach also expedites the final review and approval process.

As part of the draft review process, FDGS analyzes the Draft Deliverable content to verify it met requirements, adhered to DED standards, documented material and cosmetic deficiencies, and provided recommendations for correction or improvement. The subsections that follow provide the methodology used in reviewing the Draft Wave 1 Conversion Plan Deliverable Tasks Complete.

5.2.1. ADHERENCE TO DED

FDGS uses the deliverable standards defined in the DED as the evaluation criteria to validate that the Draft Deliverable was developed consistently in content and structure with the expectations outlined in the DED. Variances from the DED standards are documented in the deficiency log and submitted to the Vendor and Consortium.

5.2.2. REQUIREMENTS ANALYSIS

FDGS conducts requirements traceability analysis to be sure that all appropriate requirements are identified for the deliverable and are met. This analysis includes a review for readability, logical organization, completeness, accuracy, level of detail and quality.

5.2.3. DEFICIENCIES ANALYSIS

FDGS completes a thorough comparison of the deliverable to the DED and requirements in addition to a comprehensive review of the document and all attachments for completeness and readability. This process allows for a factual review of the Consortium's requirements and the Vendor's DED compared to the deliverable. All material and cosmetic deficiencies identified are documented in a deficiency log and submitted to the Vendor and Consortium.

5.2.4. RECOMMENDATIONS

FDGS provides recommendations on the structure content and overall quality of the Draft Wave 1 Conversion Plan Tasks Complete deliverable based upon the results of our comprehensive review. The recommendations provided on the draft deliverable if enacted should improve the overall quality of the final deliverable.

5.3. REVIEW OF VENDOR FINAL DELIVERABLE

FDGS' goal during review of Final Deliverables is to identify all final deficiencies in sufficient time to be addressed by the Vendor and allow for timely approval by the Consortium. As part of the final deliverable review process, FDGS begins by validating that all identified material and cosmetic deficiencies from the Draft Review are satisfactorily addressed. As with the draft review, FDGS analyzes the final deliverable content to verify requirements are met and documented material and cosmetic deficiencies identified during the draft review are resolved, and provides recommendations for correction or improvement.

As the final review is completed, FDGS identifies and documents deficiencies and communicates those issues to the Consortium and Vendor via the deficiency log process. As necessary, FDGS discusses critical findings from the Final Review with the Vendor and

Consortium to allow the Vendor additional time to correct and/or respond to identified issues. The subsections that follow provide the methodology used in reviewing the Final Wave 1 Conversion Plan Tasks Complete Deliverable.

5.3.1. ADHERENCE TO DED

FDGS uses the deliverable standards defined in the DED as the evaluation criteria to validate that the final deliverable is developed consistently in content and structure with the expectations outlined in the DED. Variances from the DED standards are documented in the deficiency log and submitted to the Vendor and Consortium.

5.3.2. REQUIREMENTS ANALYSIS

FDGS conducts requirements traceability analysis to be sure that all appropriate requirements are identified for the deliverable and are met. This analysis includes a review for readability, logical organization, completeness, accuracy, level of detail and quality.

5.3.3. DEFICIENCIES ANALYSIS

FDGS completes a thorough comparison of the deliverable to the DED and requirements in addition to a comprehensive review of the document and all attachments for completeness and readability. This process allows for a factual review of the Consortium's requirements and the Vendor's DED compared to the deliverable. All material and cosmetic deficiencies identified are documented in a deficiency log and submitted to the Vendor and Consortium.

5.3.4. RECOMMENDATIONS

FDGS uses the assessment results from review of the final deliverable in developing a recommendation to the Consortium for acceptance of the deliverable.

6. DELIVERABLE ASSESSMENT FINDINGS

This section contains the complete results of the analysis outlined in the Deliverable Assessment Methodology.

6.1. REVIEW OF VENDOR DED

This section and the subsections that follow will provide the assessment results for the Vendor's DED.

6.1.1. REQUIREMENTS ANALYSIS

This section provides the results of the requirements analysis performed on the Vendor's DED.

Table 1 – Requirements Analysis Results

Requirement		Met Requirement		Description of Deficiency	Project Impact and Issues	Suggestions for Improvement
ID	Description	Yes	No			
115	Contractor shall ensure that the System can issue all authorized benefits for converted cases on a timely basis for both continuing eligibility cases and newly determined eligible cases.	X				
116	Contractor shall meet or exceed all County, State, and Federal requirements for timely customer notifications during the Conversion process.	X				
117	Contractor shall provide support for applicable Interfaces with County, State, and Federal systems during the Conversion process.	X				
118	Contractor shall work with the Migration Counties to minimize any disruption to the public and County staff in the normal operation of business during the Conversion process.	X				

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

First Data.

Requirement		Met Requirement		Description of Deficiency	Project Impact and Issues	Suggestions for Improvement
ID	Description	Yes	No			
121	Contractor shall execute the approved Conversion Plan to convert the caseloads for each Migration County according to the agreed upon timeframes and schedule. Contractor shall ensure that both automated and manual Conversion processes are conducted in a timely and efficient manner according and within the agreed upon timeframes and schedule.	X				
122	The results of each Conversion run for each Migration County shall be reviewed by Contractor to ensure the accuracy of the Conversion and to generate a report of those cases that are unable to be converted. Contractor and the Migration County shall analyze any failed Conversion attempts, document the planned approach for another attempt(s) (such as additional data cleanup and rerun, or manual process), and execute and oversee reruns or manual processes as appropriate.	X				

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

Requirement		Met Requirement		Description of Deficiency	Project Impact and Issues	Suggestions for Improvement
ID	Description	Yes	No			
126	Upon successful completion of each Migration County's Conversion, Contractor shall prepare a Conversion Plan Task Completed document for each Migration County. The document will highlight proven practices and recommendations, as well as problem areas, issues and corresponding solutions. Contractor shall update the Conversion Plan and any processes or procedures as directed by the Consortium.	X				
	Total	**7**	**0**			

6.1.2. COMMENTS AND FEEDBACK

During the review of the Draft and Final DEDs FDGS found that the documents were not written to address all three conversion waves. We found the areas that needed to be updated to reflect all of the Conversion Plan Tasks Completed and made the appropriate recommendations. Additionally FDGS found the information provided surrounding Converted Data Testing to be too high level. FDGS provided recommendations on how to structure the data to provide clear testing results.

6.1.3. DEFICIENCIES ANALYSIS

Table 2 – Deficiencies Analysis Results

DEFICIENCY SUMMARY BY WORK PRODUCT				
WORK PRODUCTS		DEFICIENCIES IDENTIFIED		
TYPE	COUNT	MATERIAL DEFICIENCIES	COSMETIC DEFICIENCIES	TOTAL
DDED Waves 1, 2 and 3 Conversion Plans Tasks Completed	1	4	8	12
FDED Waves 1, 2 and 3 Conversion Plans Tasks Completed	1	0	1	1
Total	**2**	**4**	**9**	**13**

6.1.4. RECOMMENDATIONS

FDGS recommended referencing all three Conversion Tasks Complete deliverables within the DED so it can serve as a blanket document for all three deliverables. FDGS also recommended breaking out the sections for Converted Data Testing to independently display the results.

6.2. REVIEW OF VENDOR DRAFT DELIVERABLE

This section and the subsections that follow provide the assessment results for the Vendor's Draft Deliverable.

6.2.1. ADHERENCE TO DED

This section contains the results of the adherence to the Vendor's DED review performed on their draft deliverable.

Table 3 – Adherence to DED Results

DED Standard		Adhered to Standard		Description of Deficiency	Project Impact and Issues	Suggestions for Improvement
ID	Description	Yes	No			
1.	Section 1, Revision History	Y				
2.	Section 2, Executive Summary	Y				
3.	Section 3, Requirements		N	There requirements were only provided as an attachment.		Create a section within the document that refers to the attached requirements.
4.	Section 4, Deliverable Approach		N	The list of the subsections was not included.		This section should include a summarization of the key sections per the DED.
5.	Section 5, Open Issues from Previous Conversion Deliverables	Y				
6.	Section 6, Appendices		N	The section did not include the Requirements attachment within the deliverable.		The attachments section should be updated. Additionally, there were several recommendations to improve the overall quality of the appendices.
7.	Section 7, Resources	Y				
8.	Section 8, Deliverable Format		N	The section was not updated from the DED and referred to all three Wave deliverables and the DED.		Update the section to be reflective of the DEL.
9.	Section 9, Project Management Approval		N	This section referred to the DED.		Remove reference to the DED and update with DEL.
10.	Section 10, Approval		N	This section referred to the DED.		Remove reference to the DED and update with DEL.
	Total	**4**	**6**			

6.2.2. REQUIREMENTS ANALYSIS

This section provides the results of the requirements analysis performed on the Vendor's Draft Deliverable.

Table 4 – Requirements Analysis Results

REQUIREMENT		MET REQUIREMENT		DESCRIPTION OF DEFICIENCY	PROJECT IMPACT AND ISSUES	SUGGESTIONS FOR IMPROVEMENT
ID	DESCRIPTION	YES	NO			
115	Contractor shall ensure that the System can issue all authorized benefits for converted cases on a timely basis for both continuing eligibility cases and newly determined eligible cases.	X				Update Section Reference in Deliverable Traceability.
116	Contractor shall meet or exceed all County, State, and Federal requirements for timely customer notifications during the Conversion process.	X				Update Section Reference in Deliverable Traceability. For Deliverable Traceability add that the NOAs were tested during Program Eligibility Testing.
117	Contractor shall provide support for applicable Interfaces with County, State, and Federal systems during the Conversion process.	X				Update Section Reference in Deliverable Traceability.
118	Contractor shall work with the Migration Counties to minimize any disruption to the public and County staff in the normal operation of business during the Conversion process.	X				Update Section Reference in Deliverable Traceability.

Requirement		Met Requirement		Description of Deficiency	Project Impact and Issues	Suggestions for Improvement
ID	Description	Yes	No			
121	Contractor shall execute the approved Conversion Plan to convert the caseloads for each Migration County according to the agreed upon timeframes and schedule. Contractor shall ensure that both automated and manual Conversion processes are conducted in a timely and efficient manner according and within the agreed upon timeframes and schedule.	X				Update Section Reference in Deliverable Traceability.
122	The results of each Conversion run for each Migration County shall be reviewed by Contractor to ensure the accuracy of the Conversion and to generate a report of those cases that are unable to be converted. Contractor and the Migration County shall analyze any failed Conversion attempts, document the planned approach for another attempt(s) (such as additional data cleanup and rerun, or manual process), and execute and oversee reruns or manual processes as appropriate.	X				Update Section Reference in Deliverable Traceability

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

Requirement		Met Requirement		Description of Deficiency	Project Impact and Issues	Suggestions for Improvement
ID	Description	Yes	No			
126	Upon successful completion of each Migration County's Conversion, Contractor shall prepare a Conversion Plan Task Completed document for each Migration County. The document will highlight proven practices and recommendations, as well as problem areas, issues and corresponding solutions. Contractor shall update the Conversion Plan and any processes or procedures as directed by the Consortium.	X				
	Total	**7**	**0**			

6.2.3. DEFICIENCIES ANALYSIS

This section provides the results of the deficiencies analysis performed on the Vendor's Draft Deliverable.

Table 5 – Deficiencies Analysis Results

DEFICIENCY SUMMARY BY WORK PRODUCT				
WORK PRODUCTS		DEFICIENCIES IDENTIFIED		
TYPE	COUNT	MATERIAL DEFICIENCIES	COSMETIC DEFICIENCIES	TOTAL
FDEL #77 Conversion Plans Tasks Complete Wave 1	1	16	31	47
Total	**1**	**16**	**31**	**47**

6.2.4. RECOMMENDATIONS

The Draft Deliverable was completed using data and metrics from Mock Conversion 1.4. This deliverable served as a framework for how the Final Deliverable would look.

During FDGS' comparison of Draft Deliverable 77 Conversion Plan Tasks Complete to the DED, we recognized that the format outlined in the DED was not adhered to. We documented the deficiencies and provided them to the Vendor with recommendations for how to restructure the document.

Our primary concern with the Draft Deliverable was the lack of detail provided for Outstanding SIRs and Wave Specific Go Live activities. FDGS recommends adding the list of outstanding SIRs at Go Live, and the disposition of SIRs transitioned to the Implementation Team for additional documentation or support. The Wave Specific Go Live activities section still reads too similarly to the DED, and does not have the level of detail expected for a deliverable. FDGS recommends adding detailed statements and/or specific examples to each of the bulleted items in the section.

Once the deficiencies have been addressed, FDGS believes that the Draft Deliverable is a good foundation for a Final Deliverable for Wave 1 Conversion Tasks Complete.

6.3. REVIEW OF VENDOR FINAL DELIVERABLE

This section and the subsections that follow provide the assessment results for the Vendor's Draft Deliverable.

6.3.1. ADHERENCE TO DED

This section contains a table that provides the results of the adherence to the Vendor's DED review performed on the Vendor's Final Deliverable.

Table 6 – Adherence to DED Results

DED STANDARD		ADHERED TO STANDARD		DESCRIPTION OF DEFICIENCY	PROJECT IMPACT AND ISSUES	SUGGESTIONS FOR IMPROVEMENT
ID	DESCRIPTION	YES	NO			
1.	Section 1, Revision History	Y				
2.	Section 2, Executive Summary	Y				
3.	Section 3, Requirements	Y				
4.	Section 4, Deliverable Approach	Y				
5.	Section 5, Open Issues from Previous Conversion Deliverables	Y				Recommend adding a description for Medium SIRs in the CRI section, and in Outstanding SIR section address Low and Medium SIRs.
6.	Section 6, Appendices	Y				
7.	Section 7, Resources	Y				
8.	Section 8, Deliverable Format	Y				
9.	Section 9, Project Management Approval	Y				
10.	Section 10, Approval	Y				
	Total	**10**	**0**			

6.3.2. REQUIREMENTS ANALYSIS

This section provides the results of the requirements analysis performed on the Vendor's Final Deliverable.

Table 7 – Requirements Analysis Results

REQUIREMENT		MET REQUIREMENT		DESCRIPTION OF DEFICIENCY	PROJECT IMPACT AND ISSUES	SUGGESTIONS FOR IMPROVEMENT
ID	DESCRIPTION	YES	NO			
115	Contractor shall ensure that the System can issue all authorized benefits for converted cases on a timely basis for both continuing eligibility cases and newly determined eligible cases.	X				
116	Contractor shall meet or exceed all County, State, and Federal requirements for timely customer notifications during the Conversion process.	X				
117	Contractor shall provide support for applicable Interfaces with County, State, and Federal systems during the Conversion process.	X				
118	Contractor shall work with the Migration Counties to minimize any disruption to the public and County staff in the normal operation of business during the Conversion process.	X				

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

First Data.

Requirement		Met Requirement		Description of Deficiency	Project Impact and Issues	Suggestions for Improvement
ID	Description	Yes	No			
121	Contractor shall execute the approved Conversion Plan to convert the caseloads for each Migration County according to the agreed upon timeframes and schedule. Contractor shall ensure that both automated and manual Conversion processes are conducted in a timely and efficient manner according and within the agreed upon timeframes and schedule.	X				
122	The results of each Conversion run for each Migration County shall be reviewed by Contractor to ensure the accuracy of the Conversion and to generate a report of those cases that are unable to be converted. Contractor and the Migration County shall analyze any failed Conversion attempts, document the planned approach for another attempt(s) (such as additional data cleanup and rerun, or manual process), and execute and oversee reruns or manual processes as appropriate.	X				

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

Requirement		Met Requirement		Description of Deficiency	Project Impact and Issues	Suggestions for Improvement
ID	Description	Yes	No			
126	Upon successful completion of each Migration County's Conversion, Contractor shall prepare a Conversion Plan Task Completed document for each Migration County. The document will highlight proven practices and recommendations, as well as problem areas, issues and corresponding solutions. Contractor shall update the Conversion Plan and any processes or procedures as directed by the Consortium.	X				
	Total	**7**	**0**			

6.3.3. DEFICIENCIES ANALYSIS

This section provides the results of the deficiencies analysis performed on the Vendor's Final Deliverable.

Table 8 – Deficiencies Analysis Results

DEFICIENCY SUMMARY BY WORK PRODUCT				
WORK PRODUCTS		DEFICIENCIES IDENTIFIED		
TYPE	COUNT	MATERIAL DEFICIENCIES	COSMETIC DEFICIENCIES	TOTAL
FDEL #77 Conversion Plans Tasks Complete Wave 1	1	0	5	5
Total	**1**	**0**	**5**	**5**

6.3.4. RECOMMENDATIONS

FDGS has submitted five cosmetic deficiencies for Final Deliverable #77 - Conversion Plan Tasks Complete Wave 1. The overall content of the Final Deliverable is found to be acceptable.

FDGS is currently working with the Conversion Team in planning for Wave 2 Conversion to ensure any lessons learned, recommendations for improvement to the approach and tools, and county feedback is being incorporated into the conversion process.

7. ACCEPTANCE RECOMMENDATION

Final Deliverable #77 Conversion Plan Tasks Complete Wave 1 is well constructed and includes the relevant detail and supporting documentation. FDGS recommends acceptance of the Conversion Plan Tasks Complete Wave 1 deliverable.

8. DELIVERABLE ROLES AND RESPONSIBILITIES

This section identifies the FDGS QA and Consortium roles and responsibilities associated with the development, maintenance, review, and approval of the Assessment of Conversion Plan Tasks Completed for Wave 1.

Table 9 – Deliverable Roles and Responsibilities

ROLE	RESPONSIBILITY
FDGS Deliverable Owner Kristin Summers	Responsible for managing the Deliverable development effort.
Internal FDGS Deliverable Reviewer Wendy Battermann	Responsible for reviewing the deliverable before it is submitted to the Consortium.
Deliverable Assigned To Kristin Summers	Responsible for authoring the Deliverable.
Deliverable Approver John Boule	Responsible for the final approval of the Deliverable.
Consortium Deputy Director Karen Rapponotti	Responsible for feedback and recommended changes to the Deliverable.
Consortium Technical Manager Jon Burkett	Responsible for feedback and recommended changes to the Deliverable.

9. DELIVERABLE SCHEDULE

This section contains start and completion dates for the Assessments of Conversion Plans Tasks Completed for Wave 1.

Table 10 – Deliverable Development, Review, and Approval Schedule

#	TASK	START DATE	COMPLETION DATE
1.	FDGS submits DED to Consortium	8/28/09	8/28/09
2.	Consortium Reviewers review DED and provide feedback to Deliverable Owner	2/28/09	9/3/09
3.	Deliverable Owner incorporates changes and FDGS submits Final DED to Consortium	9/3/09	9/4/09
4.	Deliverable Owner develops Draft Deliverable	9/4/09	11/19/09
5.	FDGS submits Draft Deliverable to Consortium	11/19/09	11/19/09
6.	Consortium Reviewers review Draft Deliverable and provide feedback to Deliverable Owner	11/19/09	12/2/09
7.	Deliverable Owner incorporates changes and develops Final Deliverable	12/2/09	12/2/09
8.	FDGS submits Final Deliverable to Consortium	12/2/09	12/2/09
9.	Consortium Reviewers review Final Deliverable and provide feedback to Deliverable Owner	12/2/09	12/8/09
10.	Deliverable Owner incorporates changes and FDGS submits Final Deliverable to Consortium	12/8/09	12/9/09
11.	Consortium Approves Final Deliverable	12/909	12/9/09

10. DELIVERABLE REQUIREMENTS

This table identifies the specific requirement(s) associated with the delivery of the Assessments of Conversion Plans Tasks Completed for Wave 1.

Table 11 – Deliverable Requirements Met

REQ. #	REQUIREMENT	REQUIREMENT MET
8.	The QA Vendor shall provide a Deliverable Review and Assessment Plan that describes how the QA Vendor will accomplish and record its review and assessment of all the Deliverables listed under D&I Phase - Application Development Support Services (lines 12-55), and D&I Phase- Implementation Support Services (lines 56-82) in Attachment 1, QA Vendor Deliverables List. Since the types of information that will be assessed will vary depending on the Deliverable being assessed, the QA Vendor must employ a standard reporting format to record QA activities and facilitate the Consortium's review and acceptance of Development/M&O Vendor and Implementation Vendor Deliverables. The recording format utilized by the QA Vendor must include but is not limited to the following: A. Overall quality of the Deliverable; B. QA activities involved in the assessment of the Deliverable including but not limited to meetings attended, work observed, tests initiated and/or observed, documentation or code validated; C. Modifications to the Deliverable already incorporated as a result of QA Vendor activities; D. Assessment of the Deliverable's adherence to Deliverable Expectation Document (DED) standards; E. Requirement Validation; F. Comprehensive and specific comments, including a discussion of identified issues, deficiencies, and suggestions for improvement; and G. Recommendation as to Deliverable acceptability and any conditions linked to acceptance. For a Listing of Deliverables required of the Development/M&O Vendor and Implementation Vendor see Attachments 6 and 7 respectively.	Yes

11. DELIVERABLE ASSUMPTIONS

This section will detail any assumptions FDGS has regarding the Assessments of Conversion Plan Tasks Completed for Wave 1.

FDGS assumes that:

- The designated Consortium representatives will be able to perform the review and feedback tasks according to the Schedule in Section 6, DED and Deliverable Development, Review, and Approval Schedule.
- No Contingency Plan is required for this particular Assessment DED.

12. APPENDIX A – MATERIAL AND COSMETIC DEFICIENCIES

This appendix contains a compiled list of all material and cosmetic deficiencies identified by the FDGS reviewers over the course of the entire assessment effort.

Note: The following table format parallels the project's Deficiency Log. However, FDGS does not complete the acceptance columns in this log because FDGS must make an acceptance recommendation for the deliverable as a whole. Please refer to Section 4.1.6 for the FDGS Acceptance Recommendation for this deliverable.

Table 1 – Appendix A – Material and Cosmetic Deficiencies

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
1.	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	4	3		X	Table 3.1 - Change the font on the dates in Table 3-1 to Times New Roman.	X			x		Table 3.1 - Changed the font on the dates in Table 3-1 to Times New Roman.	19-Aug	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
2.	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Wendy Battermann	0	Global		X	Please make the following global cosmetic changes: 1 - Change "Deliverables #77, 87, and 95" to "Deliverables #77, #87, and #95". 2 - Change page headings to match portrait or landscape format settings. 3 - Spell out numbers under 11 (e.g., "six-month period" instead of "6 month period").	X			x		**Made the following global cosmetic changes:** 1 - Change "Deliverables #77, 87, and 95" to "Deliverables #77, #87, and #95". **Did not make the following change because this is actual working in the response as documented in the Migration Project Statement of Work (SOW) as documented in Exhibit K (and Exhibit L as appropriate) of the Amended and Restated Revised System Agreement and Change Order 027.** 3 - Spell out numbers under 11 (e.g., "six-month period" instead of "6 month period").	19-Aug	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

First Data.

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
3.	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Wendy Battermann	12	3.4		X	First paragraph, second sentence - For "ease of reference" normally means that the categories to be discussed are listed following the sentence rather than having the reader go through pages to reference the key points. Suggest rewording the second sentence and listing the upcoming sections after the sentence. For example, "For ease of reference, the deliverable will provide information on the following key points: - Overall Conversion Readiness - Mock Conversion History - Converted Data Test Results - Outstanding Migration Conversion SIRs - Wave Specific Go-Live - Risks and Issues - Open Items from Previous Conversion Deliverables"		X				Changed working to: "For ease of reference, the deliverable will provide information on the following key points: - Overall Conversion Readiness - Mock Conversion History - Converted Data Test Results - Outstanding Migration Conversion SIRs - Wave Specific Go-Live - Risks and Issues - Open Items from Previous Conversion Deliverables"	19-Aug	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Diane Alexander Wendy Battermann	12	3.4.1	X		This section needs to address how each metric was derived. Recommend including the more detailed table also to provide an understanding of what criteria comprise each category and how.			X	x		Added Table 6 to section 3.4.1 Overall Conversion Readiness: "Table 6 – Conversion Readiness Index Specifics details the criteria and measurements used to calculate the score of each metric."	19-Aug	Y
5.	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Wendy Battermann	12	3.4.1, 3.4.3, and 3.4.4		X	Tables 5, 6, and 7 - Update the table numbering to be in sequence with the rest of the document (i.e., Tables 3-5, 3-6, and 3-7, respectively).		X		x		Updated the table numbering to be in sequence with the rest of the document	19-Aug	Y
6.	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Diane Alexander	12	3.4.2	X		In the last bullet the description of what results will be reported needs to be more clearly defined. (#of cases reviewed, #of SIRs identified, etc) Should include the list of items that will be reported on here.			X	x		Defined "results" in the last bullet: Mock Conversion County Review Period and Results. Results will include: • # of cases reviewed; • # of Tickets created; and, • Disposition of the Tickets (after the Mock Conversion County Review).	19-Aug	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
7.	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Wendy Battermann	13	3.4.5		X	First bullet - Since semi-colons are being used to separate the bullets, consider rewording the sentence to read, "When the Conversion Cutover Activities occurred, and will reference the Cutover Checklist (as an appendix)".	X			x		Changed sentence to read, "When the Conversion Cutover Activities occurred, and will reference the Cutover Checklist (as an appendix)".	19-Aug	Y
8.	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Wendy Battermann	15	4		X	Table 4.1 - Under QA Vendor Representative, add "Kristin Summers".		X		x		Table 4.1 - Under QA Vendor Representative, added "Kristin Summers".	19-Aug	Y
9.	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Wendy Battermann	15	4		X	Change Table 4.1 to 4-1 to match previous table references.		X		x		Changed to Table 4-1 Resources Table	19-Aug	Y
10.	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	13	3.4.4		X	Capitalize "Team" for Conversion Team.		X		x		Capitalized "Team" for Conversion Team.	19-Aug	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

First Data.

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
11.	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	12	3.4.3	X		In the section Converted Data Test Results state which areas of Converted Data Test will be included (CDT, State and County Interfaces) specifically. Provide the bulleted list of areas under each section.			X	x		Changed section to: This section will be used to document the results of the Converted Data Test effort and will consist of the following areas: § State Interfaces Testing Status; § County Interfaces Testing Status; and, § Application, Forms, Reports, and Batch Process Testing Status.	19-Aug	Y
12.	8/18/09	Draft DED 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	Global	Global	X		The Title of the document needs to reference all three conversion tasks complete deliverables (77, 87 and 95) not just 77. Also update the reference to Wave 1 (W1).			X	x		Changed to "FDED 77, 87, 95 - Conversion Plan Tasks Completed.doc"	19-Aug	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

First Data.

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
13.	8/24/09	FDED 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	12	3.4.1		X	Update sentence "During this meeting Conversion Management Team will present and explain the Conversion Readiness" to read "During this meeting the Conversion Management Team will present and explain the readiness of the counties in the wave for conversion activities."		X		x		Updated sentence "During this meeting Conversion Management Team will present and explain the Conversion Readiness" to read "During this meeting the Conversion Management Team will present and explain the readiness of the counties in the wave for conversion activities."	8/26/09	Y
14.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	4	1.2.1		X	Heading for Table 1-2 is on page 4 and table is on page 5	X			x		This has been corrected.	11/10/09	Y
15.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	4	1.2		X	Table Headings seem inconsistent some have a -1 after them e.g. Table 1-1 and some don't.	X			x		This has been corrected.	11/10/09	Y
16.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	5	1.2.1		X	General Comment - standardize mentions of SIR's vs. SIRs	X			x		Standardized "SIR's" to "SIRs".	11/10/09	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
17.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	6	1.2.2.1		X	Footer of Table 3 - test should read "Approx 1 1/2 hours over the …." Hours was missing.	X			x		Changed to "Approx. 1 ½ hours over the Planned 84 hours."	11/10/09	Y
18.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	6	1.2.2.1		X	"participants we ask to review" - should this be "participants were asked to review"?	X			x		Changed to "participants were asked to review converted data and compare this data back to ISAWS."	11/10/09	Y
19.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	6	1.2.2.2		X	"Listed below are the results of this effort" however, table is on next page.	X			x		Inserted page break for section 1.3.2.3 - 1.3.2.3 Mock Conversion 1.3 (July)	11/10/09	Y
20.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean Kristin Summers	7	Table 4		X	Table does not have summary / totals at the bottom - no total hours summary.	X			x		Added summary totals at the bottom of Table 3: Mock Conversion 1.2 Actuals	11/10/09	Y
21.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	7	1.2.2.2		X	"participants we ask to review" - should this be "participants were asked to review"?	X			x		Changed "participants we ask to review" to "participants were asked to review".	11/10/09	Y
22.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean Kristin Summers	8	Table 5	X		Values for duration not populated for most tasks.		X		x		Added Mock Conversion 1.3 Actuals to Table #4	11/10/09	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

First Data.

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
23.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	9	1.2. 2.3. 1		X	"participants we ask to review" - should this be "participants were asked to review"?	X			x		Changed "participants we ask to review" to "participants were asked to review".	11/10/09	Y
24.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	9	1.2. 2.3. 2		X	"participants we ask to review" - should this be "participants were asked to review"?	X			x		Changed "participants we ask to review" to "participants were asked to review".	11/10/09	Y
25.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	10	1.2. 2.4		X	General Comment: County should be capitalized.	X				x	Don't believe that this should be capitalized.	n/a	Y
26.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	11	Tab le 7		X	Format table so all information is at the top of the cells not the bottom.	X			x		Formatted tables so all information is at the top of the cells and not the bottom.	11/10/09	Y
27.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	17	Tab le 9		X	Table 9 should be all on one page and should not break across pages.	X			x		Application, Forms, Reports, and Batch Process Testing Status is all on one page (see pg. #13)	11/10/09	Y
28.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	19	Tab le 1- 10		X	Is the table name correct - should it just be table 10?	X			x		Table names/#'s have been updated.	11/10/09	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
29.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	20	Table 11	X		Steps in table 11 not in chronological or numeric order.		X			x	This table was not intended to be listed in chronological order but instead the order in which the milestones were planned.	n/a	Y
	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	20	Table 11		X	Does Step 1.1.2.1 really take 0 minutes?	X				x	Removed the variances as these should be reviewed in Appendix 1 - Cutover Checklist Schedule	n/a	Y
31.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	22	Table 11	X		Step 1.2.4.1 says variance 0 but planned duration was 8 hrs and Actual was 6.77 hours.		X			x	Removed the variances as these should be reviewed in Appendix 1 - Cutover Checklist Schedule	n/a	Y
32.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	22	Table 11	X		Step 1.2.4.11 Variance is incorrect by 1 hour.		X			x	Removed the variances as these should be reviewed in Appendix 1 - Cutover Checklist Schedule	n/a	Y
33.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	22	Table 11	X		Step 1.2.4.2 Variance is incorrect - says 0 hrs.		X			x	Removed the variances as these should be reviewed in Appendix 1 - Cutover Checklist Schedule	n/a	Y
34.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean	26	2	X		Test refers to table 4.1 below - it's table 2-1.		X		x		Changed to "Table 2 1 Resources Table below lists the key resources required to achieve a successful signoff on this Deliverable."	11/10/09	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
35.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean Kristin Summers	26	2	X		Text refers to DED - document is not a DED.		X		x		Changed to "Table 2 1 Resources Table below lists the key resources required to achieve a successful signoff on this Deliverable."	11/10/09	Y
36.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean Kristin Summers	26	Table 2-1	X		Text refers to DED - document is not a DED.		X		x		Updated	11/10/09	
37.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean Kristin Summers	27	3		X	Verify that table name is correct. Remove references to Deliverables 87 and 95 and Waves 22 and 3.	X			x		Changed to "Deliverables #77 - Conversion Plan Tasks Completed – Wave 1"	11/10/09	Y
38.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean Kristin Summers	28	4	X		Text refers to DED - document is not a DED.		X		x		Changed to "The following is a submittal block by Contractor Project Management for Consortium's final review and approval of this DEL."	11/10/09	Y
39.	9/23/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Mark Bean Kristin Summers	29	5	X		Text refers to DED - document is not a DED.		X		x		Changed DED to DEL.	11/10/09	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
40.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers				X	All appendices need to be renamed to show their proper title as written in the DDEL. Ex. Appendix 1 - Cutover Checklist Schedule.	X			x		Updated to: Appendix 1 – Cutover Checklist Schedule; Appendix 2 - Data Validation Summary Report; Appendix 3 – Fallout Report; and, Appendix 4 -- Requirements.	11/10/09	Y
41.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers		App endi x 1		X	The project plan is incomplete with some tasks that show they have not been started.	X			x		The prpject plan is now complete for the Wave 1 Cutover Activities.	11/10/09	Y
42.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers		App endi x 4		X	The requirements attachment has several extra pages in the beginning of the document which need to be removed. Recommend only having a title page and then go to the requirements table.	X			x		Extra pages have been removed.	11/10/09	Y
43.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	4		X		Directly below the executive summary there should be a heading and section for Requirements that refer to the attachment. Per DED.		X		x		Requirements section added under Executive Summary, per DED.	11/10/09	Y
44.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	4	1.1	X		Below the Requirements section there should be a Deliverable Approach section which would include a summarization of key sections per DED.		X		x		Deliverable Approach section added under the Requirements section, per DED.	11/10/09	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

First Data.

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
45.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	4&5	1.2		X	The order of CRI elements should be consistently displayed. For example, the order is different in Table 1-1, Table 1-2 and in the list of the seven components that make up the CRI. Also, in Table 1-1 the Data Validation section is titled "Overall Fallout" the titles should be consistent.	X			x		The order of CRI elements has been updated/reordered.	11/10/09	Y
46.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	4	Table 1-1		X	Add an "As of" date to the CRI.	X			x		Updated to "Conversion Readiness Index as of 10/29/2003"	11/10/09	Y
47.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	5	Table 1-2		X	Add the CRI scores from Table 1-1 to show how they were derived.	X				x	Don't see why this is relevant given that the scores are documents in Figure 1 and Figure 2 documents how each component is assessed (which infers how they were derived).	n/a	Y
48.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	5	1.2.1		X	For Page, add that if any single element on a page is not working for any type of case the Page is not considered passing.	X				x	Don't believe that it is necessary to document/define the methodology by which we passed or failed pages.	n/a	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

First Data.

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
49.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	5	1.2.1		X	For Data Validation at the end of the statement add "through the conversion and transformation process".	X			x		Changed to "Measures the overall data fallout between the Legacy Data Source and C-IV during the cutover activities"	11/10/09	Y
50.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	6	1.2.2		X	For all Mock Conversion Section Titles add the Year to the name (EX. May 2009). Also, recommend adding a schedule of events at the top of the section: Part 2: (Start/Finish Date) County Review: (Start/Finish Date)	X			x		For all Mock Conversion Section Titles added the Year to the name (EX. May 2009).	11/10/09	Y
51.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	General			X	When referencing dates, whether in table or text, always include the month and year.	X			x		Updated in general.	11/10/09	Y
52.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	9	1.2.2.3.1		X	Capitalize Conversion Team in descriptions of 1.3.1 and 1.3.2	X			x		Capitalized Conversion Team in descriptions of 1.3.1 and 1.3.2	11/10/09	Y

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
53.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	9	1.2.2.3.1		X	Add to the Mock 1.3.1 that select individuals ran EDBC. Also add to Mock 1.3.2 that all participants could run EDBC.	X			x		Updated. MC 1.3 - "Additionally, a small set of participants were selected to run EDBC and review the results respective to these converted cases." MC 1.4 - "all participants were asked to review the Critical Case Fallout report, manually updated convert cases (i.e., update cases, and run EDBC on converted cases)."	11/10/09	Y
54.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	9	1.2.2.4		X	The introductory sentence to the section has the incorrect date.	X			x		Correct...Actual Conversion cutover activities respective to MC 1.4 began on 8/28 not 7/28. The change has been made.	11/10/09	Y
55.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	19	1.2.4	X		The list of outstanding SIRs should be included. Also, on the FDEL I would expect to see what remained outstanding and the plan that was created for each SIR.		X		x		Refer to updates made to section 1.3.4 - Outstanding Migration Conversion SIRs	11/10/09	Y
56.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	20	1.2.5		X	The first sentence should read Wave 1, not all Waves.	X			x		Updated to "This section is a summary of the actual Wave 1 Conversion Cutover Activities that occurred over the cutover weekend."	11/10/09	Y

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
57.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	20	1.2.5	X		This section does not have sufficient detail. Each of the bulleted items should be a paragraph. For the critical impacts, the detail in the notes section of Table 11 does not have enough context to really articulate how something was a critical impact. Downtime for County Staff during Cutover and Fallout Report have no information.		X		x		Details have been added. Please review.	11/10/09	Y
58.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	25	1.4		X	The last bullet should state "Appendix 4 - Requirements"	X			x		Updated to Appendix 4 - Requirements.	11/10/09	Y
59.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers		Appendix 4 Requirements	X		All section references need to be updated in the Deliverable Traceability column.		X		x		All section references have been updated in the Deliverable Traceability column.	11/10/09	Y
60.	9/28/09	Draft Del 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	6	Appendix 4 Requirements	X		For Reqt 116 add Program Eligibility testing in addition to Forms Testing as the NOAs were testing during Program Eligibility.		X		x		Updated to "Section 4.1.3 – Converted Data Test Results – Program Eligibility and Forms Testing respective to Migration and M&O Forms."	11/10/09	Y

Final Deliverable #28: Assessment of Conversion Plans Tasks Complete Wave 1

First Data.

Comment #	Date Comment Logged	Deliverable Description	Reviewer Citing Deficiency	Page	Section	Material	Cosmetic	FDGS Description of Deficiency and Recommendation	Fully Accept	Conditionally Accept	Non-Acceptance	Agree	Disagree	Vendor Documented Agreed Remedy	Date Fixed	FDGS Agree w/ Remedy (Y/N)
61.	11/18/09	Final DEL 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	6	4.1.1.1		X	In Table 1 add a description for Medium SIRs since they were also included in the measurement of the CRI.		X			x	Did not add a description for Medium SIR's because the definitions are the same. The difference between the two is whether or the element is CORE (High SIR) or NON-CORE (Medium SIR).	n/a	Y
62.	11/18/09	Final DEL 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	6	4.1.1.1		X	In the Case bullet add an "a" before "sample". "for a sample set of cases"		X		x		Changed to "...for a sample set of cases."	11/30/09	Y
63.	11/18/09	Final DEL 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	9	4.1.2.3		X	Add "2009" after In August. (the first paragraph after Table 4)		X		x		Change to "In August 2009, the C-IV Conversion Team..."	11/30/09	Y
64.	11/18/09	Final DEL 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	14	4.1.4		X	Recommend adding a statement to address Medium and Low SIRs in general did not require attention from the Implementation Team since the nature of those issues could be resolved with a work around, and typically only affected a small subset of cases.		X		x		Changed to "Medium and Low SIRs did not require attention from the Implementation Team given that these issues could be resolved using the C-IV System."	11/30/09	Y
65.	11/18/09	Final DEL 77 - Conv Plan Task Completed - Wave 1	Kristin Summers	16	4.1.5.2		X	Update Table references from Table 9 and Table 10 to Table 10 and Table 11.		X		x		Updated Table references from Table 9 and Table 10 to Table 10 and Table 11.	11/30/09	Y

IEDSS IV&V Monthly Management Briefing

JULY 14, 2015

First Data.
beyond the transaction

Agenda

Summary for June 2015

Observations

Future Activities

Performance Measures

Questions

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Summary for June 2015

Deliverables/Artifacts

- Reviews
  - System Test Summary Report
  - Revised System Test Summary Report DED
  - Operational Readiness Plan DED
  - Security Information and Event Management (SIEM) Implementation AED
  - CR PSD for Support IR14 - QC
  - Revised Unit Tested System Code
  - Application Vulnerability Assessment Report AED
  - Midpoint Survey Review for Organizational Change Management activity

© 2015 First Data Corporation. All Rights Reserved.

Summary for June 2015

Deliverables/Artifacts

- Activities
  - JAD Sessions (14)
    - Front Office
    - Interfaces
    - EDBC
    - Correspondence

- BPM (Task Management) Sessions (7)

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Summary for June 2015

Deliverables/Artifacts

- Activities
  - Walkthroughs
    - Revised Data Conversion Load and Test Plan
    - Revised Unit Tested System Code
    - System Test Summary Report DED
    - Security Information and Event Management (SIEM) Implementation AED
    - Operational Readiness Plan DED
    - Conversion Reference Code Mapping
    - Benefit Match for Converted Cases
    - Manual Correspondence

© 2015 First Data Corporation. All Rights Reserved.

Summary for June 2015

Deliverables/Artifacts

- Activities
  - Attended Training Team meetings
  - Attended Organizational Change Management (OCM) meetings
  - Attended SOTA call for Achieving Real Time Eligibility Determination webinar
  - Attended DDI Vendor Weekly Stage 2 Defect Triage Meetings
  - Monitored System Testing activities
  - Attended IEDSS Weekly Stage I Defect Management meetings
  - Attended CDMS Requirements/Design sessions

© 2015 First Data Corporation. All Rights Reserved.

Summary for June 2015

Deliverables/Artifacts

- Activities
  - Monitored System Testing
- Attended Touch Point/Document Defect Meetings
  - Self Service
    Front Office
  - Back Office
  - Interfaces
  - Conversion
  - Correspondence
  - Reports

© 2015 First Data Corporation. All Rights Reserved.

Observations

- Decision #251215 – Conversion of Historical ICES Data
  - Closed in PMC
  - Impacts 18 System Requirements
  - Need to modify/remove
- Correspondence
  - Outstanding IR approvals
  - New CRs
- Project progress
  - Case vs AG
  - Phone Application
  - Task Management
  - Re-planning process
- System Documentation Storage
  - Issue with storing/locating current versions of PSDs

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Observations

- System Test
  - Defects
  - Change Requests Code Drop 1

- Integration Test
  - No Activities

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Testing

As of 06/30/2015

Cycle	Rel 1	% Comp	Rel 2	% Comp	Rel 3	% Comp	Rel 4	% Comp	CR 1	% Comp
System Test Overall Pass %										
1									20.4	100
2									28.7	100
3	99.9	100	99.9	100	99.8	100	97.6	100	31.0	100

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Future Activities

- Attend Design sessions as scheduled
- Review Design sessions minutes and documentation
- Attend document defect sessions
- Attend IEDSS Steering Committee meetings
- Generate IEDSS Steering Committee Minutes

  Monitor and Evaluate System Testing activities
- Provide System Test observations
- Review Integration Test Scenarios and Test Cases
- Monitor and Evaluate Integration Test activities

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Future Activities

- Provide Integration Test observations
- Monitor State User Acceptance Test activities
- Attend BPM/Task Management sessions
- Attend Walkthroughs as scheduled
- Attend IEDSS Project related meetings
- Review proposed Change Requests
- Deliver Monthly IV&V Briefings
- Deliver Monthly IV&V Reports
- Review and analyze re-plan results

© 2015 First Data Corporation. All Rights Reserved.

Future Activities

- Review artifacts, work products and deliverables
  - Revised Data Conversion and Load Plan
  - DDI Vendor June, July, August Monthly Status Report
  - System Test Summary Report
  - Security Information and Event Management Solution (SIEM)
  - On-line Help
  - Performance Test Summary Report
  - Operational Readiness Plan DED
  - Integration Test Summary Report

© 2015 First Data Corporation. All Rights Reserved.

Future Activities

- Review artifacts, work products and deliverables
  - Data Conversion and Load Testing
  - Organizational Transition Plan - Pilot
  - Requirements Database Traceability Matrix
  - Design
  - Construction
  - Testing
  - IRS Safeguard Procedures Report
  - Training Materials – Instructor Led
  - Operation Readiness Plan
  - Application Vulnerability Assessment
  - Implementation Plan
  - CR IRs and Responses

© 2015 First Data Corporation. All Rights Reserved.

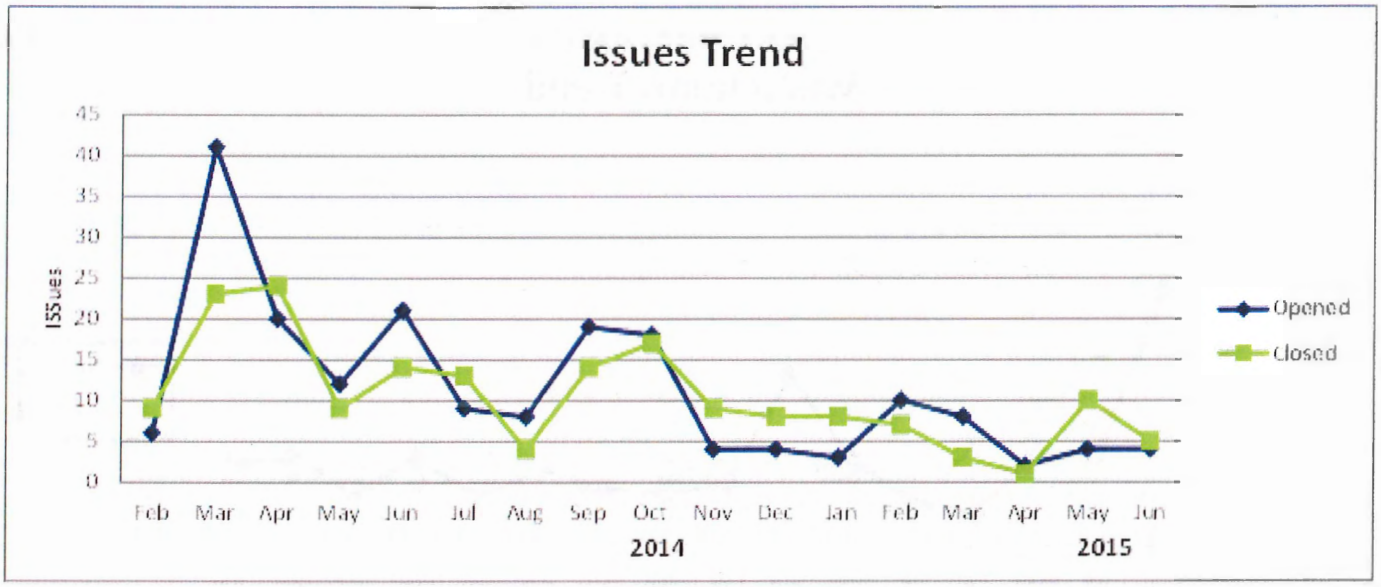
First Data.
beyond the transaction

Performance Measures

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Performance Measures



© 2015 First Data Corporation. All Rights Reserved.

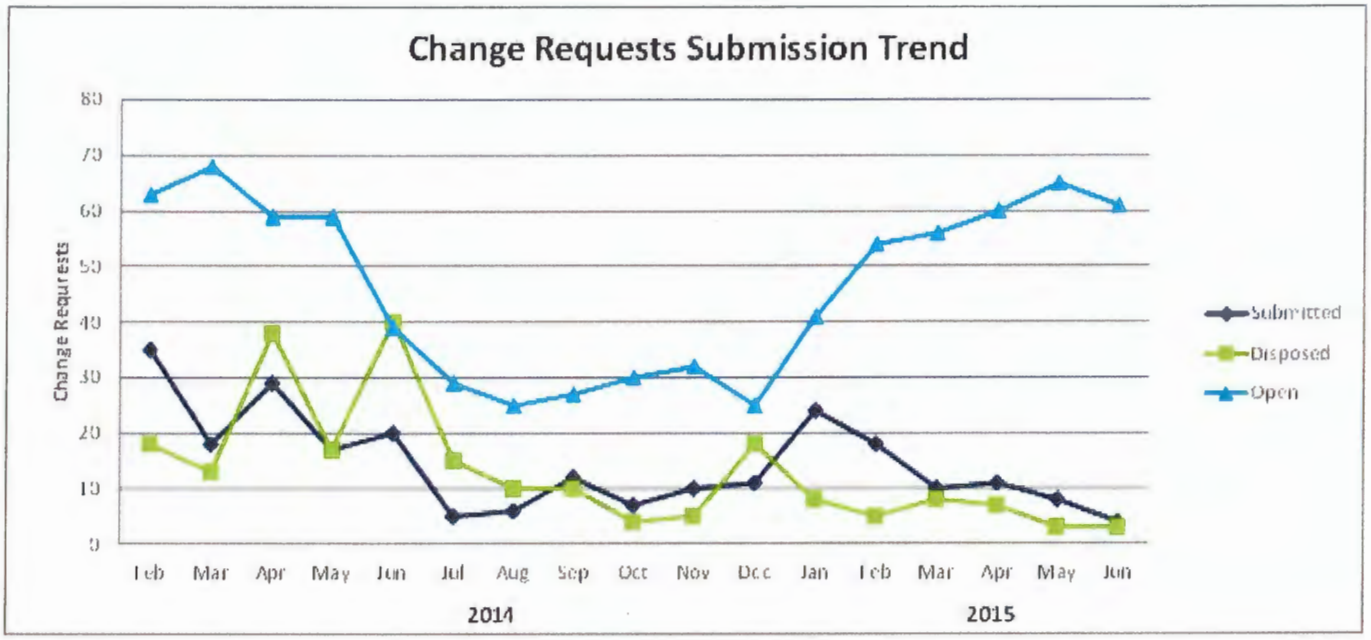
First Data.
beyond the transaction

Performance Measures

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

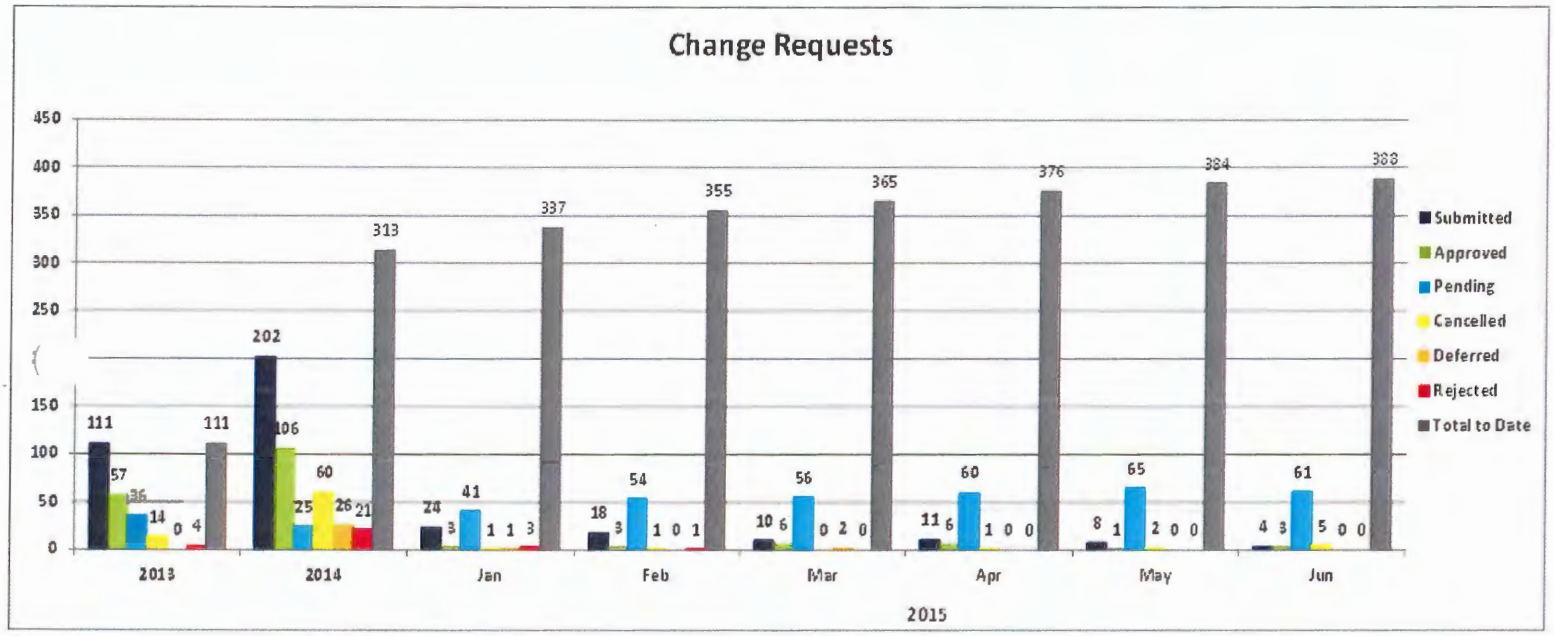
Performance Measures



© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Performance Measures



© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Questions?

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

QA Team Observations Regarding Deliverable 33h

Introduction

The OSI CalHEERS QA Section (QA Team) supported the CalHEERS PMO by conducting a high-level review focused on the updated sections of Deliverable 33h. The QA Team's review is supplemental to the overall PMO review and acceptance process. Review comments were entered into the formal review log workbook. Provided below is a summary of QA Team observations regarding the quality of Deliverable 33.

The introduction to the O&M Manual (Page 1.1) describes that Deliverable 33 is to be a single source of information for the project.

> *"The Operations and Maintenance (O&M) Manual provides a single source of documentation for all activities, processes, procedures, and tools required to operate the CalHEERS and the Covered California Service Center technical infrastructure. This manual also includes the roles and responsibilities of O&M team members who perform these activities."*

The QA Team observes that Deliverable 33 falls short of these objectives, and the State risks endorsing a flawed process by formally accepting the deliverable.

Notable deficiencies include:

- **Deliverable expectations**. Decisions regarding Deliverable 33 direction and content have been made over time but not formally documented. As a result, the original Deliverable Expectation Document (DED) is out of calibration with the current version of Deliverable 33, and is therefore unusable as a reference DED. Lack of an accurate DED complicates review of content and creates a debate about what is required within sections. There is no single source of truth for what should be included in Deliverable 33.
- **Missing content**. Sections and/or attachments are missing. In some cases, a placeholder description is provided such as, "Will be included in a future iteration of Deliverable 33."
- **Incomplete or fragmented content**. Sections are not organized to support operations. In section 19 there is insufficient design detail to validate that the delivered product meets the intended design and the requirements are met. In other cases, process descriptions cover only system integrator activies, without describing activities of the State or other process participants. In yet other cases, a cursory description in lieu of detailed instructions may be provided along with a reference link to another section, only to discover that the referenced section also lacks adequate detail.
- **Document quality**. Multiple fit and finish issues are evident throughout. Examples include, but are not limited to, inaccurate Table of Content entries, incorrect reference links within and between documents, mislabeled diagrams, and various grammatical and logical textural errors. Although such incidents are individually defended as "cosmetic errors," in the aggregate such fit and finish issues distract and increase the challenge of reviewing documents. The bottom line is the the SI can and should do a better job of reviewing/editing the deliverable documents to improve quality before submission to the State.

The following topics in this summary report provide additional detail for each category of deficiency, including references to key QA Team comments submitted to the Deliverable 33 Review Log.

Deliverable Expectations

DED out of Calibration: The review and comment process is complicated as many changes to scope, responsibilities or contracts have been made but are not reflected in the DED, change logs, or versions. This has rendered the initial DED for 33 irrelevant, and it is difficult to validate whether a requirement has been met. There is currently no single source of information that prescribes what the content for Deliverable 33 should be.

Undocumented Agreements: In many cases, there is a lack of written records for formally accepted changes or decisions to append or remove content. Through the comment review process with Accenture we learned that the QA comment regarding the sections alignment to the DED was invalid because of the State's agreement to remove CRM management as part of the deliverable since CoveredCA now manages the CRM. The QA Team was able to verify that CoveredCA and State Management approved of this change in scope in an email. However, there is no formal documentation or traceability for that decision. A majority of the section content was removed, and no notation was made as to why. This is but one example where "handshake agreements" were made on the direction or scope of the content, but not formally documented.

Reviewer	Page	Section	Comment
David Sanabria		19	DED for DEL33h was not available to reviewer, and thus an older DED for 33a was used instead. This version of the DED identified Section 19 as Section 29. There is a risk that the DED used does not match actual expectations for this section.
Karen Glabas	12.1	12.1.1	The scope of the BCP appears to be limited to displacement of the System Integrator personnel from the following application development facilities (ADF): 2329 and 2399 Gateway Oaks. This was perhaps an appropriate scope prior to Amendment 8 (when this scope was agreed to) however, Amendment 8 allowed a shift of most application development personnel off shore. Therefore, and perhaps more importantly, Section 12 must address business continuity for the off shore facility(ies) as well, as it is a significant development site.
Kristin Pepper		6	The deliverable does not meet the documentation as required by DR66. The requirement indicates that processes and procedures for the following support areas should be included as part of the deliverable. 1. Equipment, software, backups and restoration 2. Configuration changes - met in the appendices 3. Security of the Equipment, software and Network 4. Monthly usage reports - mostly met, however, the availability report requirement is not met.
Kristin Pepper		15	The structure of the deliverable does not follow the structure defined in DED34-Initial IVR O&M Management Plan as the DED indicates it should. DED Section 5 item number 15.
Kristin Pepper	6	6	The DED has a requirement for a Change/Release Management plan that describes the entire Change Request process. The CR process is not defined within the Release Plan. This should include all of the tools and templates to support Change Management.
Richard Green	5.3.4	5.6.7	Last Implementation Complete Report is for Release 6/7/8. Why are the releases post 8 not included here?
Wendy Battermann	4.27	4.5.3	Activity 10 Table, Steps section, last paragraph - Does the statement infer that if the vendor (assuming this is a non-Accenture vendor) can't resolve the problem, that Accenture takes it back to try to resolve it on their side? Please clarify in process text and Figure 4.6, as needed.
Wendy Battermann	16.4	16.2.1	If you are making an assumption, state as such. For example, "Since the Service Center Business Operations and the Facilities Management Plan are owned and managed by Covered California, it is assumed that any facility-related items (e.g. power outages, access to site, site layout) and Service Center Business Operations are defined in documents under Covered California control and would not be included in this O&M Manual."

Sample Deliverable Expectation QA Team Comments

Missing Content

There are sections where Accenture has stated that the content is "on hold," will be included in a future version of the deliverable, or are dependent upon additional CRs to modify the baseline system.

Missing Appendices: There were several Appendices that were either missing entirely or missing significant sections of the content.

Pending Future Contract Amendments: Some items were noted as being dependent on a "future contractural amendment." However, specific criteria for what might change in a contract amendment, and documentation of the decision to address this topic in a future contract amendment, were not provided.

Planned for Future Iteration of Deliverable 33: Some missing items were indicated to be included in a "future iteration" of Deliverable 33. However, specific delivery time estimates were not provided.

Dependent Upon Future CRs: Language indicates that some baseline system functionality is not available, therefore necessitating additional CRs.

Reviewer	Page	Section	Comment
David Sanabria	17	Appendix 7.4	PDF version of Appendix 7.4 contains 190 pages of useless, blank formatted tables. None of the content from the original Excel workbook is visible (four tabs missing). The PDF should be recreated and then confirmed to match original document.
Kristin Pepper	15.1 .	15.1.3	The content of this section is a general reference to other processes in the O&M manual. There is no actual description of the overview of the IVR Management process. Additionally, the section references should be more clear and provide better guidance.
Tony Fortenberry	24.1	24.5.1.20	Heading 24.5.1.20. SYSTEM BATCH EHIT TRANSACTION TIME reads, "On hold pending implementation of CR 42017." Question: Is this item still on hold? If so, when will it be delivered?
Tony Fortenberry	24.26	24.6	APPENDIX 24.2 – OPERATIONS METRICS IMPLEMENTATION AND METHODOLOGY is not present in the Appendices subfolder. The description in Section 24.6 Procedural Appendices table reads, "Will be included in a future iteration of Deliverable 33." Question: Where is Appendix 24.2? When will it be delivered?
Tony Fortenberry	24.8	24.5.1.19	Heading 24.5.1.10 24.5.1.10. SYSTEM DEFICIENCY CORRECTION – ORIGINAL reads, "On hold pending future Contractual Amendment." Question: Is this item still on hold? If so, when will it be delivered?
Tony Fortenberry	24.8	24.5.1.10	Heading 24.5.1.10 24.5.1.10. SYSTEM DEFICIENCY CORRECTION – ORIGINAL reads, "On hold pending future Contractual Amendment." Question: Is this item still on hold? If so, when will it be delivered?
Tony Fortenberry	3.16	3.1.1	Appendix 3.1 – Accenture IDF – Help Desk and Workplace Services Runbook is missing from the Appendices subdirectory.

Sample Missing Content QA Team Comments

Incomplete or Fragmented Content

Fragmented Content: There were several comments made that referenced key missing steps to the processes, or that the process was not fully documented. We also saw that processes were inadequately described when they would simply reference other sections. There was no description from beginning to end for how to maintain the systems.

Incomplete Process Descriptions: One of the Quality Assurance (QA) Team's general comments included that if the intention of the document is to be an Operations Manual document it does not sufficiently depict a holistic view of how

business is conducted on the project. The document is primarily focused on the SI managed aspects of the project and does not demonstrate the State or other vendor managed activities. This creates a fragmented view of the operations and it becomes unclear when responsibilities transition between the SI and State, or what the State or other vendor roles and responsibilities are.

Incomplete or Insufficent Design Documents: In some cases, design descriptions are either insufficient or incomplete. Through three sessions of comment review for section 19 we debated with Accenture that the design documents for the planned "Management Dashboard" are not sufficiently complete to describe the required functionality or useable design of the Dashboard. Without adequate design detail, it is unlikely a confirmed understanding between the State and Accenture is possible regarding the design of the Dashboard. The document is not organized for Operations support and to date is not fit for purpose.

Reviewer	Page	Section	Comment
Karen Glabas		12	Appendix 12.5.5, PDF format is missing pages 15 - 35 - please regenerate and provide the full document.
Wendy Battermann	4.65	4.7.3.1	Activity 12, Steps section - Missing important step in process. Where is the communication of the alternate procedure to initiator, teams, and end users? Update appropriately.
Wendy Battermann	4.65	4.7.3.1	Activity 12, Steps section - Incorrect process direction/reference. Figure 4.15 – Problem Resolution and Closure shows the process ends with activity 12, but the process description instructs the reader to "go to Section 4.7.5 - Reporting and Continual Improvement. Update appropriately. Also, change "Process" to Proceed."
Wendy Battermann	4.53	4.7.1.1	Activity 5 Table, Steps section - Missing part of instructions to proceed to match Figure 4.13 – Problem Detection, Logging, Categorization, and Prioritization. Before the text "Proceed to activity 6," add, "The Configuration Management team will proceed to Section 17 – Configuration Management, and the Asset Management team will proceed to Section 18 – Asset Management."
David Sanabria	19.5	19.1.1	Document implies that Systems Operations Dashboard has not been built, however the application (OBIEE) is actually installed and is listed on the CalHEERS SharePoint page. Section 19.1.1, paragraph 1, line 4 says "The Systems Operations Dashboard will showcase". a. If this application is actually available for use, this language should be updated to reflect present test: "The Systems Operations Dashboard showcases". Additional language and phrasing throughout the section refers to "to-be state" and uses future tense wording. In order to be more clear, the language tense should be updated to use present tense, or else provide information to the reader to provide the project/change/or other external reference where the reader can find the current status of the Sys Ops Dashboard capability. b. Paragraph 1, line 7 says "This document will describe the 'to-be' design...". Does this mean that the document is incomplete, and when completed will actually provide the "to-be" design? Or does the document already describe the "to-be design", and this wording is just awkward and/or out of date? Suggestion: Clarify when the document will provide the "to-be design" or update this paragraph to eliminate the confusion and note the "to-be design" is already in this document.

Sample Incomplete or Fragmented QA Team Comments

Document Quality

Table of Contents: There were issues with inconsistent pagination numbering between the document, missing content, inconsistent naming of figures between the section content and the Table of Contents and other cosmetic issues. These are primarily cosmetic issues that could be easily addressed prior to State review.

Document References: The referential integrity issues to sections listed within the document create a workload issue for reviewers. For example, instead of describing a maintenance process the vendor will refer the reader to another section; however, the maintenance process is not described there. This creates a document that is fragmented and incomplete. Furthermore, this could become amplified if Accenture begins performing quarterly updates of a few sections at a time.

Consistency: In general, the document lacks continuity with the level of detail provided. For example, one section may provide a detailed account of each contributors role, and others are high-level. It was difficult to provide comments to state the information is inadequate when the DED is no longer relevant.

Reviewer	Page	Section	Comment
David Sanabria	17	Appendix 17.1	PDF file version of Appendix 17.1 has bad page breaks
David Sanabria	17	Appendix 17.3	Appendix 7.3 does not have any headers or footers, and is inconsistent with appearance standards for MS Word Documents. The document should be updated to use CalHEERS paragraph and character styles. Headers and footers should be added. The PDF version should be recreated.
Karen Glabas	12		For all BCP appendices , section 4.3 Checklist for Recovery, Checklist and Procedures table - the link provided in the column **Reference to operational recovery procedure** is inactive. Please fix in all BCP appendices.
Kristin Pepper	15.9	15.6	The section refers the reader to Section 16 for more information on Software and Equipment management, however, that is not addressed in deliverable 16.
Kristin Pepper	6.5	6	Appendix 6.5 does not have the current version of the milestone schedule currently used in Release Management.
QA Team			If the intention of the document is to be an e Operations Manual document it does not depict a holistic depiction of how business is conducted on the project.
Tony Fortenberry	3.1	3.1.1	Broken reference link: "As defined in **Error! Not a valid bookmark self-reference.**"
Wendy Battermann	4.13	4.5.1.1	Activities 10 and 11 Table - Check role consistency between this section and Section 17. The closest role to incident management that is mentioned in Section 17 is the CI User. There is no mention of the Incident Creator or Incident Initiator. Make consistent between sections.

Sample Document Quality QA Team Comments

Appendix 6

Workstream Status Report

Workstream Status	
Week Ending:	10/3/14

Workstream: Independent Verification & Validation (IV&V)

Summary of Activities Completed	Summary of Planned Activities

• Participated:
  • Daily UTE Touch Point
  • Defect triage calls
  • Weekly Change Control Team
  • Renewal Team Meeting
  • CMS/Idaho Weekly Check in call
  • IV&V daily team review
  • GI Check Point 5 Demo
  • Outreach and Education Committee
  • Blueprint Test Execution
  • R0, R1, R2 SIT Result s Review
  • PMO Weekly Status (Integration) touchpoint
  • PMO Weekly Training Plan Touchpoint
 	
• Deliverables Reviewed and Feedback Provided
  • Re-review Database Design Document
  • CP5 Demo Feedback
 	
• Deliverables Submitted
  • Weekly IV&V Status Report
  • Attestations as ready and needed
  • Month 5 IV&V Report, Status Report, and Technology Vendors Reports
	• Planned Participation:
	  • Daily UTE Touch Point
	  • Defect triage calls
	  • PMO Weekly Status Touchpoint (GetInsured)
	  • CMS/Idaho Weekly Check-in call
	  • Weekly Change Control Board
	  • Weekly IV&V Check in
	  • PMO Training Plan Touch point
	  • Weekly DHW status meeting
	  • R2 UAT 1B
	  • Blueprint Test Execution
	
	• Deliverables to be Reviewed
	  • Preliminary Contingency Recovery Plan (not delivered)
	  • R2 Preliminary Manuals and Training Materials
	  • Security/Privacy assessments
	  • R0 R1 User Manuals (first draft reviewed in July, not re-delivered)
	  • R1 Performance Test Plan, Scenarios/Scripts (in review now, due 10/7)
	
	• Deliverables to be Submitted:
	  • DRAFT Pre-Implementation Assessment of Security/Privacy Plan
	  • Project Artifact Archive (Flash Drive format)
	  • Deliverables Observation Report

Your Health IDAHO

New Issues and Risks

Workstream: Independent Verification & Validation (IV&V)

Item	Workstream at Risk	Severity	Mitigation/Resolution Plan	Date Added	Status
Deviations from established process, e.g.: • Issue/Risk Review • Training Materials Review	Governance	**Medium**	Monitor closely, limit deviations from process to absolutely necessary occasions	**9/25/2014**	Monitor
Carrier concern relating to steps regarding re-enrollment; training materials could resolve this but their creation is behind schedule.	Stakeholder Management / Outreach	**High**	Focus more attention on Carrier concerns regarding Enrollment; Develop a written Process Document for EARLY distribution to Carriers to alleviate concern prior to Training Documents.	**9/25/2014**	**OPEN**
Proprietary Software concerns on the part of GetInsured are impacting documentation quality, e.g.: Database Design Document	GetInsured	**High**	Conformance to MITA standards is recommended; YHI and GI may need contractual agreement for sharing proprietary information concerning documentation, especially Data-related documentation	**9/25/2014**	**OPEN**

DHCS
California Department of HealthCareServices

Weekly PMR Meeting Minutes

Project:	Short-Doyle Data Analytics	**For week of:**	April 15, 2016
Submitted by:	Jim Glick	**Date submitted:**	April 19, 2016

Conference Call Number: 1-866-565-9019 pc: 6785389#

Distribution and Attendee List:

(X indicates that the member was present; T indicates present via teleconference

X	Bob Sands	X	Marty Bornstein	X	Tony Amato
	Amanda Huston	T	Jim Glick	X	Greg Loos
			Ron Fitzgerald		Greg Hanes

Completed Activities:

Activity	*Status*	*Assigned to*	*Comments*
SIU Social Connect Project	Completed	Amanda	SIU provided social connection report for LA Strike Team

In Progress Activities:

Activity	*Status*	*Assigned to*	*Comments*
Dual Factor Authentication	In Progress	Greg/Ron	Pondera would like to work with DHCS ITSD's network and system team to do some further troubleshooting. *Working, but not as expected. Test session to be scheduled this week now that Tony G has returned. Also, scheduling session to review Laura Langston's social connect. No Updates – meeting to be scheduled by Bob with Barney to discuss the options.*
Delivery of claims data for Short Doyle with the new data elements	In Progress	Marty / Amanda	The first file was delivered to Pondera, who completed analysis and cleared for the rest of the historical data delivery. 1. ESB (Prakesh) will give us a schedule. 2. Q/A needs to be assigned a. Monthly (ESB) b. Subset of historical files (Mark G., Marco?) c. review only the October, April files every year.

DHCS
California Department of
HealthCareServices

Weekly PMR Meeting Minutes

In Progress Activities:			
Activity	*Status*	*Assigned to*	*Comments*
Encounter Data	In Progress	Marty	Optum having spool issues. But ready to zip files and send. *2011 – 2014 have been created and work is continuing on 2015 and then the 2016 file will be created – these should be available by the end of the week. Q/A will likely be done by Bernie.*
Hotlist Development	In Progress	Amanda / Tony Amato	Received the first file format (no data). Pondera is reviewing and working on dashboard integration development requirements. Hotlist indicator will be added to FDaaS SuperSearch and Profiles. *Stan said just '1' was added.* Mockup sent to Bob for review. Plan to integrate this into SS when new merged dashboard is released.
Mental Health Analysis	In Progress	Amanda / Tony G	Policy meeting held 4/8/16. Pondera provided notes and action items listing. Mental Health will continue to review flags with Pondera for upcoming Dashboard merge. Meetings are held Monthly
Mental Health Inv. Project	In Progress	Amanda	Data discussion held on 4/5/16. SIU team will prepare a full intelligence brief. Amanda would like to review the draft with Tony G prior to strike team briefing. Plan to set up this review session for next week.
CDCR	In Progress	Bob	Bob has obtained agreement from CDCR to provide DHCS with a Quarterly Report. Tony Guzman will prepare a Data Use Agreement with CDCR. *Tony A. will follow up with Tony G. Brenda is working on a unified data approach for all departments – there will most likely be a quarterly report.*

DHCS
California Department of HealthCareServices

Weekly PMR Meeting Minutes

In Progress Activities:			
Activity	*Status*	*Assigned to*	*Comments*
Ownership Information and Data Dictionary	In Progress	Tony G / Marty	Pondera's data on provider file is stale and unstable. Meeting last week with Munay. Summary as follows: 1) Munay's system contains the most accurate MH provider information (Facilities and Billing providers only) that updates every day 2) All of the provider fields requested are avail 3) Info for providers in other programs can be obtained from SMART database 4) No validation for rendering providers unless it's FFS. In which case, they check the first 3 digits of their Tax ID 5) Bene eligibility and other requested demographics are contained in MISDSS in the "Fame_Response" table 6) Mark Gustafson to follow up with Munay in getting access to Munay's MH Provider data 7) Munay also has access for ITWS, system housing all databases for Medi-Cal
Gatekeeper List	In Progress	Amanda	Gatekeeper list received from PED. We have identified data quality issues such as missing NPI, naming convention mismatches, etc. Bob set up a meeting for mid-May with PED.
Link Team Enhancements	In Progress	Amanda	Meeting held to review link team feedback on SS and Network Analyzer. Pondera is processing the requests for upcoming development sprints. Team should meet bi-weekly to review progress and review new items.
Social Connect	NEW	Greg	Discuss status of application going forward

Planned Activities:			
Activity	*Status*	*Assigned to*	*Comments*
Work with Strike Team to identify and incorporate additional data sources	Planned	Bob / Amanda / Tony Guzman	Team will work with the State to individually identify new data sources for FDaaS integration • Group home data from CDSS (waiting on

DHCS
California Department of
HealthCareServices

Weekly PMR Meeting Minutes

Planned Activities:			
Activity	*Status*	*Assigned to*	*Comments*
			updated MOU). Bob sent citations for A&I public records request exemptions to CDSS. *Bob will facilitate a meeting with CDSS to follow-up.* • OSHPD – Pondera is reviewing data and will make recommendation. More appropriate for Fee for Service and Managed Care. • Citizen Audit – meeting with Debi was held Monday to review results. Debi and team had not yet reviewed report and therefore did not advise on what data they want integrated into dashboard. They agreed to review the report and provide feedback. They will also provide SIU with a list of names that they would like checked in Citizen Audit database.
Dashboard Merge (DMC and MH)	Planned	Pondera Dev	First monthly file has arrived. Need estimate from IT on delivery of remaining files. Waiting for updated data to produce full results and ranks, identify iterations of claims, more accurate payment amounts, place of service identification, etc.
Case Management Enhancements	On Hold	Amanda / Bob	Amanda provided an enhancement list to Bob to review prior to making any updates for guidance and approval.

Decisions:			
Activity	*Status*	*Assigned to*	*Comments*

Upcoming Milestones			
Milestone	*Resource*	*Start Date*	*End Date*

DHCS
California Department of
HealthCareServices

Weekly PMR Report

Open Project Issues:

#	Finding	Risk Likelihood	Recommended Action	Status	Open Date	Target Resolution Date	Owner

Open Project Risks:

Data integrity issues – see above on "data issues" – this updated data was scheduled to be received on 3/23/15 (still outstanding).

Data Issues:

#	Finding	Risk Likelihood	Recommended Action	Status	Open Date	Target Resolution Date	Owner

Appendix 7

COLORADO HEALTH BENEFIT EXCHANGE

First Data.

State of Colorado Health Benefit Exchange

IV&V Bi-Monthly Report
Review #1 Initial Assessment

For Period of December 2012- January 2013

Version 1.0
Submitted January 14, 2013

Draft Work Product

Revision History

Version No.	Date	Summary of Changes	Modified By

Draft Work Product

Table of Contents

1.0 Introduction 4
1.1 Background 4
1.2 Purpose and Scope 4
1.3 Approach and Methodology 5
1.4 Roles and Responsibilities 6
2.0 Executive Summary 6
2.1 Overall Project Status 7
3.0 Assessment and Recommendations 11
3.1 Details of Analyzed Areas 12
4.0 Risks and Issue Management 75
4.1 Risk Log 75
4.2 Issue Log 80
5.0 Appendix 84
A. Meetings Attended 84
B. Interviews Conducted 85
C. Example Graphical/Timeline 86
D. Example End to End Release Schedule 87
E. IV&V_COHBE Project Schedule_011413 88

Draft Work Product

1.0 Introduction

This section provides an overview of the Colorado Health Benefit Exchange (COHBE) and the scope of Independent Verification and Validation (IV&V) Services as it relates to the COHBE.

1.1 Background

The Patient Protection and Affordable Care Act (PPACA) was signed into law on March 23, 2010. Following, in May 2011, the Colorado General Assembly passed Senate Bill 11-200, which established the Colorado Health Benefit Exchange (COHBE), a public entity governed by a Board of Directors. COHBE selected CGI as the Systems Integrator (SI). CGI commenced work on June 06, 2012. The Colorado Health Benefit Exchange (COHBE) intends to increase access, affordability and choice for individuals and small employers purchasing health insurance in Colorado. The implementation of the Exchange System will be in accordance with federal guidance from Centers for Medicaid Systems, HIPPA and IRS 1075 regulations. The Exchange will also provide technical interoperability with, multiple federal, state and carrier systems required to operate individual and SHOP Exchanges. The design of the Exchange System will leverage several commercial-off-of-the-shelf (COTS) products plus modifications made by the System Integrator (SI), CGI. Additionally, the Contact Center Solution will utilize Oracle RightNow. The following COTS products are as follows:

- hCentive: The product will enable eligibility determination, plan selection and enrollment capabilities.
- Healthation: The product will enable billing/accounts receivables.
- Oracle CRM: The product will provide the Customer Relationship Management functionality.

1.2 Purpose and Scope

COHBE selected First Data to provide Independent Verification and Validation ("IV&V"). The IV&V consist of services to provide an independent assessment of deliverables and performance under the Systems Integrator (SI), CGI Contract. To confirm CGI's compliance with the following activities: requirements of the CGI Contract, applicable laws, regulations and other government requirements, COHBE third party software license agreements, policies, procedures and requirements, and industry best practices (collectively, "Exchange Requirements"). The main goal of IV&V is to assist the COHBE Project by identifying technical, financial or scheduling deficiencies with CGI's performance under the CGI Contract; or in meeting the Exchange Requirements as early as possible in the life cycle.

Draft Work Product

The IV&V Team will perform five bi-monthly interim Exchange reviews. The services will be provided in the timeframes as specified below, as more specifically directed by COHBE within a reasonable time prior to each review:

Review #	Duration of Review	Approximate Timeframe	Status
1	7 weeks	November – January '13	Completed
2	3 weeks	February '13	Not Started
3	3 weeks	April '13	Not Started
4	3 weeks	June '13	Not Started
5	3 weeks	August '13	Not Started

1.3 Approach and Methodology

In order to conduct the review of the COHBE Project, the IV&V Team will use the three-phased framework as specified by COHBE:

Phase 1 - Gather required materials from COHBE and review materials off-site. These materials include but are not limited to the following:

- CGI Contract
- COHBE software license agreements
- Applicable government requirements
- COHBE policies, procedures, and requirements including:
    - Security and privacy
    - Back office processes and procedures
    - Interfaces and data sharing
    - Reporting
- Business process documentation
- Requirements analysis and change control procedures
- Schedule management, progress reporting and metrics
- Exchange design and development activities and artifacts
- Testing activities and documentation
- Deployment activities

Draft Work Product

- CGI Contract deliverables
- Customer service center implementation deliverables

Phase 2 - Conduct initial on-site meeting and present plan for all on-site activities, e.g. on-site interviews, attend meetings, review documents, follow-up Q&A and wrap-up meeting/debrief.

Phase 3 – Prepare the draft report to COHBE identifying any failure of the Exchange to comply with the Exchange Requirements, obtain COHBE comments, prepare and submit final report and present major findings/recommendations to COHBE leadership.

1.4 Roles and Responsibilities

The following table documents the roles and responsibilities associated with the development, review and approval of the deliverable.

Deliverable Roles and Responsibilities

ROLE	PERSON	RESPONSIBILITY
First Data Deliverable Owner	Yen L. Pham	Responsible for the Bi-Monthly Review deliverable.
Colorado Health Benefit Exchange Lead	Gary Schneider	Responsible for feedback, and approval to the deliverable.

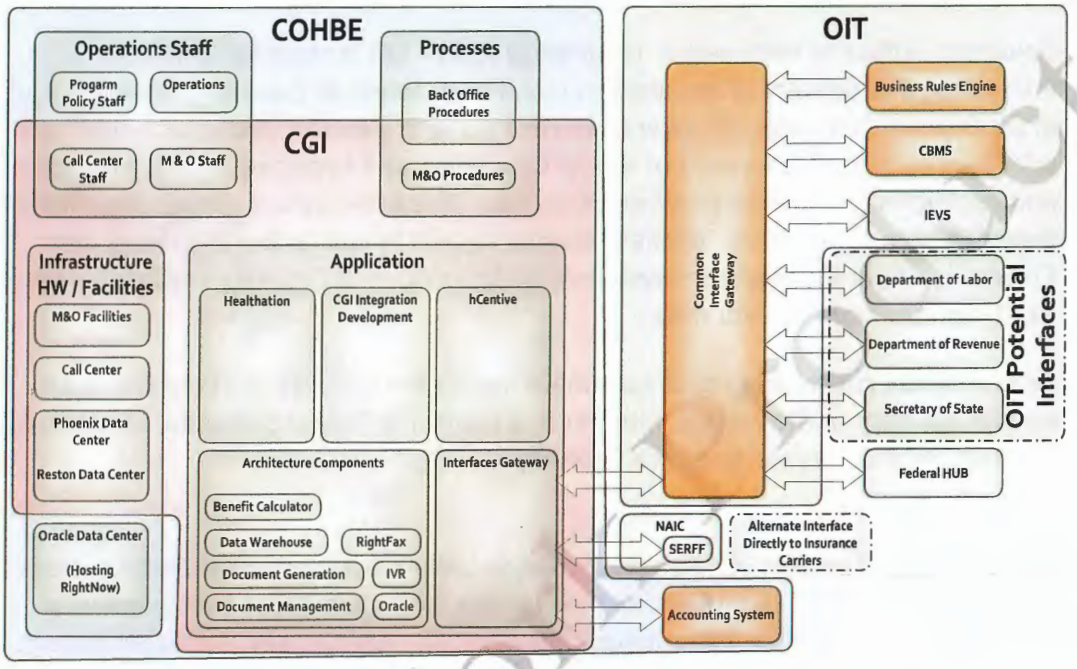
2.0 Executive Summary

This section provides an overview of the monthly reviews conducted by the IV&V Team. This assessment covers the period from November 26, 2012 through January 11, 2013. The report is a point in time. The IV&V Team typically has a cutoff point of one week prior to when the report draft is due. However, if significant new information is available, we will incorporate into our final report. For this review, the cutoff point was January 02, 2013 for the exception of the Technical areas; the cutoff point was January 10, 2013. This was due to the lack of response of requested materials and time from the CGI, in which resulted in an Amendment to the existing Change Order to extend the IV&V assessment period. This report includes review of numerous artifacts, participation in various meetings (reference Appendix A) and discussions with several COHBE Staff members (reference Appendix B). First Data has proactively communicated concerns to both COHBE and CGI as applicable for purpose of timely corrective actions.

Draft Work Product

2.1 Overall Project Status

The Exchange System consists of many components and several organizations and vendors to build. The following graphic represents these components, organizations and vendors.



The organizations of the Colorado Exchange are:

- COHBE – Has the overall responsibility for implementing an Exchange in the State of Colorado. COHBE has the operational responsibilities for the Exchange as well as contract management responsibilities for all of the contracts that build, maintain and operate the Exchange. These contracts include CGI, hCentive, Oracle and the Accounting System. COHBE is also a major source of funding for the OIT Common Interface Gateway and the associated interfaces. In addition to the four primary organizations or vendors who have specific contract responsibilities, there are a number of other items represented in the graphic that have been identified as either planned or potential interfaces notated by the dotted lines.

- CGI – Is the System Integrator (SI) to COHBE and has responsibility for the design, development, integration, implementation and operation of the Exchange System. The integration of all hardware and software components that are part of the Exchange System should meet the requirements as specified in the contract. The scope of the CGI contract also includes hardware, facilities, data center service and operational services.

Draft Work Product

- hCentive – Is the developer of the COTS product that forms the basis of the online Exchange System. The software licensed belongs to COHBE and CGI is responsible for the customization and integration of the hCentive COTS product into the Exchange System.

- Governor's Office of Information Technology (OIT) – OIT is responsible for the integration and delivery of information technology across all Executive Branch Agencies in the State of Colorado. OIT intends to contract with a vendor and establish MOU's with the Colorado Department of Health Care Policy and Financing (HCPF) to procure and implement a Common Interfaces Gateway. This gateway will include the eligibility determination transactions for the Exchange System as well as key interfaces with Colorado Benefit Management System (CBMS), Integrated Eligibility Verification System (IEVS) and the Federal Data HUB.

There are several key critical areas that potentially impact the October 2013 Go-Live date. These are Management of the Project, Monitor and Control of Project Schedule, hCentive COTS product and OIT/HCPF Common Interface Gateway.

- Management of Project –Effectively managing the project is essential to the success of the project. CGI lacks of integration management, which includes management of scope, time, cost, quality, communications, and risk. Additionally, corrective actions are not timely. The management of scope has been in the 'Red' Status for several weeks; though some activities have taken place to resolve the issue; a documented Action Plan does not exist to move the status out of 'Red'. There is not a clear cross walk of the Change Request (CR), manual versus automated Back Office procedures; and how these map to the technology contract. The management of quality has been in the 'Green' Status for several weeks but many work products are incomplete such as the Project Schedule and the HIX Solution High Level Requirements. The Use Case lacks clarity on the design of the Exchange System. Not all of the work products are shared or reviewed with COHBE, which can lead to re-work. A Release Schedule does not exist; which leaves a lot of ambiguity. The active management of risk has been intermittent and untimely. There are several Critical and Major Risks logged but yet some of the Risks have no Mitigation Plan nor does it provide a detail Action Plan.

- Methodology - CGI lacks a consistent overall methodology that is applied to the Project Schedule, System Development Life Cycle, defined set of deliverables and work products. As the project progressed, modifications to the methodology, deliverables and work products has been made on a tactical (break fix) basis versus strategic (holistically planned) approach. CGI started with a methodology for the Project Schedule but because the methodology was not working, a combination of iterative and

Draft Work Product

waterfall methodologies have been adapted. For example, the use of Iterations 1-5, 6-10, etc. in the list of project deliverables has lost meaning without the use of their proposed methodology. This has resulted in a number of terms that are used to describe a unit of functionality including, increment, Use Case, Release and Group, that are all being tracked in various project documents. When the current methodology was inadequate for prioritization, reporting and delivery, each of these terms was added to their methodology on an as needed basis. Another example is the Wireframes were not a proposed work product or deliverable, but was later added to provide clarity to the design of the Exchange System. However, Wireframes are not being completed for every Use Case due to a lack of time. This evolved methodology lacks the internal consistency necessary to be confident that the system will meet all of the requirements.

- Project Schedule – The Project Schedule is an integral tool in managing a Project. The CGI Project Schedule lacks consistent organization and methodology. The Project Schedule had evolved over time through several discreet methodologies and the cumulative effect resulted in a Project Schedule that has the remnants of each of the previous methodologies. Therefore, it is difficult to decipher how the use cases and technical work converge into a holistic solution (including all horizontal work streams). The Project Schedule has an enormous amount of late tasks. There is no time built in the Project Schedule to handle re-work or defect. CGI is unable to determine at this time how these tasks affect the Go-Live Date. CGI has been and is currently in the process of re-structuring their Project Plan, in addition to re-visiting various delivered deliverables and work products. A date has not been provided as to when the Project Plan will be comprehensive and steady; nor a re-delivery date of the deliverables and work products. It is uncertain whether all of the components for the Exchange will be ready by October 2013. Additionally, there are two other schedules, the COHBE Project Schedule, and HCPF/OIT Project Schedule; it is critical the activities align across the Project Schedules. Each of the Project Schedules is managed individually; this adds additional risk to the project as no one owns the breadth of the project as a whole.

- hCentive – The hCentive product will implement all of the online functionality in the Exchange system and used by customers, brokers, navigators and COHBE workers. The hCentive product was procured as a COTS product but has never been implemented in a form that is similar to COBHE needs or requirements. This makes the product more similar to a custom development effort than the installation of a COTS product. hCentive' s significant development effort requires a much greater insight than COHBE and CGI currently have or would usually be required for a COTS product. The Project Schedule does not document a sufficient level of visibility into these efforts including the alignment of development, testing and deployment activities between CGI and hCentive. Additionally, hCentive releases are not being delivered in deployable

Draft Work Product

modules, e.g. the functionality in each release is not complete from either an individual user role or group of user's perspective. For example, a single dot release does not deliver all of the functionality for Broker/Navigators or for Anonymous Shop. Therefore, the successful testing of hCentive is dependent on the completion of the entire hCentive development effort and required customizations. This means that significant potential defects in the hCentive functionality are not discernible until the last release because the end-to-end functionality is not testable in the earlier releases.

- OIT/HCPF Common Interfaces Gateway – The interface is the eligibility transaction of the Exchange System is the eligibility transaction. There is a potential risk that the Exchange Eligibility Rules will not be ready by the October Go-Live date. Currently, discussions are in progress amongst OIT/HCPF and the Deloitte vendor whether the Eligibility Rules Engine was part of the original scope. This is discerning as the 'eligibility rules' is an integral piece of the Exchange System. Additionally, procurement with OIT is currently in progress and HCPF lacks the resources for the development of the interface. CGI has started development of the interface without having the full details of the interface design, which adds additional risk. COHBE is solely dependent on OIT to build the eligibility transaction and there is no mitigation plan in place.

The Exchange Project is behind schedule, the key critical key areas mentioned attribute to the schedule slippage. Below is a high-level summary of the late items. As noted, since the Project Plan and work products are influx it is challenging to assess what is truly factual. The numbers below and the numbers referenced throughout the report may not be accurate but based on materials collected at a point in time.

Item	Metric
Late Tasks	640
Critical Tasks	840 with zero or negative slack
Late + Critical Tasks	155
Use Cases	42 completed out of 51 planned
Design	10 completed of 89 planned
Deliverables	8 completed of 17 planned

The preceding areas contain the details of the assessment and recommendations. In addition, the identified risks and issues.

Draft Work Product

3.0 Assessment and Recommendations

This section includes the assessment and recommendations identified as part of the Bi-Monthly Review effort. Each area of concern is categorized using the following rating:

Symbol	Rating	Description
	Met requirement	All the processes, as identified, are working within contractual standards and were reported accurately. Though there may be some issues, risks or areas of potential improvement, they do not affect the project's success.
	Review could not be fully conducted	Data provided by COHBE or CGI to conduct the review did not permit full compliance validation or either data was unavailable due to the current phase of the project. First Data will need to work with COBHE or CGI to determine if any further documentation is available to perform a complete compliance validation review.
	Met requirement with inaccuracies	Review determined that relevant contractual standards meet, but inaccuracies were found in the data, processes, or end reporting used in the demonstration of compliance. There may be some issues, risks or areas of potential improvement; they could affect the project's success.
	Requirement not met	Element reviewed did not meet project compliance and may require immediate attention and/or escalation to senior management. There are some issues, risks or areas of potential improvement; they do affect the project's success.

Draft Work Product

3.1 Details of Analyzed Areas

Status	No.	Area	Sub-Area	Assessment and Recommendations
	1	**Project Schedule**	**COHBE**	**Assessment** COHBE has developed a draft version that incorporates their best knowledge with respect to the key activities, associated deadlines and interdependencies to October 1, 2013 and in some cases beyond. **Recommendation** 1. Since there are multiple Project Plans, it is imperative to align all of the Project Schedule.
	2	**Project Schedule** *(Version Dated 010113)*	**CGI**	The Project Schedule is not monitored and managed in a timely manner: Of the 3717 total tasks, there are approximately 640 late tasks. On a project , the typical standard for late tasks should be +/-2%, the Exchange Project is at 17%. The details are as follows: **Task Owner** / **No of Late Tasks** Architecture 19 Architecture BI 3 Back Office 26 COHBE 4 Development 301 Functional 61 hCentive 16 Healthation 26 Implementation 33 **Task Owner** / **No of Late Tasks** Operations 6 PMO 6 Project Management 6 Quality 2 Solution Architecture 32 Testing 21 Training 1 Unassigned 77

Status	No.	Area	Sub-Area	Assessment and Recommendations
				There are 43 late tasks in Release 0.2. It is not transparent in the Project Schedule of those that were late, which ones were re-prioritized for the upcoming release. It is unclear how the late tasks affect the overall project schedule. There are 54 late tasks in Release 0.3. It is not transparent in the Project Schedule whether the tasks will complete on time. If these tasks are not complete on time, it is unclear how these late tasks affect the overall project schedule. There are 35 late tasks in Release 0.4. It is not transparent in the Project Schedule whether the tasks will be complete on time. If these tasks are not complete on time, it is unclear how these late tasks affect the overall project schedule. 508 late tasks do not have an assigned Software Release. A Task has a Software Release when it is software related. In general, all other tasks for Go-Live are in Release 1. However, there are components such Notices, Logical Data Model, Technical Architecture, Imaging, Thunderhead, and Healtation, etc. that are fundamental to the Exchange System. It is not transparent whether these components will be ready for Go-Live. The approved Change Requests are not transparent in the Project Schedule. The schedules only reflects the CR3 but are integrated across many tasks. There are references to 'Iterations and/or Increments' referenced via various

Status	No.	Area	Sub-Area	Assessment and Recommendations
				deliverables and documents, though it is not transparent in the Project Schedule which tasks are related to Iterations 1-5 versus 10-15 versus 16-20. For traceability purposes, nomenclature made in the Project Schedule should align with Deliverables, Work Products and SOW. The Project Schedule does not reflect formal review of Functional and Technical work products such as General System Design, Detail System Design, and System Test Scripts/Scenarios, etc. This has led to re-work and could potentially lead to additional re-work downstream. Consensus amongst all Stakeholders should occur in the onset. CGI has stated due to the compressed Project Schedule, time for re-work and/or for defects is not built-in. It is likely this will affect the overall project schedule. Reference the Area SDLC- Design Area for section specific assessment and recommendations. The Project Schedule lacks consistent organization and methodology. There are references to Phases, Increments, Iterations and Use Cases, etc. but the use of the references is not consistent throughout the Project Schedule. It is challenging t to determine how they all coincide. A few of the Working Teams members have stated, the 'next steps' are not transparent in the Project Plan; therefore it has been difficult to plan for upcoming activities. Additionally, the tasks lack detail information as to which modules fit into which release. Some examples are: • Task 3066 System Test Start R 0.2: Unable to determine which modules will be part of R 0.2. • Tasks 11400 UAT Start R 0.3: Unable to determine which modules will be part of R 0.3.

Status	No.	Area	Sub-Area	Assessment and Recommendations
				• Task 5848 hCentive Roadmap: This task contains several sub-tasks that are for specific releases. Unable to determine modules contained in the release and differentiate between development by HCentive, CGI or custom versus baseline. • Task 11736 Define Functional Specifications for Carrier Interfaces: This has a couple of sub-tasks but does not reflect the dependencies with Issuer Activity, DOI, Activity, HHS Activity, nor COHBE Activity. The tasks related to Carrier are not collectively organized. The tasks related to System test are in the middle of the project schedule and tasks related to Functional Specifications are at the end of the Project Schedule. The Project Schedule does not contain COHBE, hCentive or OITs specific tasks; therefore, the dependencies and critical path is not transparent. Additionally, it is unclear who will be monitoring and managing the individual, Project Schedules. The Project Schedule lacks a holistic view of the full development life cycle; therefore, it is difficult to decipher the current phase of a particular task. The Project Schedule is a combination of iterative and waterfall methodologies that have adapted over the course of the project to meet the changing needs at that point in time. Additionally, the work streams were developed by various resources, and were never modified to have a cohesive method. Some examples are: • Task 11402 Development for Healthation Component: There is no Analysis Phase, System Test or Release indicated.

Status	No.	Area	Sub-Area	Assessment and Recommendations
				• Task 2261 JAD/Use Cases/Detailed Design/Build: This tasks lumps all of the activities together, whereas other tasks areas are broken out by phase. The Project Schedule lacks detail information and key milestones dates from Stakeholders. COHBE and CGI Project Staff should have a common understanding of development activities; and where the business process activities converge. This ensures milestones and critical dependencies are met. For example: • Task 11720 Create End to End for Group 1: Lacks information on what is contained in Group 1. • Task 11733 Define Functional Specifications for OIT Interfaces: Task only contains two lines items reflecting developing high-level business requirements and functional specifications. There is a lack of information detailing OIT tasks versus CGI and COHBE tasks. In addition, lacks of integration points and key dates. • Task 117736 Functional Specifications for Carrier Interfaces: Task only contains four line items reflecting of high-level sub-tasks. There is a lack of information detailing analysis, design, integration points, key dates, etc. The Project Schedule contains 917 critical tasks, of those, there are 814 tasks with either zero or negative slack, which indicates there is an issue and most likely will impact the overall project schedule. There is a lack of a consistent formal review of the Project Schedule with

Status	No.	Area	Sub-Area	Assessment and Recommendations
				COHBE. **Recommendation** 1. Assess the late tasks and determine how they affect the overall project schedule. 2. Assign Software Release to each task in order to verify whether these components will be ready for Go-Live. 3. Assess the late tasks in Release 0.2, Release 0.3 and Release 0.4 and determine if these are on the critical path. Determine if these late tasks affect the overall project schedule. Develop an Action Plan to get back on schedule. 4. Add an identifier to approved Change Requests within the Project Schedule for transparency. 5. Add the relationship of 'Iterations and/or Increments' to the tasks. 6. Integrate formal reviews of Functional and Technical work products to provide more visibility around General System Design (GSD) and Detail System Design (DSD) is needed due to CGI's methodology Approvals of work products should occur before moving onto the next phase to avoid re-work. 7. Restructure the Project Schedule to have a consistent 'methodology'. Each 'Iterations/Phase/Group" should have an Analysis, Design, Build, Test, Deploy task. Standardize the schedule to enable easy filtering of each area, for example using WBS Level 1 and 2 to differentiate CGI from COHBE tasks. CGI recommends utilizing the predecessors of the Development Integration tasks and/or the Development Tracking Spreadsheet to provide a view of all Use Cases that are part of a given release. Though the predecessors of the "Development Integration" tasks enables the end user to view all of the various Use Cases that are part of a given release, it does not provide a view of which

Status	No.	Area	Sub-Area	Assessment and Recommendations
				modules fit into a release, as the Use Cases crosses several releases. The "Development tracking spreadsheet" contains a detailed development progress of the Use Case inventory, but not at a module/functional level. 8. Integrate the Project Schedule to have a universal view and gain a perspective on cross dependencies and critical paths amongst Stakeholders. Assign an owner to manage the integrated Project Schedule. CGI recommends utilizing a combination of the summary task containing the software releases, the release notes and the gap analysis spreadsheet to determine cross dependencies and critical paths. The summary only contains very high-level tasks but does not provide the end user a detail view. Tasks such as Gap Analysis, Release, etc. should reflect in the Project Schedule for transparency, additionally review of these work products by COHBE. 9. Restructure the Project Schedule to include milestones, groupings of end-to-end scenarios, and integration points for each module (e.g. hCentive, Interface Carrier, etc.). CGI recommends utilizing the Functional Architecture Spreadsheet in combination with the Project Schedule to view the priority groupings. However, this still does not provide the end user a holistic view of a project in one location. 10. Due to the overwhelming number of tasks, develop a graphical depiction reflecting integration points and of key dates, this will provide transparency to the Working Teams. An example referenced in Appendix C. 11. Develop an end-to-end Release Schedule detailing the specific modules to ensure common understanding and, transparency; keep the Release Schedule aligned with the Project Schedule. An example referenced in Appendix D. 12. Review the Project Schedule on a weekly basis with COHBE, highlighting: • The late and critical tasks, how these impact the October Go-Live Date

Status	No.	Area	Sub-Area	Assessment and Recommendations
				• Risks and Issues • Action Plan and Mitigation Plan if applicable • Changes to the Project Schedule
	3	**Deliverables**	**DEL01 Development and Integration Test Environments Available** *(Version Dated 072712)*	**Assessment** This deliverable is a software deliverable as specified by the contract, therefore there is not any CGI documentation that exists for review. However, COHBE created documentation to validate the software installed is operational in the environment. First Data reviewed this documentation; it included screen captures from the environment configuration and management tools as well as high-level architecture diagrams documenting the relationship between the individual architecture components. This was the first of many software deliverables specified in the CGI contract. Overall, the documentation provides validation of the installation and configuration of the environment. This is relatively clear since the environment consists of the standard products including WebLogic and Oracle database products. This may not be as clear in the future, because much of the software dropped into the environment will be configured products such as hCentive or custom code developed by CGI. **Recommendation** 1. CGI should make changes to future software deliverables to include: • The DED should reflect that CGI should provide documentation of the configuration and installation. • The software deliverables should specify the software requirements the

Status	No.	Area	Sub-Area	Assessment and Recommendations
				delivered would meet. This will be important for test planning and execution of specific scripts and scenarios.
	4	**Deliverables**	**DEL02 CGI Project Management Plan** *(Due to various documents associated with the Plan, the version is in assessment section.)*	**Assessment** There are several documents contained in this deliverables: A. Change Management Plan (*Version 1.0 Dated August 23, 2012)* The document is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the corresponding Deliverable Expectation Document (DED) however, the specified processes stated in the Change Management Plan is currently not being executed. Reference the Area SDLC- Project Management Area for section specific assessment and recommendations. B. Communication Management Plan (*Version 1.0 Dated August 23, 2012)* The document is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the corresponding Deliverable Expectation Document (DED). C. Critical Dependency Procedure (*Version 1.0 Dated August 24, 2012)* The document is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the corresponding Deliverable Expectation Document (DED). D. Human Resources Management Plan (*Version 1.0 Dated August 24, 2012)* The document is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the

Status	No.	Area	Sub-Area	Assessment and Recommendations
				corresponding Deliverable Expectation Document (DED). E. Issue Management Plan (*Version 1.0 Dated August 23, 2012)* The document is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the corresponding Deliverable Expectation Document (DED). F. Non-Software Work Product Management Plan (*Version 1.0 Dated August 22, 2012)* The document is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the corresponding Deliverable Expectation Document (DED). G. Project Controls and Standard Management Plan (*Version 1.0 Dated August 25, 2012)* The document is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the corresponding Deliverable Expectation Document (DED)) however, the specified processes stated in the Project Controls and Standard Management Plan is currently not being executed. Reference the SDLC- Project Management Area for specific assessment and recommendations. H. Risk Management Plan (*Version 1.0 Dated August 23, 2012)* The document is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the corresponding Deliverable Expectation Document (DED).

Status	No.	Area	Sub-Area	Assessment and Recommendations
				Recommendation First Data does not have any specific recommendations for this deliverable at this time.
	5	**Deliverables**	**DEL03 Detailed Project Schedule**	**Assessment** There is no document per se to review, as the deliverable was a detailed Project Schedule. First Data was unable to access the original Project Schedule in SharePoint that was contractually due August 13, 2012; additionally performing an assessment on an old version would not be valuable. Therefore, First Data has reviewed the latest version. Reference the Project Schedule- CGI Area section for specific assessment and recommendations. **Recommendation** First Data does not have any specific recommendations for this deliverable at this time.
	6	**Deliverables**	**DEL04 Quality Management Plan for Implementation** *(Version 0.12 Dated October 24, 2012)*	**Assessment** The deliverable is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the corresponding Deliverable Expectation Document (DED) however, the specified processes stated in the Quality Management Plan is currently not implemented. Reference the Area SDLC- Project Management Area for specific assessment and recommendations. **Recommendation**

Status	No.	Area	Sub-Area	Assessment and Recommendations
				First Data does not have any specific recommendations for this deliverable at this time.
	7	**Deliverables**	**DEL05 - Requirements Validation Document** *(Version 1.6 Dated October 8, 2012)*	**Assessment** The deliverable is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the corresponding Deliverable Expectation Document (DED). The document and associated spreadsheets and diagrams were internally consistent and congruent with the evaluation criteria specified in the DED. First Data identified the following concerns related to this deliverable: • The COHBE – CGI SOW specifies that the requirements will be loaded into a requirements management tool and cross-referenced to subsequent development artifacts including System components, design artifacts, and test scripts and scenarios. • The relationship of the technical requirements to components of the architecture is not explicit. Most requirements are functional requirements and map directly to Use Cases. There are, however, Miscellaneous Technical Requirements that may apply to most use cases but exclusively to none in particular. It is more appropriate to map the Miscellaneous Technical Requirements to components within the Technical Architecture design. However, there are not technical deliverables for this design within the CGI contract. **Recommendation** First Data does not have any specific recommendations for this deliverable at

Status	No.	Area	Sub-Area	Assessment and Recommendations
				this time. Recommendations related to the DED process and work products beyond the set of formal Deliverables are in the SDLC- Design Area. The recommendations related to the tools used to track and maintain requirements are in SDLC- ALM Tool Area.
	8	**Deliverables**	**DEL06 Dental and Vision- Planning and Analysis Document**	**Assessment** The deliverable is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the corresponding Deliverable Expectation Document (DED). According to the COHBE DED Deliverable Log version 12/18/12 5:40 pm, the contractual due date was 08/24/12. The document was delivered on 10/15/13. **Recommendation** 1. First Data does not have any specific recommendations for deliverable at this time. 2. CGI should update the COHBE DED Deliverable Log to reflect accurate dates for traceability purposes.
	9	**Deliverables**	**DEL07 Security Plan**	**Assessment** According to the COHBE DED Deliverable Log version 12/18/12 5:40pm, this deliverable is late. The contractual due date was 08/31/12. **Recommendation** 1. CGI should perform an analysis to evaluate whether this deliverable affects

Status	No.	Area	Sub-Area	Assessment and Recommendations
				the current work efforts or overall project schedule. 2. CGI should update the COHBE DED Deliverable Log to reflect accurate dates for traceability purposes.
	10	Deliverables	**DEL08 – Software Delivery to Integration Test for Iterations 1-5** (*Version 1.1 Dated September 13, 2012)*	**Assessment** The deliverable is consistent and aligns with the evaluation criteria specified in the COHBE – CGI Statement of Work (SOW) dated June 6, 2012 and the corresponding Deliverable Expectation Document (DED). The document and associated spreadsheets and diagrams were internally consistent and congruent with the evaluation criteria specified in the DED. First Data identified the following concerns related to this deliverable: • The CGI SOW contains a description of the overall SDLC processes and work products and governs the scope and content of this deliverable. The DED identifies many of the components of the SDLC including Test Process, Software Delivery from Unit to Integration Test, specific Unit Test and Integration Test Entrance Conditions. • The CGI SOW identifies DEL 08 but the scope and content requirements not defined. It is difficult to determine what this deliverable should contain without specific descriptions. The definition of iterations is not contained in other project documentation including the Project Schedule beyond the name of the deliverable. This is a particular concern moving forward that Iterations are not defined and do not have a relationship with tasks, releases or functionality from a Use Case perspective. The concern documented in Section 4.1 Risk Log. • The deliverable follows the organization specified in the DED but does

Status	No.	Area	Sub-Area	Assessment and Recommendations
				not appear to document accurately the functionality being delivered as part of this deliverable by naming the Use Cases and requirements that are being met. **Recommendation** 1. CGI should develop a crosswalk between the deliverables for each set of iterations (1-5, 6-10, etc.) and the hCentive releases, Use Cases and Requirements to ensure the completeness of the overall system.
	11	Deliverables	DEL09 Capacity and Performance Plan	**Assessment** According to the COHBE DED Deliverable Log version 12/18/12 5:40pm, this deliverable is late. The contractual due date was 09/21/12. **Recommendation** 1. CGI should perform an analysis to evaluate whether this deliverable affects the current work efforts or overall project schedule. 2. CGI should update the COHBE DED Deliverable Log to reflect accurate dates for traceability purposes.
	12	Deliverables	DEL10 Software Delivery to Integration Test for Iterations 6-10	**Assessment** According to the COHBE DED Deliverable Log version 12/18/12 5:40pm, this deliverable is late. The contractual due date was 10/28/12. **Recommendation** 1. CGI should perform an analysis to evaluate whether this deliverable affects the current work efforts or overall project schedule.

Status	No.	Area	Sub-Area	Assessment and Recommendations
				2. CGI should update the COHBE DED Deliverable Log to reflect accurate dates for auditing purposes.
	13	Deliverables	DEL11 Software Delivery to Integration Test for Iterations 11-15	**Assessment** According to the COHBE DED Deliverable Log version 12/18/12 5:40pm, this deliverable is late. The contractual due date was 12/10/12. **Recommendation** 1. CGI should perform an analysis to evaluate whether this deliverable affects the current work efforts or overall project schedule. 2. CGI should update the COHBE DED Deliverable Log to reflect accurate dates for traceability purposes.
	14	Deliverables	DEL12 Test Plan (System and UAT)	**Assessment** According to the COHBE DED Deliverable Log version 12/18/12 5:40pm, this deliverable is late. The contractual due date was 12/21/12. **Recommendation** 1. CGI should perform an analysis to evaluate whether this deliverable affects the current work efforts or overall project schedule. 2. CGI should update the COHBE DED Deliverable Log to reflect accurate dates for auditing purposes.
	15	Deliverables	DEL13 Training Plan	**Assessment** According to the COHBE DED Deliverable Log version 12/18/12 5:40pm, this

Status	No.	Area	Sub-Area	Assessment and Recommendations
				deliverable is late. The contractual due date was 12/21/12. **Recommendation** 1. CGI should perform an analysis to evaluate whether this deliverable affects the current work efforts or overall project schedule. 2. CGI should update the COHBE DED Deliverable Log to reflect accurate dates for traceability purposes.
	16	Deliverables	DEL14 Software Delivery to System Test	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	17	Deliverables	DEL15 Software Delivery to System Test - Dental and Vision	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	18	Deliverables	DEL16 Performance Test Plan	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	19	Deliverables	DEL17 Interface	**Assessment**

Status	No.	Area	Sub-Area	Assessment and Recommendations
			Specification Document	The Deliverable is due at a future date. **Recommendation** N/A
	20	**Deliverables**	**DEL18 Detailed System Design (DSD)**	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	21	**Deliverables**	**DEL19 Software Delivery to Integration Test for Iterations 16-20**	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	22	**Deliverables**	**DEL20 Software Delivery to Integration Test for Dental and Vision**	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	23	**Deliverables**	**DEL21 Tables and Rules User Guide**	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A

Status	No.	Area	Sub-Area	Assessment and Recommendations
	24	Deliverables	DEL22 Training Materials	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	25	Deliverables	DEL23 Software Delivery to User Acceptance Test	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	26	Deliverables	DEL24 Help Desk / AVR Plan	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	27	Deliverables	DEL 25 Supporting Production Environments Available	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	28	Deliverables	DEL26 System Test Results	**Assessment** The Deliverable is due at a future date. **Recommendation**

Status	No.	Area	Sub-Area	Assessment and Recommendations
				N/A
	29	Deliverables	DEL27 Software Delivery to Pilot Environment - Dental and Vision	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	30	Deliverables	DEL28 Software Delivery to Pilot Environment	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	31	Deliverables	DEL29 Online User Guide	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	32	Deliverables	DEL30 User Acceptance Testing Resolutions Document	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	33	Deliverables	DEL31 Performance Test Execution	**Assessment** The Deliverable is due at a future date. **Recommendation**

Status	No.	Area	Sub-Area	Assessment and Recommendations
				N/A
	34	Deliverables	DEL32 Deployment / Roll-Out Plan	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	35	Deliverables	DEL33 Enterprise Readiness Assessment Report	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	36	Deliverables	DEL34 Business Continuity Plan	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	37	Deliverables	DEL35 Continuity of Operations (COOP)	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	38	Deliverables	DEL36 Quality Management Plan for Operations	**Assessment** The Deliverable is due at a future date. **Recommendation**

Status	No.	Area	Sub-Area	Assessment and Recommendations
				N/A
	39	Deliverables	DEL37 Operating Procedures Guide	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	40	Deliverables	DEL38 System Documentation	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	41	Deliverables	DEL39 Software Delivery to Production Go-Live Environment - Dental and Vision	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	42	Deliverables	DEL40 Software Delivery to Production Go-Live Environment	**Assessment** The Deliverable is due at a future date. **Recommendation** N/A
	43	Functionality	hCentive	**Assessment** hCentive is a critical component of the Exchange System. The hCentive COTS

Status	No.	Area	Sub-Area	Assessment and Recommendations
				product with Colorado specific modifications encompasses the entire online portion of the application which includes: • Account Management • Broker / Navigator • Eligibility • Enrollment • Plan Management • Individual and Employer SHOP The designed utilizes requirements from Use Cases that decompose various business areas. First Data reviewed the Requirements as documented in DEL 05 – Requirements Validation Document and Use Cases for each business area as well as participated in many discussions regarding the design and scope of the system. Several hCentive specific characteristics have a significant impact to the overall system design and may continue to affect the project moving forward. These are: • The project is significantly dependent on the successful completion of the hCentive COTS product and required customizations since this is almost the entire online portion of the Exchange System. • hCentive does not exist as a functioning Exchange System in another state. • hCentive is currently developed as Federal solution as well as to support

Not Produced

Status	No.	Area	Sub-Area	Assessment and Recommendations

				several State Exchange. This is a significant development effort that is not congruent with identifying hCentive as a COTS product. The concern documented in Section 4.1 Risk Log.
				• hCentive' s significant development effort requires a much greater insight than COHBE and CGI currently have or would usually be required for a COTS product. That visibility is not reflected in the Project Schedule. This is further discussed in the Project Schedule- CGI Area.
				• CGI does not conduct reviews of the Detailed Design before delivery of the hCentive releases. This is further documented in the SDLC- Design Area.
				• hCentive releases are not being delivered in deployable modules, e.g. the functionality in each release isn't complete from either an individual user role or group of users perspective. For example, delivering all of the functionality for Broker/Navigators or for Anonymous Shop within the dot release. Therefore, the implementation of hCentive is dependent on the completion of the entire hCentive development effort and required customizations. This:
				  o Decreases the flexibility of the implementation because the only version of the application that could be deployed is the complete one.
				  o Decreases the effectiveness of the testing effort because end-to-end functionality cannot be tested until the last hCentive release and significantly increases the regression testing effort.
				  o Forces the back loading testing effort with the testing of end-to-end functionality near the end of the Testing phase. This concern documented in the Section 4.1 Risk Log.

Status	No.	Area	Sub-Area	Assessment and Recommendations
				o Significant potential defects in the hCentive functionality are not discernible until the last release because the end-to-end functionality is not testable in the earlier releases. This has an even greater potential impact because there is not any slack in the Project Schedule after the testing tasks begin. o Any delays in delivery of hCentive releases are almost certain to be critical path without slack. o hCentive was originally procured as part of the CGI solution. Subsequently, the hCentive product has been separated from the CGI contract and is being licensed directly by COHBE. This concern documented in the Section 4.1 Risk Log. **Recommendation** 1. CGI should revisit the scope of each hCentive release to ensure that each release is logically cohesive in relationship to CGI's implementation strategy and that the release meets the business needs from either an individual user role or group of users. 2. CGI should have a detailed Test Plan that identifies which scripts are to be completed for each release prior to promotion of the release to the testing environment. Additionally, the detailed Test Plan should be reviewed by COHBE and the appropriate interface testing partners prior to promotion. 3. CGI should determine the efficacy of the hCentive solution and ensure that the functionality that is required can be built within the required time frame. This determination should be done as soon as possible to give COHBE the opportunity to pursue alternatives. This concern documented in the Section 4.1 Risk Log.

Work Product

Status	No.	Area	Sub-Area	Assessment and Recommendations
	44	Functionality	Account Management	**Assessment** First Data reviewed the Account Management Requirements as documented in DEL 05 – Requirements Validation Document and Use Cases documented in Share Point in the Deliverables and WIP/Analysis & Design/Use Cases directory as well as participated in team design sessions. Generally, the Requirements and Use Cases are consistent and complete. A focus of the team has been to provide additional clarity around the roles that would be supported by hCentive and the Security Architecture. Currently, it appears that the hCentive application should be able to be changed to support the identified roles within the Account Management Use Cases; specifically, the customers, workers, brokers and navigators. As noted in the SDLC- Design section Area, CGI is currently developing the wireframes and the team will validate that business area after the incorporation of CRs into the Use Cases and completion of the CGI. The wire frames were planned to be completed on January 7, 2013 but they have not yet been completed. There are specific Recommendations as to the need for architecture work products to be identified and tracked to technical requirements that are documented in the SDLC- Design Area. **Recommendation** First Data does not have any specific recommendations for Account Management at this time.
	45	Functionality	Broker / Navigator	**Assessment** First Data reviewed the Broker / Navigator Requirements as documented in DEL 05 – Requirements Validation Document and Use Cases documented in Share

Status	No.	Area	Sub-Area	Assessment and Recommendations
				Point in the Deliverables and WIP/Analysis & Design/Use Cases directory as well as participated in team design sessions. The Broker / Navigator functionality as defined by the current version of the Use Cases is not consistent with the baseline functionality as built within the hCentive application. This is reflected in the following Change Requests related to Broker/Navigator functionality: • CR-24, Changes to BN Requirements for filters instead of searches • CR-25, Changes to Navigator compensation requirements • CR-29, Change to remove Broker to purchase insurance • CR-32&33, Change to accommodate a hierarchy within Navigator entities • CR-61, Broker remote view of customers screen **Recommendation** 1. CGI should develop a contingency plan to accommodate the roles of Brokers and Navigators within the system that would have a lesser degree of impact to hCentive's development efforts relying on a phased implementation of final functionality. 2. COHBE should begin to provide the Broker/Navigator community additional communications regarding CGI's planned phased implementation and the practical need to limit the scope of the project to a ensure successful implementation.

Status	No.	Area	Sub-Area	Assessment and Recommendations

	46	Functionality	Eligibility	**Assessment**
				First Data reviewed the Eligibility Requirements as documented in DEL 05 – Requirements Validation Document and eligibility Use Cases documented in Share Point in the Deliverables and WIP/Analysis & Design/Use Cases directory. The Eligibility Area may need much further analysis to complete the Detailed Design.
				
				• The level of detail that is necessary to describe the potential combinations of flows and outcomes does not exist within the Use Cases. Specifically, it is not clear the flow will accommodate a flow of one individual within the family to one page and another to a different page. This occurs in:
				  o Mixed households where individuals are eligible for a combination of subsidy, Medicaid and employer plans.
				  o Families in the same household or families who consist of individuals claimed on multiple tax returns.
				• In addition to the Use Cases, completion of the Detailed System Design will necessitate the completion of the requirements, design and file layouts of the State Interfaces as well as work with the OIT vendor to explore all possible outcomes of the eligibility transactions.
				• The analysis required to determine exactly what data the eligibility transaction will return cannot begin until a contract is in place between OIT / HCPF and Deloitte. This concern documented in the Section 4.1 Risk Log.
				First Data is unable to determine the efficacy of the Eligibility solution solely based on the work products and deliverables that have been produced by the

Status	No.	Area	Sub-Area	Assessment and Recommendations
				project to date. **Recommendation** 1. CGI should include the necessary level of detail for all possible combinations of eligibility results in the Detailed Design as described above. 2. Detailed System Design for the State Interfaces should start as soon as possible. This concern documented in the Section 4.1 Risk Log. 3. A contract and MOU should be completed as soon as possible. This has further impact and is documented in the Functionality, Eligibility and SDLC, Design Areas. The work on this interface is necessary to confirm their current design of the application and should begin even if the requirements are not robust or not completely defined. An initial work order should be established as part of the OIT contract and MOU to allocate OIT and HCPF vendor resources to assist in the analysis and refine the scope of the effort.
	47	Functionality	Enrollment	**Assessment** First Data reviewed the Enrollment Requirements documented in DEL 05 – Requirements Validation Document and Use Cases documented in Share Point in the Deliverables and WIP/Analysis & Design/Use Cases directory. Generally, the Requirements and Use Cases are consistent and complete. **Recommendation** First Data does not have any specific recommendations for Enrollment at this time.

Status	No.	Area	Sub-Area	Assessment and Recommendations
	48	Functionality	Plan Management	**Assessment** First Data reviewed the Plan Management Requirements documented in DEL 05 – Requirements Validation Document and Use Cases documented in Share Point in the Deliverables and WIP/Analysis & Design/Use Cases directory. Generally, the Requirements and Use Cases are consistent and complete. **Recommendation** 1. First Data does not have any specific recommendations for Plan Management at this time.
	49	Functionality	Individual and Employer SHOP	**Assessment** First Data reviewed the Individual and Employer SHOP Requirements documented in DEL 05 – Requirements Validation Document and Use Cases documented in Share Point in the Deliverables and WIP/Analysis & Design/Use Cases directory. Generally, the Requirements and Use Cases are consistent and complete. **Recommendation** 1. First Data does not have any specific recommendations for Employer SHOP at this time.
	50	Interfaces	State	**Assessment** First Data reviewed the Health Care Policy and Financing (HCPF) interface high-level business requirements (HLBR) sent 121912. Generally, the requirements are consistent and complete. HCPF has approved the HLBRs and have started

Status	No.	Area	Sub-Area	Assessment and Recommendations
				on development of the Order of Magnitude (OOM). There are current discussions as to whether the Eligibility Rules Engine will be part of the work effort. Once a decision has been made, the Business Requirements Design (BRD), the level of work effort (LOE) and the Work Plan will be the next steps. Due to the timelines, CGI has started development of the interface without having the full details of the interface design, which adds additional risk. Moving forward with development of the interface without HFCF's detail design could lead to potential re-work. Additionally, there are several factors that impedes the development of the interface and Eligibility Rules Engine: • HCPF currently lacks resources. • A contract currently does not exist with OIT and COHBE; procurement currently in progress. • A HCPF Work Plan has not been developed. • The key milestones and inter-dependencies are not been defined. COHBE is solely dependent on CGI and HCPF to build the interface. Additional assessments related to the State Interfaces are documented in the Functional-Eligibility and SDLC Area. **Recommendation** 1. Develop timeline to ensure common understanding amongst Stakeholders. (Reference recommendation #10 in Project Schedule- CGI Area) 2. Develop a Contingency Plan in the event CGI and OIT are unable to complete the interface. 3. Assist HCPF by lending additional resources. 4. Provide an interim work order for allotted number of hours so Deloitte may engage due to the compressed timeframe.

Status	No.	Area	Sub-Area	Assessment and Recommendations
	51	Interfaces	Carrier	First Data reviewed the Carrier Interface Requirements documented in DEL 05 – Requirements Validation Document and Use Cases documented in Share Point, Deliverables and WIP/Analysis & Design/Use Cases. Generally, the Requirements and Use Cases are consistent and complete. The current Carrier interface design is based on industry standard transaction sets that are well supported within the Vendor community. Additionally, the involvement and participation of multiple individual Carriers has been consistent and participatory the Carrier Advisory Group. There are two alternative methods for the development of the Carrier Interfaces that CGI is currently evaluating: • Purchase a COTS translator from Oracle • Manually code the entire interface The specific COTS translator for the standards that CGI has evaluated is an Oracle translator. The Oracle translator is well supported by the architecture but has been described as 'pricey' by CGI and includes support for a large number of standard transactions that are not required by the application. Manually coding the entire interface would consume additional coding resources but would only support the standard transactions that are needed. Support for this custom coded interface is not expected to be significant because the standards do not change frequently and backward compatibility is usually assured.

Status	No.	Area	Sub-Area	Assessment and Recommendations
				Recommendation 1. CGI should purchase the Oracle X12 translator to expedite development and minimize impact on skilled resources. The same resources that would be utilized to code the translation of a few X12 transactions would be better spent developing the parts of the system that are truly custom and cannot be purchased. Additionally, any changes to the standards would be covered by the maintenance agreement for the COTS product.
	52	Security	N/A	**Assessment** There are three interrelated areas that, in aggregate, ensure the security of the COHBE application. These are: • Account Management • DEL 07, Security Plan • Architecture Design First Data reviewed the draft Security Requirements, DEL 07, Security Plan, the system architecture design from the CGI Proposal, as well as the application use cases that implement the security components in the online environment. Additionally, First Data reviewed two security related Issues (#20 and #25). Generally, the security of the designed system should meet the system requirements. Additional Security related Assessments and Recommendations are documented in the Functionality, Account Management Area. **Recommendation** First Data does not have any specific recommendations for Security at this

Status	No.	Area	Sub-Area	Assessment and Recommendations
				time.
	53	**Service Center and Back Office**	**Service Center**	**Assessment** COHBE is currently in the process of securing a vendor to develop and implement the Contact Center Solution. Once the vendor is established, a more detailed assessment can occur. Additionally, COHBE is in the process of selecting the Contact Center site. With the given timeframe, there is a risk the Service Center will not be ready by the October Go-Live date. The concern documented in Section 4.1 Risk Log. **Recommendation** 1. In the interim, COHBE should start to: • Identify the Technology Platform of the Stakeholders • Determine a Service Center Model o Identify types of interaction expected to receive; and start discussions with Stakeholders as how this will mechanically work • Identify and document Agent Call Flows • Identify and document Operational Processes and Metrics • Identify the need at a minimum to operate in October 2013. Develop a plan for the remaining work effort. 2. Develop a Contingency Plan if the Service Center is not available. 3. First Data has reviewed the proposed Business Requirements and Technical Architecture v1.0 dated 11/14/12 and has provided the following comments: Section 1 Document Purpose: Add the following information- • Hardware Requirements and Software Requirements • Network:

Status	No.	Area	Sub-Area	Assessment and Recommendations
				○ Network configuration (e.g. Number of DS-3 lines for data connectivity for CTI requirements, services used for backup network service, etc.) • The T-1 PRI lines required based on number of Agents and estimated Interactive Voice Response (IVR) usage. What will be deployed to provide uninterrupted power supply to the network equipment (e.g. UPS System) • Toll Free rate; describing the total volume of toll free minutes used by the Service Center each month based on estimation. Section 4 Project Overview: Include Change Management, Business Processes, Operating Procedures, and Performance Management Metric requirements. Section 4- 4.1 Project Overview and Background: Part of the deliverables should include a detailed Project Schedule. Section 4- 4.1.1 Business Process Documentation: Recommend deliverable to include- • Project Schedule • Requirements- ○ IVR Menuing – Configuration and deployment of COHBE specific menu and provide the appropriate transfer logic to agents. ○ Call Routing – Configuration and deployment of routing logic and agent skill-group with appropriate queuing and messaging. ○ Web Interaction Routing – Configuration and deployment of Web Chat routing to agents.

Status	No.	Area	Sub-Area	Assessment and Recommendations
				o Reporting – Deploy the reporting platform to create and generate reports. o Quality Monitoring – Configuration and deployment of call and screen recording, search, retrieval, and performance management software. (Not sure if COHBE plans to incorporate this component.) o Computer Telephony Integration (CTI) – Deploy CTI softphone and transfer logic to agent desktops to support telephony. o Workforce Management – The configuration and deployment of agent scheduling and staffing application. o Telephony – The configuration and deployment of telephony and voice messaging. • High Level Design Description (e.g. Solution To Be) • Training Approach • Testing Approach • Deployment Approach • Implementation Approach Section 5 Business Requirements: Include the following components: Reports, Quality Management and Workforce Management. Section 5 Business Requirements 5.2.7.6 Callback Functionality: Depending upon the number of Agents that will staffed at the Service Center; this could be a great feature of either a potential issue. If not staffed accordingly, the opportunity for the callback might not work as planned. Suggest implementing Call Back post-implementation once the Call Center stabilizes and metrics

Status	No.	Area	Sub-Area	Assessment and Recommendations
				extracted to determine capacity. Section 5 Business Requirements 5.27 Description: Include Administrator Rights role to allow routing modification based on business needs. Section 5 Business Requirements 5.2 IVR Scripts: My assumption is there will be detail discussion of IVR menu and this is just a depiction of a suggested model. Section 5.4 Eligibility Determination 5.4.7 Description: More information needed to determine impacts. Add option to enter information directly into COHBE website to avoid information passed from RightNOW to COHBE Website.
	54	**Service Center and Back Office**	**Back Office**	**Assessment** First Data reviewed the Back Office Requirements documented in DEL 05 – Requirements Validation Document and Use Cases documented in Share Point, Deliverables and WIP/Analysis & Design/Use Cases. Generally, the Requirements and Use Cases are consistent and complete. The volumes of manual activities pushed to the Back Office due to the deferral of technology functionality. It is unclear how much this will grow and how this affects the original scope of the contract. Additionally, there is a lack of clarity as to when the technology will be implemented post-implementation. **Recommendation** 1. Document the newly identified manual activities. Cross-reference these activities to the original contract. Determine the cost associated with the newly identified activities against the deferral of the technology components.

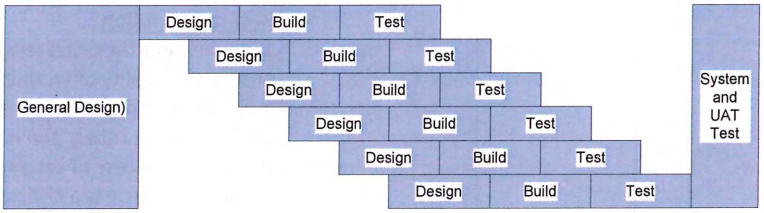
Status	No.	Area	Sub-Area	Assessment and Recommendations
				2. Identify and document the software release for the deferred technology items.
	55	Training	N/A	**Assessment** Training has not yet commenced. **Recommendation** First Data does not have any specific recommendations for Training at this time.
	56	SDLC	Project Management	**Assessment** The Change Management processes are not executed as follows: Page 13 Section 2.3.6 Conduct Impact Analysis states Change Request with CR Priority of Urgent should have an Impact Analysis within 5 business days and a CR Priority of High should have an Impact Analysis within 10 business days, though there are numerous requests that have not followed the process as stated. Some examples are: • CR ID 36 SHOP must handle employees eligible for COBRA coverage: The CR Priority of High and was open 11/8/12 but does not have an Impact Analysis Due Date or Impact Analysis; per the process, this should have an impact analysis within 10 business days. • CR ID 16 Clarification of APTC CSR segregation requirements: The CR Priority of High and was open 10/4/12 but had an Impact Analysis Due Date of 10/24/12; per the process this should have an impact analysis within five business days.

Status	No.	Area	Sub-Area	Assessment and Recommendations
				The Issue Management processes are not executed as follows: Page 13 Section 2.3.3 Continuous Issue Response Monitoring and Control states the Issues monitored to ensure they are resolved in a timely manner to reduce potential negative impacts to the project or operational activity. However, the specified processes stated in the Issue Management Plan currently not implemented. Some examples are: • Issue ID 18 Incremental Development is Behind: The Issue has a Severity of Major and opened 10/9/12 but is still open and lacks an Action Plan and Next Resolution Due Date. • Issue ID 35 OIT Gateway Interfaces: The Issue has a Severity of Critical and opened 12/9/12 but is still open and lacks an Action Plan and Next Resolution Due Date. • Issue ID 40 ELG-004 Apply for Exemption at risk for affecting development: The Issue has a Severity of Critical and opened 12/17/12 but is still open and lacks an Action Plan and Next Resolution Due Date. The Project Controls and Standard Management processes are not executed as follows: Page 8-10 states various reports will be created on a weekly basis to monitor and measure the project but no such documents exists: • Schedule Quality Report measures the number of tasks without resources, tasks without successor(s), tasks that are scheduled in the past, and tasks that show work in the future but there is no such document. • Schedule Slippage Report Tasks reflects total tasks with slack of five

Status	No.	Area	Sub-Area	Assessment and Recommendations
				days or less that have been delayed from week-over-week. These tasks are at risk of affecting the critical path if slippages continue and therefore need close monitoring. • Critical Path Report reflects all tasks that have zero days or less of total slack. If tasks with less than 0 days of total slack are encountered, corrective action should be taken to resolve the negative slack condition to keep the task from pushing project completion milestones or deliverable deadlines. • Resource Allocation Report reflects resource allocation as a percentage of a Full Time Equivalent (FTE) Employee. The target range for allocation is between 80% and 120% of an FTE. • Baseline Variance Report reflects active tasks that are currently scheduled later than their baseline finish are presented. This gives management the option of rescheduling the tasks, re-bases lining, or if there are no major impacts, accepting the variance. The Risk Management Plan processes are not executed as follows: Page 15 Section 2.3.3.2 Develop Risk Action Plan states an Action Plan is required for every Action Type though some Risk do not have an Action Plan. • Risk ID 29 Timeliness of CMS and CCIIO Requirements Definition: Has a Risk Probability of Near Certainty and Risk Severity of Critical but it lacks a detailed dates to the Action Plan. • Risk ID 5 COHBE Resource Availability: Has a Risk Probability of Likely and Risk Severity of Major but it lacks a detailed dates to the Action Plan.

Status	No.	Area	Sub-Area	Assessment and Recommendations
				Page 16 Section 2.3.3.3 Develop Contingency Plan states a Contingency Plan should be developed for risks that are classified as high-probability and/or high-severity though Risks that have been identified, as 'high-probability and/or high-severity' do not have a Contingency Plan. • Risk ID 26 Release Deployment: Has a Risk Probability of Highly Likely and Risk Severity of Critical but it lacks a Contingency Plan. • Risk ID 22 Potential Gaps between hCentive App and COBHE Requirements: Has a Risk Probability of Near Certainty and Risk Severity of Critical but it lacks a Contingency Plan. The Quality Review processes are not executed as follows: Page 9 states Quality Reviews will be performed as follows but no such documents exists in SharePoint: **Frequency** / **Description** / **Tool** / **Output** Monthly / Conduct quality reviews. / SharePoint / Deliverable Audit Log Monthly / Review deliverables against the applicable work product standards. / SharePoint / Process Verification Log Every Other Month / Evaluate progress toward satisfying the project success factors. / SharePoint / Success Factor Log Page 10 states Continuous Process Improvement will be performed as follows but no such documents exists in CGI Enterprise Tools:

Status	No.	Area	Sub-Area	Assessment and Recommendations
				Frequency Periodic **Description** Monthly Health Checks/CPMF Findings & Action Plan **Tool** CGI Enterprise Tools **Output** Monthly Health Checks/CPMF Findings & Action Plan According to the Communication Management Plan, the following meetings should be established but they do not exists: • hCentive Project Management Status Meeting Weekly meetings • hCentive Cross-State Focus Group Monthly meetings • Healthation Executive Oversight Meeting-Project Level Monthly meetings **Recommendation** 1. Implement the processes as stated in the Project Management Plan(s) to ensure the quality of work effort is as expected. The lack of measuring and monitoring Tasks, and Critical Dependency, Issue and Risk could influence the ability to make timely and informed decisions and have an adverse effect on the overall success of the project. 2. Since hCentive is a critical component of the Exchange, COHBE Project should attend if the hCentive meetings referenced above if they do not already.
	57	SDLC	Design	**Assessment** First Data reviewed the design of the Exchange System including the Use Cases documented in Share Point, Deliverables and WIP/Analysis & Design/Use Cases, Wireframes and Storyboards. There are a number of interrelated issues with

Status	No.	Area	Sub-Area	Assessment and Recommendations
				the scope, content and organization of these items as they relate to a standard iterative or incremental development methodology. A standard interactive or incremental development methodology would determine the scope of the overall system as part of a general design like a waterfall methodology based project. Analysis would be conducted during this effort to identify individual components whose design, code and test could be completed discretely. The remainder of the tasks would be to complete the design, code and test of each of the identified components. Each of the components would be reviewed on a flow basis as the design, build and test was completed. This is represented in the following graphic. **Incremental Approach**  There are some notable differences in CGI's approach to Design versus the Standard Incremental approach. These are: • General Design o The general system design was partially documented in Use

Status	No.	Area	Sub-Area	Assessment and Recommendations
				Cases but the Use Cases do not contain the level of detail to document how the system will work. To supplement the Use Cases, a set of wireframes were created by COHBE staff. The COBHE Wireframes are not consistent with way the baseline hCentive application has been built. o CGI has developed their own wireframes that are consistent with the hCentive application created as part of the development of the Functional Specifications and Detailed Design for each Functional release. A contingency plan should be developed either if an agreement on the CR's cannot be reached or if the hCentive solution does not meet requirements. o The Wireframes and Storyboards will not be completed for each Use Case but selectively developed focusing only on the Use Cases where COHBE desires a deeper understanding of how the system will be built. o The Functional Design is not a formal deliverable defined in the CGI contract but the wireframes are part of the General Design of the Exchange. The wireframes are not reviewed and approved by COHBE prior to beginning Detailed Design. o The list of incremental components was not based upon a single methodology and consistently applied. For example, some of the increments are hCentive Release based while others like Security cross multiple releases. o Not all requirements have been mapped to the Use Cases, Wireframes and Storyboards. For example, the Miscellaneous Technical requirements for Security should be mapped to all Use

Status	No.	Area	Sub-Area	Assessment and Recommendations
				Cases but are not mapped to any. o Not having clear requirement traceability makes it very difficult to ensure the overall completeness of the system. This is further documented in the SDLC- Tools Area. • Design, Build, Test o As documented in the Schedule, CGI Area, the Project Schedule is organized by hCentive release; R0.2, R0.3 and R0.4. However, the hCentive Releases are not planned to completely implement a given Use Case nor a specific part of predefined incremental components. o There are not interim reviews and approvals of the components of the Detailed Design scheduled prior to development work. o The collections of work products that will constitute the Detailed Design have are being defined even though development work has already begun for some components. o Common language to refer to a unit of work that will be completed, measured and tracked using the iterative methodology has not been agreed to. For example, the documentation the relationship between Functional Design, Wireframes, Storyboards and Detailed Design partially overlaps and is unclear. **Recommendation** 1. CGI should develop a mitigation plan to complete the wireframes for all Use Cases without affecting the overall project. 2. The Functional Design and Detailed System Design should be documented

Status	No.	Area	Sub-Area	Assessment and Recommendations
				and include the Wire Frames and Workflow documentation that are part of a package that can be coded. This directly relates to the need for the completion of the DEL 18 – Detailed System Design DED as documented in the Project Schedule Area. The concern is documented in Section 4.2 Issue Log. 3. CGI should: • Define a standard methodology for decomposing the system into discrete components that can be developed, measured and tracked consistently. This recommendation directly relates to the organization of the CGI Project Schedule. Related information is documented in the Project Schedule- CGI Area. • Clearly define the work products that will document the design of the system. • Identify and develop additional technical specifications beyond the deliverables where miscellaneous technical requirements will be met. • Use ALM to map requirements to these technical work products including technical deliverables, designs documents and architecture components just as functional requirements are mapped to Use Cases.
	58	SDLC	Data Model	**Assessment** First Data reviewed the draft CGI Logical Data Model (LDM) provided by CGI on 010813. Additionally, First Data participated in a walkthrough of the LDM with COHBE and CGI staff. The LDM is in process and a complete LDM has not yet been created. The methodology for developing the LDM is consistent with the standard application development processes for systems with significant COTS components. The methodology generally consists of identifying the

Draft

Status	No.	Area	Sub-Area	Assessment and Recommendations
				information that requirement to support the COTS products and identifying the information that is received from and sent by various interfaces. This methodology applied to the hCentive and Healthation COTS products and will be applied to the OIT interfaces with particular emphasis on the data requirements of the Business Rules Engine. The analysis of the data requirements to support the OIT interfaces cannot begin until a contract and MOU are in place with OIT, CMS and Deloitte. **Recommendation** 1. COHBE should obtain the data model used by the Corticon Business Rules Engine. 2. CGI should work with Deloitte and hCentive to coordinate the detailed data requirements for hCentive based upon the data sent and received to the OIT Gateway and the Eligibility transactions.
	59	SDLC	Architecture	**Assessment** First Data reviewed the HLRD _COHBE-HIX_v0-11 (Architecture Document) and the COHBE Solution Overview 8-20-12. Additionally, First Data participated in walkthroughs of the Development Architecture. The Development and Integration Environment Application Configuration is incomplete and late. This is documented and more fully described in SDLC-Build Area. Overall the Architecture Document is incomplete. The outline structure is a good beginning but the document could not be used to build the environments. First Data requested additional clarification and information that would describe the Architecture but was unable to obtain this information prior to the completion of this review:

Status	No.	Area	Sub-Area	Assessment and Recommendations

				• The virtual machine configuration for some environments including:
				  o Staging
				  o Production
				  o Training
				• A diagram depicting the use of VLANS to connect the tiers of the system
				• A diagram depicting the integration of identified network that are identified in Section 3.7.1
				• Sizing for all WAN connections are identified in Section 3.7.2 and 3.7.3.
				• Monitoring for all other servers and network equipment beyond what it documented in Section 4.2 First Data was not able to determine if this section was complete without understanding the exact production configuration of servers and network equipment and connections.
				• The backup requirements are identified but they only describe the application and database servers. It is not clear if these backup requirements apply to all of the other servers identified in the document.
				• A design of the production architecture that includes the physical network, physical servers and virtual servers. This design will be used to predict the performance of the overall solution as well as to ensure that the test environments are being built parallel to production.
				
				Recommendation
				1. CGI should create detailed design of the production and development architecture that: Identifies specific instances of virtual servers including CPU's (speed and type), memory; identifies software stack for each server; identifies data center management servers and software stack.

Status	No.	Area	Sub-Area	Assessment and Recommendations
	60	SDLC	Build	**Assessment** First Data reviewed the draft contents of the Build Package for hCentive Release 0.2, which is an incomplete draft of DEL 10 Software Delivery to Integration Test for Iterations 6-10, as well as met with CGI to discuss the development processes. First Data requested but did not receive the coding standards that CGI utilizes in their code reviews however detailed records of the application of those standards for the each component of the build was received. The Development and Integration Environment Application Configuration is incomplete and late because the installation and setup of Healthation has not yet been completed (WBS 10.2.2 in the Project Schedule). The incomplete build out of the environments was also the subject of Project Issue #29 which has been closed. The absence of the installation and configuration of the Healthation COTS product does not currently impact testing because the functionality isn't required as part of the current build process. This will become a problem when that functionality is scheduled for testing in March, 2013. DEL 10 Software Delivery to Integration Test for Iterations 6-10 deliverable contains: • A summary of the release • Release notes • A list of code reviews conducted signed by team lead • Unit Test Checklist • hCentive information release notes

Status	No.	Area	Sub-Area	Assessment and Recommendations
				The draft DEL 10 information that was reviewed was generally reflective of the expected content for the build but incomplete due to the draft version of the deliverable. First Data identified a few issues with the deliverable. These are: • The scope of the deliverable in relationship to the specific functionality was difficult to assess because it did not completely implement some of the use cases. For example, the Use Case for AM001 identifies eight (8) Requirements that would be met by the functionality described but the AM001 documents included with the Build only reference three (3) of them. • The deliverable did not describe the results of the implementation tests which include testing with the Jenkins tool that ensures a clean build. • The deliverable didn't define the scope of this software delivery in relationship to the other Delivery to Integration Test deliverables. This made it difficult to determine the completeness of the release. **Recommendation** 1. CGI should create define all of the Delivery to Integration Test deliverables within the context of the scope of the overall system to ensure complete coverage of all required functionality.
◐	61	SDLC	Test	**Assessment** First Data reviewed the high level CGI Test Plan. Detailed Test Plans are scheduled to be developed beginning in January 2013. First Data reviewed all of the Testing documentation recorded in the ALM tool for to date. The documentation contained in the ALM tool is incomplete as follows:

Status	No.	Area	Sub-Area	Assessment and Recommendations
				• Only contains the relationships between the Requirements, Use Cases and Test Scripts for Release 0.2. • Does not contain all of the defects that have been identified by the testing team. • Does not contain the necessary cross-referenced identification of defects to demonstrate the necessary integration with the JIRA Configuration Management software. **Recommendation** 1. CGI should load the relationships between all Requirements and all Use Cases into the ALM tool. 2. CGI should create the remaining Test Scripts for Release 0.3 and 0.4. 3. CGI should map the requirements to the Test Scripts and Test Conditions for the subsequent releases to ensure that all requirements are planned for completion with the final release.
	62	SDLC	Deployment and Implementation	**Assessment** The majority of deployment tasks and activities have been completed on the project with the exception of the Software Delivery to Integration Test for Iterations 1-5. First Data's review of deliverable is documented in Deliverables, DEL08 – Software Delivery to Integration Test for Iterations 1-5 Area. First Data also reviewed the draft of DEL10- Software Delivery to Integration Test for Iterations 6-10. This reviewed included the Build Notes and other functionality documentation. The following was also identified:

Status	No.	Area	Sub-Area	Assessment and Recommendations
				• The lack of definition of the staging environment and development processes in the available technical architecture documents make it difficult to determine if all of the Miscellaneous Technical Requirements are being met. For example: o The definition of the above build testing and promotion processes should be contained in the summary document that was not yet complete. o The Build package did not describe any differences between what was planned to be deployed and what was deployed. o The Build package did not describe the scope of future releases. This would be helpful in fully understanding the context of the promotion of this set of functionality. **Recommendation** First Data does not have any specific recommendations for Deployment at this time.
	63	SDLC	ALM Tool	**Assessment** First Data reviewed the implementation of the ALMComplete software implementation for the Colorado Exchange Project. This includes two walkthroughs of the software with CGI as well as reviewing the information that is stored in the tool. This First Data review Area includes information about the capabilities of the tool. Frist Data's review of the use of the ALM tool is documented in the SDLC, Build and SDLC, Test Areas. The following issues have been identified with the ALM tool:

Status	No.	Area	Sub-Area	Assessment and Recommendations
				• COHBE Staff currently do not have access to ALM and use spreadsheets to track and maintain requirements. • CGI has not yet completed a design of the development environment that includes all of the tools that are used including ALM and JIRA. First Data requested that this design be provided but had not received it prior to this Assessment. First Data recognizes that this documentation is not a formal deliverable but had to have been created as part of building out an environment this complex. First Data has identified an issue that these design documents are not available. • The ALM tool does not appear to have the required interfaces to the JIRA tool for defect track. This is identified in the Defect Tracking area of the tool where each ALM defect does not have a corresponding JIRA defect identification number. **Recommendation** 1. CGI should give COHBE staff access to ALM to ensure that there is one place for the tracking of all requirements and to ensure that the subsequent requirements traceability can be performed. 2. CGI should complete the design of the development environment including the ALM tool. 3. CGI should complete the integration of the tools in the development environment specifically the interface between ALM and JIRA.
	64	SDLC	Change Request (CR) and Tool	**Assessment** CGI is currently using SharePoint as the Change Request (CR) Tool. SharePoint is a good tool for collaboration on a project to share and manage information

Status	No.	Area	Sub-Area	Assessment and Recommendations
				and documents but SharePoint is not an automated tool to track and manage CRs. To manage scope effectively, it is important to timely act upon the Change Request. The CR Tool lacks the capabilities to: • Generate reports on a summary or detail level. • Capture and report key information such as Team Responsible, Tester, Release, Programs Impacted, Report Impacted, Regulation Reference, Regulation Effective Date, Defect Reference, Project Phase, Level of Effort (LOE) and LOE by Teams and Person. • Efficiently monitor the CR. There is inconsistency in tracking and the documentation of the CRs. Below are some examples: • CR 18 Roadmap Requirements #1: Has CR Status of Deferred and CR Priority of Urgent but there is lack of information on who approved the CR, Impact Analysis, Identification if Risks or Issues and next steps. • CR 2 Roadmap Requirements #2: Has CR Status of Deferred and CR Priority of Urgent but there is lack of information on who approved the CR, Impact Analysis, Identification if Risks or Issues and next steps. • CR 4 Dental and Vision Scope: Has a CR Status of Approved for Implementation but there lack of information on who approved the CR, LOE, the next steps, release, business driver, acceptance criteria and related. There is no indication of next steps. The CR has an Impact Analysis Due Date of 10/24/12 but there is no Impact Analysis documented. Prior to approval, there should be documentation of key information to ensure shared understanding. • CR 39 Carrier Appeal Process: Has a CR Status of Approved for

Status	No.	Area	Sub-Area	Assessment and Recommendations
				Implementation but there is a lack of information on who approved the CR, LOE, the next steps, release, acceptance criteria and attachments. CR states 'Need agreed-upon LOE to build into Change Order. See meeting minutes from Cameron.' There is a lack of the next steps on obtaining LOE and the minutes not attached. Prior to approval, there should be documentation of key information to ensure shared understanding. There are 83 open Change Request (CR); it is unclear how these affect the overall project schedule. **Recommendation** 1. For the size of the COHBE project, a more robust tool is required to easily manage and track the CRs through the life cycle for traceability purpose. Implement an automated CR Tool to track Change Request. In addition, having a robust tool will be helpful during the Maintenance and Operation phase as CRs and defects will most likely persist. 2. CR should have a page mock-up when applicable as part of the review process to ensure common understanding. 3. CGI should track and cross-reference the CRs to the Use Cases and Requirements. The tracking can occur either in the ALM Tool or by integrating ALM with a change management tool. 4. Assess the CRs in a timely manner as these might have an impact on the overall project schedule.

Status	No.	Area	Sub-Area	Assessment and Recommendations
	65	Organization Resources	CGI	**Assessment** First Data reviewed a detailed CGI organization chart and compared the resources with the tasks in the Project Schedule. Many resources are only allocated to the project on a percentage basis. There are also numerous problems with the Project Schedule as documented above but the number of late tasks clearly indicate that there are not sufficent resources. CGI resources are stretched very thin and this could impact the quality of the work products. CGI has recently made some staffing changes. These are: • Moved existing resource to Deputy PM • Added a new Implementation Manager • Added 2 PMO resources • Added 10 developers • Added a new full-time BI/DW Architect **Recommendation** 1. CGI should allocate additional resources immediately to complete the replaning effort since it is still unclear whether the existing and newly added resources will be sufficent. 2. CGI should identify candidates for all project teams that have the requisite skill set and availability for immediate assignment to the project after the replanning effort has been completed. 3. CGI should add additional resources to PMO, as there are mulitple efforts occuring: re-structuring of the Project Schedule and maintaining and monitoring the Project Schedule. 4. CGI should perform a gap analysis of resources against the remaining work effort and determine the resources

Status	No.	Area	Sub-Area	Assessment and Recommendations
				required.
	66	**Organization Resources**	**COHBE**	**<u>Assessment</u>** COHBE currently has a total of 30 Staff and is currently in the process of hiring the following additional Staff members: • Implementation Manager • Two additional BA resources • Project Manager (on the operations side) to maintain and manage COHBE's project plan and its integration with CGI's plan • Customer Service Manager • Testing Lead For the size of the project, COHBE has been able to take on an enormous amount of work with the existing resources. However, COHBE resources are stretched very thin; there are few individuals that cover multiple areas. The PMO area in particular is deficient. This area requires oversight of the CGI Project Schedule, Deliverables, Change Requests Log, Contracts, Risk Log and Issue Log. Lack of oversight could lead to collateral damage downstream. Particularly for this Exchange Project, as CGI lack integration management and lacks a consistent methodology that is applied to the project. As the project moves towards the Testing and Implementation Phase, this will most likely require additional resources to support the Project. **<u>Recommendation</u>** 1. Add additional resources to the PMO Team. 2. Implement an organization structure that parallels with CGI hierarchical structure:

Status	No.	Area	Sub-Area	Assessment and Recommendations

				• PM
				  o Deputy PM
				  ▪ Quality Manger
				  ▪ PMO Lead
				  o Solution Architect
				  o Implementation
				  ▪ Functional Manager
				  ▪ Testing Manager
				  ▪ Development Manager
				  ▪ Technical
				  o Policy SME/Operations Manger
				  ▪ Back Office Lead
				  ▪ Training Lead
				  ▪ Privacy Compliance Manager
				  ▪ Service Center PM
				2. Have more onsite physical presence at CGI to gain more insight to the development of the Exchange System.

	67	**Software Agreements**		**Assessment** There are a number of Software agreements that are or will be part of the overall Exchange System. The contract with CGI has been executed and the contract with hCentive is in process. Future contracts will be signed for an accounting system and with Oracle for RightNow. Generally, each of the license agreements is consistent with the standard license agreements that each vendor uses with each of their customers. **Recommendation**

Status	No.	Area	Sub-Area	Assessment and Recommendations
				1. COHBE should complete the remainder of these contracts and license agreements as soon as possible since the products have already been selected and are being incorporated into the solution.
	68	Miscellaneous	PMO Meeting	**Assessment** *(Based on meeting held on December 19, 2012.)* There is no visibility as to the state of the overall project schedule. The Scorecards are missing some key information and/or either inconsistent with the Project Schedule (version 12/11/12 6:15pm). Below are a few examples: • OVERALL STATUS section: It is unclear whether the Overall Status measures against Go-Live or whether it measures against the Project Schedule. • FUNCTIONAL TEAM SCORECARD: It is unclear how the overall status is in yellow when according to the Work Plan the following tasks are late: a. Account Manager b. Broker Navigator c. Determine Eligibility d. Development for Enrollment e. Development for Plan Management f. SHOP for Individual Plan g. SHOP for Employer Plan • BACKOFFICE SCORECARD: It is unclear how the overall status is green when according to the Work Plan there are late tasks. In addition, the 'Upcoming Activities' and milestones states 'Establish a weekly review of risks and concerns with COHBE Back Office Analyst' but a risk has not

Status	No.	Area	Sub-Area	Assessment and Recommendations
				been logged for Back Office. • SOA SCORECARD: The SCORECARD did not reflect DEL11 as a late deliverable. It is unclear whether the 'In Progress Deliverables and Work Products' section references the formal Deliverables. CGI has mentioned they were working on revising the COHBE DED Deliverable Log; but did not provide a specific date. • hCentive SCORECARD: There is confusion as to which is baseline versus customization and hCentive's scope of work versus CGI's. The Project Schedule does not reflect the detail level of work effort. There was a discussion amongst the Stakeholders and a list was developed. **Recommendation** 1. Discuss the Project Schedule at the PMO Meetings to provide transparency. 2. The SCORECARDS should align with the Project Schedule. 3. CGI should provide clarity on the definition of 'OVERALL STATUS' and discuss with COHBE as to which would add more value to the group. It is important to have clarity on the SCORECARD as this could have different implications. (CGI was also unsure of the intent of the overall status.) 3. CGI should review the entire SCORECARD against the Project Schedule and provide/document the overall impact to the project schedule within the SCORECARD for transparency. Other SCORECARDS do not align with the Project Schedule. 4. CGI should log the Risk(s) in the Risk Log. 5. CGI should log the Issue(s) in the Issue Log. 6. CGI should add a Risk section to the Scorecards. 7. CGI should include all relevant Deliverables and update the Deliverable Log.

Status	No.	Area	Sub-Area	Assessment and Recommendations
	69	Miscellaneous	**Issue Log** *(Extracted 121912 10:30am)*	**Assessment** It is imperative to monitor the Issues closely to ensure identified Issues are resolved in a timely manner to reduce potentially negative impacts to the project. There is a lack of monitoring the Issue Log. There are several Critical and Major Issues logged but yet some of the Issues have no Action Plan nor does it provide a detail progress of the issue. Below are some examples: • Issue 18 Incremental Development is Behind Schedule: Has an Issue Severity of Major and has a past due Resolution Due Date of 12/6/12 but the next steps not documented nor does it state the overall impact to the Project Schedule. The Issue was last modified 12/13 2:44pm but the Resolution Plan was not updated. • Issue 22 Need to determine and revise schedule for Final Go Live scope: Has an Issue Severity of Major and a past due Resolution Date of 12/5/12 but the next steps are not documented nor does it states the overall impact to the Project Schedule. The Issue was last modified 12/13/12 2:35pm but the Resolution Plan not updated. • Issue 35 OIT Gateway Interfaces: Has an Issue Severity of Critical and it does not have an Action Plan. The Issue was last modified at 12/13 2:36pm but the Resolution Plan was not updated. Of the 12 open issues, all have a past due Resolution Due Date. Unable to determine days overdue to ensure issues are resolved in a timely manner. **Recommendation**

Status	No.	Area	Sub-Area	Assessment and Recommendations
				1. A more robust tool is required to report, communicate and monitor the issues; and to resolve in a timely manner. Implement an automated Issue Tool to track Issues. 2. Update the Issue(s) that lack an Action Plan. 3. Update the Issue(s) with current progress. 5. Monitor the Issue(s) and update accordingly. 6. Review the Issue Log on a weekly basis as these have an impact to the overall Project Schedule.
	70	**Miscellaneous**	**Risk Log** *(Extracted 121912 10:30am)*	**Assessment** There is a lack of monitoring the Risk Log. There are several Critical and Major Risks logged but yet some of the Risks have no Mitigation Plan nor does it provide a detail Action Plan. Below are a few examples: • Risk 5 COHBE Resource Availability: Has a Risk Severity of Major and has a past due Risk Action Due Date of 9/24/12. The Risk Action Plan lacks details. There is no Contingency Plan indicated. The Risk last modified at 9/10/12 1:39pm. • Risk 26 Release Deployment: Has an Issue Severity of Critical and has a Next Mitigation Step Due Date is 12/31/12. This risks logged 9/10/12, there has been no action taken on this risk. Nor does it state the overall impact to the Project Schedule. The Risk last modified at 11/28/12 4:29pm. • Risk 23 hCentive Bandwidth for Support of COHBE Enhancements: Has a Risk Severity of Major and has a past due Risk Action Due Date of 9/17/12. The Risk Action Plan lacks details. There is no Contingency Plan indicated. The Risk last modified at 11/28/12 4:09pm.

Status	No.	Area	Sub-Area	Assessment and Recommendations
				Of the 21 open risks, 12 lack a Risk Action Due Date and five have a past due Risk Action Due Date. Unable to determine days overdue to ensure risks are resolved in a timely manner. **Recommendation** 1. Update the Risk(s) that lack a Mitigation and or Contingency Plan. 2. Update the Risk(s) with the latest progress. 3. Monitor the Risk(s) and update on a recurring basis. 4. Review the Risk Log on a weekly basis as these have an impact to the overall Project Schedule.

Draft Wor

4.0 Risks and Issue Management

First Data has identified potential issues and risks outside of the issues and risks already identified by the project. We recommend that the project review and incorporate these into the Project Risk and Issue management processes. Below is a high-level definition of a risk versus an issue:

- A risk is usually an unknown event that may affect the course of a project plan, while an issue is a risk that has been realized, although not always.
- A risk has no effect in its current state, while an issue is an immediate problem; that needs to be resolved on the spot.
- A risk may be absorbed into a project with no effect at all, while an issue usually has effects, mainly negative.

4.1 Risk Log

ID	Risk Impact	Probability of Occurrence	Date Submitted	Risk Description	First Data Recommendations
1	High	High	1/14/13	CGI may not be able to incorporate the Change Requests that has been identified as required for the October Go-Live date.	1. Develop processes and procedures that minimize the need for the requested functionality. 2. Work with CGI to scale back the requested functionality to reduce the estimated level of effort.
2	High	High	1/14/13	OIT may not have the Rules Engine developed and implemented within the required time frames.	1. Contract directly with Deloitte to stand up a Corticon server that could be called by COHBE and CBMS 2. Treat Medicaid as just another carrier with one requirement (400% poverty) Let Medicaid figure out the right aid code on their existing system and timeframes. 3. Build the Fed hub interface to the OIT using the same standard interface used by the Feds. State gateway

ID	Risk Impact	Probability of Occurrence	Date Submitted	Risk Description	First Data Recommendations
					unavailability could be avoided by changing the destination of the COHBE interface. 4. Request that the Feds make available an exact copy of the Federal BRE for implementation at the state data center including the rules and exact product specifications. 5. Request that the Governor's office direct OIT and HCPF to execute a contract with Deloitte by January 31, 2013 so work can begin understanding that it may not be accurately scoped and necessitate a change request. The work on this interface is necessary to confirm their current design of the application and should begin even if the requirements are not robust or complete. An initial work order should be established as part of the OIT contract and MOU to allocate OIT and HCPF vendor resources to assist in the analysis and refine the scope of the effort.
3	High	High	1/14/13	The separation of the license agreement and associated MOU with hCentive from the CGI contract could create a gap in responsibility that would decrease the accountability of CGI for the complete system solution.	1. Add clear requirements to the hCentive MOU to meet the online requirements that are part of the CGI contract. 2. Monitor gaps between the requirements and the proposed solution through the requirements traceability matrix to identify areas that must be addressed by either CGI or hCentive. 3. It is not practical to recombine these two contracts given that the CGI contract has already been executed and would, therefore, constitute a change order with CGI. First Data recommends that COHBE be aware of the potential issue and monitor the overall system for compliance with requirements throughout the SDLC. CGI as the system integrator should have primary

ID	Risk Impact	Probability of Occurrence	Date Submitted	Risk Description	First Data Recommendations
					responsibility for bridging any gaps in the integration of hCentive as a COTS product.
4	High	High	1/14/13	Currently, there are no formal review functional or technical work products prior to coding (e.g. General System Design/Wireframes, Detail System Design, etc.) This has led to re-work and could lead to re-work downstream. (E.g. The Carrier Portal Use Case is currently be re-evaluated whether it contains accurate and detail information while development has already started.	1. Review all Use Cases and evaluate whether it contains the level of details needed for development. Review modules that are currently in development and verify it meets the requirements. 2. Implement formal reviews of functional and technical work products to ensure common understanding, avoid re-work and transparency.
5	High	High	1/14/13	Development tools that are not part of the same suite are being used by the project including SOAUI, ALM and .JIRA. Difficulties coding the custom integration of these tools could impact the projects ability to meet the project schedule.	1. Closely monitor and track the integration effort and any customizations that are required. This includes the development of custom or special reports and interface development. 2. It may be necessary to monitor the interfaces (specifically between ALM and JIRA to ensure that defects are not being lost or assigned incorrectly.
6	High	High	1/14/13	hCentive is a COTS product that is undergoing significant development to be a capable and complete Exchange solution. This development effort may not be successful within the timeframes required for Exchange implementation.	1. COHBE should pursue a parallel track to join the Federal system. This effort should include working with CGI to identify a final go no-go decision point that is prior to having to select the Federal solution but after sufficient testing of the hCentive portions of the Exchange System have been completed. 2. First Data recognizes that hCentive and CGI are the vendors for the Federal solution and the mitigation strategy identified makes it unlikely that the Federal system would be available. However, it is possible that the Federal System would be completed while the

ID	Risk Impact	Probability of Occurrence	Date Submitted	Risk Description	First Data Recommendations
					Colorado Exchange System is not.
7	High	High	1/14/13	hCentive releases are not being delivered in deployable modules, e.g. the functionality in each release isn't complete from either an individual user role or group of users perspective . Therefore, the implementation of hCentive is dependent on the completion of the entire hCentive development effort and required customizations. This forces the back loading the testing effort with the testing of end-to-end functionality near the end of the testing phase.	1. CGI should reevaluate the scope and content of the hCentive releases to focus on functionality that is complete as measured by either user role and group or functional area. 2. First Data recognizes that altering hCentive's development schedule to accommodate this realignment of functionality is complicated by the fact that the software is being developed to be used by other hCentive customers. However, developing an Implementation Plan based on end user functionality may be beneficial to these same hCentive customers' implementation efforts and not just apply to the Colorado Exchange System.
8	High	High	1/14/13	COHBE is currently in the process of securing a vendor to implement the Contact Center Solution and selecting a Contact Center facility. With the given timeframe, there is a risk the Service Center will not be ready by Go-Live.	1. COHBE should secure a vendor as soon as possible. Determine requirements for Go-Live versus what can be implemented post-implementation. 2. Start discussions with Stakeholders to ensure shared understandings.
9	High	High	1/14/13	There is a lack of oversight in regards to CGI Project Schedule, Risk Log and Issue Log, which could lead to collateral damage downstream.	1. COHBE should have more onsite presence at CGI to gain more insight. 2. COHBE should hold CGI more accountable on their integration management.

ID	Risk Impact	Probability of Occurrence	Date Submitted	Risk Description	First Data Recommendations
10	High	High	1/14/12	There are three Project Schedules: CGI, COHBE, HCPF/OIT. Each of the Project Schedules is managed individually; this adds additional risk to the project as no one owns the breadth of the project as a whole.	1. Set-up weekly meetings to discuss and share Project Schedule. 2. Assign a resource(s) to manage the inter-dependencies of the Project Schedules.

Draft Work P

4.2 Issue Log

ID	Issue Severity	Date Submitted	Issue Description	Issue Status	First Data Recommendations
1	High	1/14/13	There is lack of managing and monitoring the Project Schedule. The Project Schedule has: Over 600 late tasks Over 800 task that have been identified as Critical Task with zero or negative slack It is unclear how these affect the overall project schedule.	CGI is currently re-structuring the Project Schedule and determining the impacts.	1. Re-evaluate the Project Schedule; if the methodology is not working then change the methodology. 2. Evaluate the late tasks and determine how these affects the overall project schedule. Set a due date. 3. Develop an Action or Mitigation Plan for the late tasks. Set a due date. 4. Review and update the Project Plan on a weekly basis. Communicate the schedule slippage and impacts to all Stakeholders.
2	High	1/14/13	Many of the procedures and documents that were created at the beginning of the project may have changed as CGI placed them into practice. CGI states they will need to update all of the Project Management Plan components in the near future to document the processes and procedures that are currently employed if different from the original process.	A date has not been provided as to when these will be updated.	1. CGI to develop an Action Plan to start updating the Project Management Plans, as these are integral to ensure quality of the work products delivered. Set a due date.

ID	Issue Severity	Date Submitted	Issue Description	Issue Status	First Data Recommendations
3	High	12/6/12	First Data has attempted several times to reach out to CGI to better gain a perspective on CGI's development/deployment activities beyond what is documented in the Project Work Plan and documentation but it has not been successful. This impedes First Data's ability to deliver a complete work product to COHBE.	CGI provided materials and resources starting on 1/2/13. COHBE extended the IV&V Assessment period.	1. None at this time, though this is a potential risk for future IV&V Reports as the duration of the assessment period is quite shorter. The ability of CGI to respond in a timely manner is a concern.
4	High	1/14/13	The DED for DSD has not been completed and the DSD for parts of the system have been completed. The DSD that has been completed may have to be reworked if the DED requires a greater level of detail or additional information than has been documented.	None at this time.	1. The DED for DSD should be completed as soon as possible.
5		1/14/13	CGI has not yet completed a design of the development environment that includes all of the tools that are used including ALM and JIRA. First Data recognizes that this documentation is not a formal deliverable but had to have been created as part of building out an environment this complex.	First Data requested that this design be provided but had not received it prior to this Assessment.	1. The designs for the development environment be created and provided to COHBE for their review.

ID	Issue Severity	Date Submitted	Issue Description	Issue Status	First Data Recommendations
6	High	1/14/13	The definition of Iterations is not contained in other project documentation including the Project Schedule beyond the name of the deliverable. This is a particular concern moving forward that Iterations are not defined and don't have a relationship with tasks, releases or functionality from a Use Case perspective.	None at this time.	1. Develop a crosswalk to relate hCentive releases, Use Cases and requirements. 2. Request CGI to rename these deliverables if additional definition is warranted or the relationships are unclear.
7	High	1/14/13	Only 10 of the 89 planned Design have been completed. It is unclear how this impacts the overall project schedule.	None at this time.	1. Evaluate how these impact the current work effort and impacts to the project. 2. Create an Action Plan.
8	High	1/14/13	Only 8 of the 17 planned Deliverables have been completed. It is unclear how this impacts the current work efforts.	None at this time.	1. Evaluate how these impact the current work effort and impacts to the project. 2. Create an Action Plan.
9	High	1/14/13	CGI lacks integration management which, includes scope, time, cost, quality, communications, and risk. This has impacted current work efforts and has attributed to the late tasks and deliverable.	None at this time.	1. Evaluate current processes and identify gaps. 2. Implement formal project management processes.

ID	Issue Severity	Date Submitted	Issue Description	Issue Status	First Data Recommendations
10	High	1/14/13	CGI lacks a consistent overall methodology that is applied to the Project Schedule, System Development Life Cycle, defined set of deliverables and work products. The evolved methodology lacks the internal consistency necessary to be confident that the system will meet all of the requirements.	None at this time.	1. Re-evaluate the current methodology and utilize a strategic approach.
11	High	1/14/13	The Project Schedule is an integral tool in managing a Project. The CGI Project Schedule lacks consistent organization and methodology.	None at this time.	1. Re-evaluate the Project Schedule. 2. Discontinue modifications to the methodology. 3. Persist a consistent methodology.

Draft W

COLORADO HEALTH BENEFIT EXCHANGE

First Data.

5.0 Appendix

A. Meetings Attended

Date	Meetings Attended
Weekly	PMO Joint Status Meeting
Weekly	COHBE/CGI Leadership Meeting
Weekly	CCB
Weekly	All Staff Meeting
11/26/12	COHBE / CGI Project Review
11/27/12	Weekly
11/29/12	COHBE IT & Implementation Committee
11/30/12	COHBE + Carrier Interoperability: Technology Solution Approach
	Schedule Walkthrough/Review
12/5/12	HCPF Interoperability Team Status Meeting
	Review PMO Items with CGI
	COHBE Touch Point
12/6/12	COHBE All Staff Working Session
	SHOP AG
	Review Project Plan Questions for CGI
	On-site CGI COHBE/hCentive meeting
12/7/12	JAD Discovery: AM-016 Login Management
12/10/12	Weekly COHBE BA meeting
	COHBE Board Meeting
12/12/12	HCPF Interoperability Team Status Meeting
	OIT/COHBE Technical Integration
12/13/12	COHBE & HCPF Policy Coordination & Alignment
	Fed HIX / COHBE Cross Team Meeting
12/17/12	Horizontal Leads Meeting
	SERFF and Data Model
12/20/12	ALM Complete Review with CGI
	CGI Weekly architecture group meeting
12/21/12	Testing Checkpoint

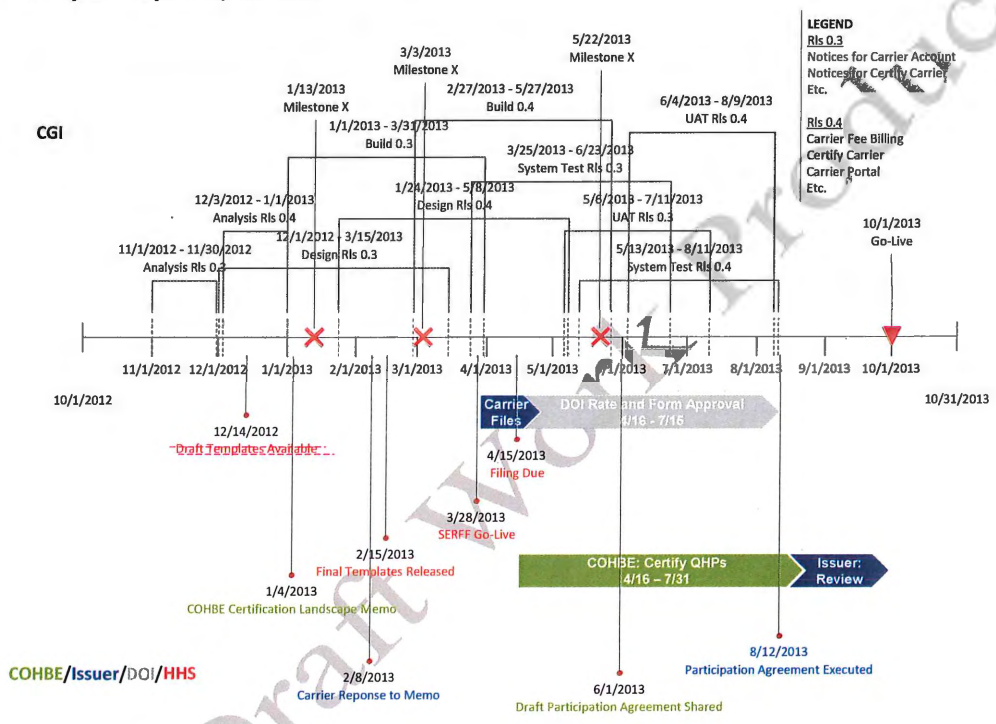
Draft Work Product

B. Interviews Conducted

Date	Interviewee	Title
12/10/11	Gary Schneider and Chuck Fish	IT Project Manager/PMO Lead
12/11/12	Patty Fontneau	CEO
12/12/12	Lindy Hinman	Chief Operating Officer
12/12/12	Jed Summerton	Technical Lead and Business Intelligence
12/13/12	Cammie Blais	Chief Financial Officer
12/20/12	Matt Benson	Interface Lead
12/20/12	Stephanie Eng	Health Plan Account Manager
12/21/12	Adele Work	Implementation Lead

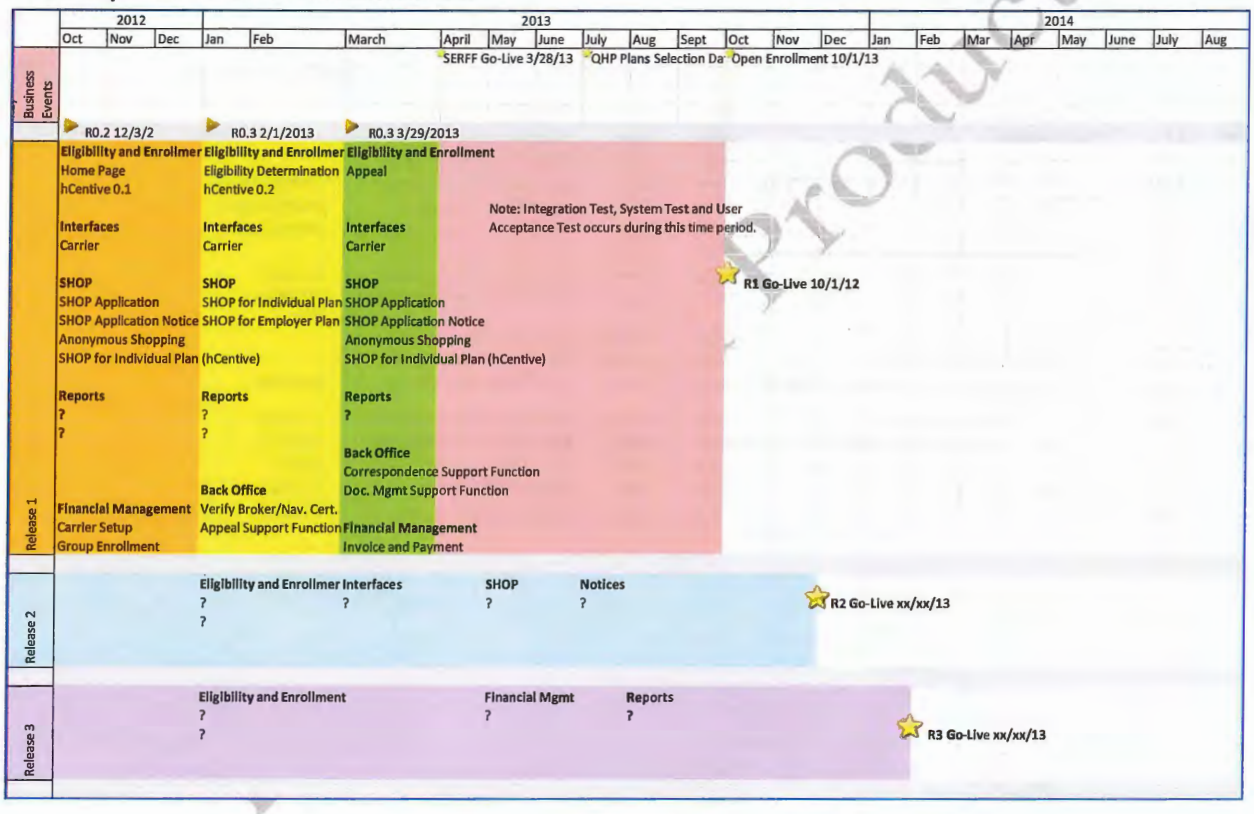
Draft Work Product

C. Example Graphical/Timeline



Draft Work Product

D. Example End to End Release Schedule



Product

E. IV&V_COHBE Project Schedule_011413

ID	Task Mode	WBS	Task Name	% Complete	Duration	Start	Finish	Predeces	Resource Names	Notes	No S
1		1	COHBE IV & V Services	45%	200 days	Fri 11/16/12	Thu 8/22/13				
2		1.1	Project Initiation	100%	3 days	Fri 11/16/12	Tue 11/20/12				
3		1.1.1	Confirm COHBE Project Approach	100%	1 day	Tue 11/20/12	Tue 11/20/12				
4		1.1.1.1	Validate High Level Timeline with Critical Dates	100%	1 day	Tue 11/20/12	Tue 11/20/12		COHBE,First Data		
5		1.1.1.2	Validate Major Tasks	100%	1 day	Tue 11/20/12	Tue 11/20/12		COHBE,First Data		
6		1.1.1.3	Validate Communication Processes and Protocols	100%	1 day	Tue 11/20/12	Tue 11/20/12		COHBE,First Data		
7		1.1.2	Conduct Kick-Off meeting with COHBE Management	100%	3 days	Fri 11/16/12	Tue 11/20/12				
8		1.1.2.1	Prepare and produce Kick-Off meeting materials	100%	2 days	Fri 11/16/12	Mon 11/19/12		First Data		
9		1.1.2.2	Conduct Kick-Off meeting with COHBE Management Team	100%	1 day	Tue 11/20/12	Tue 11/20/12	8	COHBE,First Data		
10		1.2	Project Management Initiation	100%	7.5 days	Tue 11/20/12	Thu 11/29/12				
11		1.2.1	COHBE IV & V Project Work Plan	100%	7.5 days	Tue 11/20/12	Thu 11/29/12				
12		1.2.1.1	Review Tasks, Tasks Dependencies, Milestones, and Resources	100%	1 day	Tue 11/20/12	Tue 11/20/12		First Data		
13		1.2.1.2	Prepare COHBE IV & V Work Plan	100%	3.5 days	Wed 11/21/12	Mon 11/26/12	12	First Data		
14		1.2.1.3	Submit COHBE IV & V Project Work Plan to COHBE	100%	0 days	Mon 11/26/12	Mon 11/26/12	13	First Data		
15		1.2.1.4	COHBE reviews and provides comments	100%	2 days	Mon 11/26/12	Wed 11/28/12	14	COHBE		
16		1.2.1.5	Incorporate COHBE Comments	100%	1 day	Wed 11/28/12	Thu 11/29/12	15	First Data		
17		1.2.1.6	Submit COBHBE Final IV & V Project Work Plan to	100%	0 days	Thu 11/29/12	Thu 11/29/12	16	First Data		

Draft Product

ID	Task Mode	WBS	Task Name	% Complete	Duration	Start	Finish	Predeces	Resource Names	Notes	No S
18		1.3	**IV&V Activities**	40%	198 days	Tue 11/20/12	Thu 8/22/13				
19		1.3.1	Task 1	40%	198 days	Tue 11/20/12	Thu 8/22/13				
20		1.3.1.1	Review #1- Initial Assessment	95%	43 days	Tue 11/20/12	Thu 1/17/13				
21		1.3.1.1.1	Phase 0	100%	4 days	Tue 11/20/12	Fri 11/23/12				
22		1.3.1.1.1.1	Request required materials from COHBE	100%	4 days	Tue 11/20/12	Fri 11/23/12		First Data		
23		1.3.1.1.2	Phase 1	100%	17 days	Mon 11/26/1	Tue 12/18/12				
24		1.3.1.1.2.1	Review materials	100%	17 days	Mon 11/26/12	Tue 12/18/12		First Data		
25		1.3.1.1.3	Phase 2	100%	28 days	Mon 12/3/12	Wed 1/9/13				
26		1.3.1.1.3.1	Draft Schedule of on-site activities	100%	1 day	Mon 12/3/12	Mon 12/3/12		First Data		
27		1.3.1.1.3.2	Meeting with COHBE- Review Schedule of on-site activities	100%	1 day	Mon 12/3/12	Mon 12/3/12		COHBE,First Data		
28		1.3.1.1.3.3	Assessment (e.g. on-site interviews, attend meetings, review documents, Q & A, etc.)	100%	10 days	Tue 12/4/12	Mon 12/17/12	27	First Data		
29		1.3.1.1.3.4	Extended Assessment to review CGI materials	100%	3 days	Mon 1/7/13	Wed 1/9/13			12/20/12: Intial request made to CGI on 12/6/12; several attempts were made thereafter. CGI has not provided materials for review. COHBE requested an extension of the assessment period. This will push the delivery of the report to week of	
30		1.3.1.1.4	Phase 3	87%	23 days	Tue 12/18/12	Thu 1/17/13				
31		1.3.1.1.4.1	Draft Report Review #1 Initial Assessment	100%	20 days	Tue 12/18/12	Mon 1/14/13	28	First Data		
32		1.3.1.1.4.2	Submit Draft to COHBE for Review	100%	0 days	Mon 1/14/13	Mon 1/14/13	31	First Data		
33		1.3.1.1.4.3	COHBE Review Period	0%	1 day	Tue 1/15/13	Tue 1/15/13	32	COHBE	Comments due to FD by end of day.	
34		1.3.1.1.4.4	Update Draft with COHBE Comments	0%	1 day	Wed 1/16/13	Wed 1/16/13	33	First Data		
35		1.3.1.1.4.5	Submit Final Report Review #1 Initial Assess	0%	0 days	Wed 1/16/13	Wed 1/16/13	34	First Data		
36		1.3.1.1.4.6	Meeting with COHBE- Review Final Report	0%	1 day	Thu 1/17/13	Thu 1/17/13	35	COHBE,First Data		

Draft

ID	Task Mode	WBS	Task Name	% Complete	Duration	Start	Finish	Predeces	Resource Names	Notes	No S
37		1.3.1.2	Bi-Monthly Review #2- February	0%	19 days	Mon 2/4/13	Thu 2/28/13				
38		1.3.1.2.1	Phase 0	0%	1 day	Mon 2/4/13	Mon 2/4/13				
39		1.3.1.2.1.1	Request required materials from COHBE and	0%	1 day	Mon 2/4/13	Mon 2/4/13		First Data	If not available in SharePc	
40		1.3.1.2.2	Phase 1	0%	5 days	Mon 2/11/13	Fri 2/15/13				
41		1.3.1.2.2.1	Review materials	0%	5 days	Mon 2/11/13	Fri 2/15/13		First Data		
42		1.3.1.2.3	Phase 2	0%	5 days	Mon 2/11/13	Fri 2/15/13				
43		1.3.1.2.3.1	Draft Schedule of on-site activities	0%	1 day	Mon 2/11/13	Mon 2/11/13		First Data		
44		1.3.1.2.3.2	Meeting with COHBE- Review Schedule of on-site activities	0%	1 day	Tue 2/12/13	Tue 2/12/13	43	COHBE,First Data		
45		1.3.1.2.3.3	Assessment (e.g. on-site interviews, attend meetings, review documents, Q & A, etc.)	0%	4 days	Tue 2/12/13	Fri 2/15/13	43	First Data		
46		1.3.1.2.4	Phase 3	0%	9 days	Mon 2/18/13	Thu 2/28/13				
47		1.3.1.2.4.1	Draft Bi-Monthly Report Review #2	0%	6 days	Mon 2/18/13	Mon 2/25/13	45	First Data		
48		1.3.1.2.4.2	Submit Draft to COHBE for Review	0%	0 days	Mon 2/25/13	Mon 2/25/13	47	First Data		
49		1.3.1.2.4.3	COHBE Review Period	0%	1 day	Tue 2/26/13	Tue 2/26/13	48	COHBE	Comments due to FD by end of day.	
50		1.3.1.2.4.4	Update Draft with COHBE Comments	0%	1 day	Wed 2/27/13	Wed 2/27/13	49	First Data		
51		1.3.1.2.4.5	Submit Final Bi-Monthly Report Review #2	0%	0 days	Wed 2/27/13	Wed 2/27/13	50	First Data		
52		1.3.1.2.4.6	Meeting with COHBE- Review Final Report	0%	1 day	Thu 2/28/13	Thu 2/28/13	51	COHBE,First Data		

Draft Work

ID	Task Mode	WBS	Task Name	% Complete	Duration	Start	Finish	Predeces	Resource Names	Notes	No S
53		1.3.1.3	Bi-Monthly Review #3- April	0%	19 days	Mon 3/25/13	Thu 4/18/13				
54		1.3.1.3.1	Phase 0	0%	1 day	Mon 3/25/13	Mon 3/25/13				
55		1.3.1.3.1.1	Request required materials from COHBE and	0%	1 day	Mon 3/25/13	Mon 3/25/13		First Data	If not available in SharePc	
56		1.3.1.3.2	Phase 1	0%	5 days	Mon 4/1/13	Fri 4/5/13				
57		1.3.1.3.2.1	Review materials	0%	5 days	Mon 4/1/13	Fri 4/5/13		First Data		
58		1.3.1.3.3	Phase 2	0%	5 days	Mon 4/1/13	Fri 4/5/13				
59		1.3.1.3.3.1	Draft Schedule of on-site activities	0%	1 day	Mon 4/1/13	Mon 4/1/13		First Data		
60		1.3.1.3.3.2	Meeting with COHBE- Review Schedule of on-site activities	0%	1 day	Tue 4/2/13	Tue 4/2/13	59	COHBE,First Data		
61		1.3.1.3.3.3	Assessment (e.g. on-site interviews, attend meetings, review documents, Q & A, etc.)	0%	4 days	Tue 4/2/13	Fri 4/5/13	59	First Data		
62		1.3.1.3.4	Phase 3	0%	9 days	Mon 4/8/13	Thu 4/18/13				
63		1.3.1.3.4.1	Draft Bi-Monthly Report Review #3	0%	6 days	Mon 4/8/13	Mon 4/15/13	61	First Data		
64		1.3.1.3.4.2	Submit Draft to COHBE for Review	0%	0 days	Mon 4/15/13	Mon 4/15/13	63	First Data		
65		1.3.1.3.4.3	COHBE Review Period	0%	1 day	Tue 4/16/13	Tue 4/16/13	64	COHBE	Comments due to FD by end of day.	
66		1.3.1.3.4.4	Update Draft with COHBE Comments	0%	1 day	Wed 4/17/13	Wed 4/17/13	65	First Data		
67		1.3.1.3.4.5	Submit Final Bi-Monthly Report Review #3	0%	0 days	Wed 4/17/13	Wed 4/17/13	66	First Data		
68		1.3.1.3.4.6	Meeting with COHBE- Review Final Report	0%	1 day	Thu 4/18/13	Thu 4/18/13	67	COHBE,First Data		

Draft Wo

ID	Task Mode	WBS	Task Name	% Complete	Duration	Start	Finish	Predeces	Resource Names	Notes	No S
69		1.3.1.4	Bi-Monthly Review #4- June	0%	19 days	Mon 5/27/13	Thu 6/20/13				
70		1.3.1.4.1	Phase 0	0%	1 day	Mon 5/27/13	Mon 5/27/13				
71		1.3.1.4.1.1	Request required materials from COHBE and	0%	1 day	Mon 5/27/13	Mon 5/27/13		First Data	If not available in SharePo	
72		1.3.1.4.2	Phase 1	0%	5 days	Mon 6/3/13	Fri 6/7/13				
73		1.3.1.4.2.1	Review materials	0%	5 days	Mon 6/3/13	Fri 6/7/13		First Data		
74		1.3.1.4.3	Phase 2	0%	5 days	Mon 6/3/13	Fri 6/7/13				
75		1.3.1.4.3.1	Draft Schedule of on-site activities	0%	1 day	Mon 6/3/13	Mon 6/3/13		First Data		
76		1.3.1.4.3.2	Meeting with COHBE- Review Schedule of on-site activities	0%	1 day	Tue 6/4/13	Tue 6/4/13	75	First Data		
77		1.3.1.4.3.3	Assessment (e.g. on-site interviews, attend meetings, review documents, Q & A, etc.)	0%	4 days	Tue 6/4/13	Fri 6/7/13	75	First Data		
78		1.3.1.4.4	Phase 3	0%	9 days	Mon 6/10/13	Thu 6/20/13				
79		1.3.1.4.4.1	Draft Bi-Monthly Report Review #4	0%	6 days	Mon 6/10/13	Mon 6/17/13	77	First Data		
80		1.3.1.4.4.2	Submit Draft to COHBE for Review	0%	0 days	Mon 6/17/13	Mon 6/17/13	79	First Data		
81		1.3.1.4.4.3	COHBE Review Period	0%	1 day	Tue 6/18/13	Tue 6/18/13	80	COHBE	Comments due to FD by end of day.	
82		1.3.1.4.4.4	Update Draft with COHBE Comments	0%	1 day	Wed 6/19/13	Wed 6/19/13	81	First Data		
83		1.3.1.4.4.5	Submit Final Bi-Monthly Report Review #4	0%	0 days	Wed 6/19/13	Wed 6/19/13	82	First Data		
84		1.3.1.4.4.6	Meeting with COHBE- Review Final Report	0%	1 day	Thu 6/20/13	Thu 6/20/13	83	COHBE,First Data		

Draft Work

ID	Task Mode	WBS	Task Name	% Complete	Duration	Start	Finish	Predeces	Resource Names	Notes	No S
85		1.3.1.5	Bi-Monthly Review #5- August	0%	19 days	Mon 7/29/13	Thu 8/22/13				
86		1.3.1.5.1	Phase 0	0%	1 day	Mon 7/29/13	Mon 7/29/13				
87		1.3.1.5.1.1	Request required materials from COHBE and	0%	1 day	Mon 7/29/13	Mon 7/29/13		First Data		
88		1.3.1.5.2	Phase 1	0%	3 days	Mon 8/5/13	Wed 8/7/13				
89		1.3.1.5.2.1	Review materials	0%	3 days	Mon 8/5/13	Wed 8/7/13		First Data		
90		1.3.1.5.3	Phase 2	0%	5 days	Mon 8/5/13	Fri 8/9/13				
91		1.3.1.5.3.1	Draft Schedule of on-site activities	0%	1 day	Mon 8/5/13	Mon 8/5/13		First Data		
92		1.3.1.5.3.2	Meeting with COHBE- Review Schedule of on-site activities	0%	1 day	Tue 8/6/13	Tue 8/6/13	91	First Data		
93		1.3.1.5.3.3	Assessment (e.g. on-site interviews, attend meetings, review documents, Q & A, etc.)	0%	4 days	Tue 8/6/13	Fri 8/9/13	91	First Data		
94		1.3.1.5.4	Phase 3	0%	9 days	Mon 8/12/13	Thu 8/22/13				
95		1.3.1.5.4.1	Draft Bi-Monthly Report Review #5	0%	6 days	Mon 8/12/13	Mon 8/19/13	93	First Data		
96		1.3.1.5.4.2	Submit Draft to COHBE for Review	0%	0 days	Mon 8/19/13	Mon 8/19/13	95	First Data		
97		1.3.1.5.4.3	COHBE Review Period	0%	1 day	Tue 8/20/13	Tue 8/20/13	96	COHBE	Comments due to FD by end of day.	
98		1.3.1.5.4.4	Update Draft with COHBE Comments	0%	1 day	Wed 8/21/13	Wed 8/21/13	97	First Data		
99		1.3.1.5.4.5	Submit Final Bi-Monthly Report Review #5	0%	0 days	Wed 8/21/13	Wed 8/21/13	98	First Data		
100		1.3.1.5.4.6	Meeting with COHBE- Review Final Report	0%	1 day	Thu 8/22/13	Thu 8/22/13	99	COHBE,First Data		

Draft Work

access health CT

Connecticut Health Benefits Exchange

IV&V Status Report

October 23, 2013

First Data.
b›yond the transaction

Contents

Introduction 3

IV&V October 1st Go Live Assessment for Release 2 3

Technical Infrastructure 3

Security 4

Testing 5

Performance and Stress Testing 7

Technical Operations 8

BEST Assessment 8

IV&V Status Report for Release 3 of CT-HIX 10

Project Management Assessment 10

Coordination with ConneCT 11

Technical Assessment Overview 13

Technical Architectural Review 13

Technical Architectural Findings 13

Technical Architectural Risks 14

Solutions Architectural Review 15

Workflow Interoperability and MITA Compliance 15

Solutions Architectural Risks 15

Security Architectural Review 16

Technical Operational Support Capability Review 17

Technical Operational Support Capability Risks 18

Testing Assessment 21

Release 3 Implementation Dates 21

Release 3 Iteration Scope 22

Outstanding Defects 23

Blueprint Scenario Testing 23

User Acceptance Testing 23
Testing Environment 23
Performance Testing 25
Reference Material Listing 26
Appendix A. Previously Identified Findings (Open) 29
Appendix B. Previously Identified Risks and Findings (Closed) 45

Introduction

The October IV&V Status Report is an update of the September IV&V report. This month's updates include a section addition summarizing the results of the October 1 launch of the Connecticut Health Exchange (Release 2 of the CT-HIX application) and some proposed "lessons learned" for going forward with Release 3 based on the IV&V team's observations. Release 3 of CT-HIX application is scheduled for production implementation on December 18, 2013 and will implement the requirements of the Affordable Care Act that will be in place for January 1, 2014.

The following three sections will follow the general format of previous IV&V Status Reports: Project Management Assessment, Technical Assessment and Testing Assessment. It is the goal of the First Data IV&V team to be more actively involved in Release 3 of CT-HIX testing of since the team has the opportunity to be more involved in this release's system development life cycle as well as the testing methodology being utilized.

IV&V October 1st Go Live Assessment for Release 2

The October 1, 2013 "Go Live" launch of the Connecticut Health Exchange was successful and has remained available to the public continually since October 1. The entire Access Health CT team and its partners are to be commended, especially considering the complexity of the Affordable Care Act (ACA) business rules, not to mention late rule changes, the complexity of the technical environments supporting the CT-HIX application, and the pressures of meeting public expectations on October 1. Previous IT engagements usually were implemented with a small group of partners whereas the CT-HIX effort had a far greater number of partners and service providers working together for the first time,

The IV&V October 1st Go Live Assessment follows the format used in the September IV&V Status Report for the October 1 Go Live Readiness Assessment.

Technical Infrastructure

The implementation of the CT-HIX Production technical infrastructure was completed in time for October 1 because of a concerted effort by all parties involved: Access Health technical staff, State Bureau of Enterprise System Technologies (BEST) staff, the Deloitte project team, and the KPMG project team. At times some of the Staging infrastructure was being completed in conjunction with the Production infrastructure implementation.

Much of the success of this effort to meet the October 1 deadline was due to efforts by the Access Health technical staff to consolidate all the tasks involving the infrastructure

implementation into one Go Live checklist, then document the sub-tasks required for each task identified in the CT-HIX Implementation Plan to ensure each step is completed, and finally to create a change management process that included managing the changes to the infrastructure with the changes ("releases" and fixes) to the CT-HIX application and the other services being implemented such as SHOP and the Exchange Help Desk.

This need for a more coordinated change management process was one of the risks identified in previous IV&V Status Reports and it appears that the effort to consolidate this management was instrumental in making the October 1 Health Exchange launch successful in Connecticut.

The lesson learned for future technical infrastructure management is to formalize change management of the CT-HIX application and the technical environments into a coordinated process that:

- Requires much less hands-on effort than the October 1 launch required.
- Includes a governance process that ideally makes Access Health senior technical staff responsible for coordinating changes across the CT-HIX application and the technical infrastructure environment supporting it.
- Includes a formal configuration management process for future changes to the technical infrastructure.
- Includes a version control process for migrating changes to the CT-HIX application in fewer releases so that more thorough regression testing can be conducted.

Security

Some of the glitches that customers experienced on the first day of October could have been resolved ahead of time if the security requirements of the Internal Revenue Service (IRS) were communicated earlier and the additional security components at BEST were implemented sooner. Some security components were implemented the week before October 1 and there is at least one component that is still being put in place. This situation, along with the inability to test outside Internet access through these security components in the User Acceptance Testing environment, made it impossible to anticipate the impact these components would have on the Health Exchange's external users. The unknown effect of these various security devices working with each other for the first time was a concern. When problems emerged after go-live (outside users getting into the Exchange and setting up accounts), the security changes added a layer of complexity to diagnose the source of the problems.

Lessons learned for security in the future:

- Security policies must be articulated, infrastructure requirements to support those policies can then be defined, including support practices for such devices. As components are added, the entire infrastructure array must be tested and a comprehensive change management process compiled to assure a stable environment.
- The Security infrastructure must be consistent across all environments (UAT, Staging and Production).
- Testing by all types of outside users should be conducted through the Internet in the UAT environment. Tunneling into the UAT environment via VPN access for UAT testing does not adequately test the outside firewalls and security appliances.

Testing

The September testing effort concentrated on three distinct areas: User Acceptance (UAT), Blueprint Scenario and End-to-End. User Acceptance had actually begun in early August. During the testing effort, there were regularly scheduled builds as well as occasional patches. Patches were employed sparingly. In the early part of the UA testing, a higher-than-expected number of defects were identified and reported. The Deloitte development team worked through the defects. Since go-live, Deloitte continues to work through the remaining defects. The UA test team continues to test and close these defects. The Maximus Call Center was provided a list of the open defects prior to go-live in order for their team to be educated about and assist callers that encountered a known defect.

At the time of go-live, there are three ahCT environments hosted at Bureau of Enterprise Systems and Technology (BEST) within the Department of Administrative Services (DAS):

- User Acceptance,
- Staging, and
- Production.

BEST policies prohibit external access (Internet) to the User Acceptance environment. There are security applications deployed in Staging and Production that were not deployed in User Acceptance. The applications themselves were tested, but not in concert with the Deloitte solution. Given the importance of secure Internet access to the ahCT, these constraints were a serious concern.

The paper submission workflow processes were tested prior to go-live. This included testing with ahCT vendors Xerox and Scan Optics. FileNet is an essential application to these processes. During the two weeks proceeding go-live, the FileNet application had performance issues. IBM as well as external subject matter expertise was brought in. The

cause was identified and mitigated prior to go-live. BEST is continuing to closely monitor the FileNet application, given its importance to many business processes.

Deloitte and bswift submitted their respective Blueprint scenarios submissions on or before August 15. Their submissions were reviewed and comments returned to the respective submitter. Additional information where requested in the comments was uploaded. On September 28, a preliminary review of all scenarios was provided from Booz Allen Hamilton (BAH) to the submitters. Based on the review, bswift provided additional documentation on October 4. On October 5, two additional feedback documents were provided by BAH. In discussing the document with bswift, they were comfortable that the additional documentation previously provided addressed the document's comments. Deloitte is expected to respond shortly to the October 5 documents.

In some instances, the reviewers were looking for scenarios that confirmed functionalities which are being deferred to later releases. In the case of scenarios that confirmed the vendor's ability to transmit the 834 transaction, CMS's inability to accept the transaction was the limitation. Lastly, at the time of the testing, notices going to the clients were still under review, thus not part of the test result submissions.

In addition, CMS published updated submission requirements (version 1.6) that Access Health is presently addressing. During the week of October 14, Access Health will begin some testing that is not impacted by the new 1.6 requirements. Deloitte anticipates that the version 1.6 requirements will be addressed in Release 3.2 on December 4.

Deloitte completed its Blueprint End-to-End testing on September 20, 2013. Access Health employs seven services through the Federal Data Services hub. The tests were executed from within the Deloitte application. The tests were executed from the Staging environment hosted at Bureau of Enterprise Systems and Technology (BEST) within the Department of Administrative Services (DAS).

Once successfully completed, the test case results were uploaded to CALT. Screenshots and logs were included as part of the uploaded documentation. Deloitte executed and submitted their results as follows:

Test Case Number	H1 Remote Identity Proofing	H3 SSA Composite	H4 Verify Lawful Presence	H7 Close Case	H9 Verify household Income/Size	H19 Advance Payment Premium	H31 Non Employer Sponsored Minimum
TC20011	1	1	1		1	1	1
TC20012						1	
TC20018	1	1	1	1	1		1
TC20022						1	1
TC20032	1	1	1	1	1		1
TC20062	1	1	1	1	1		1
TC20079						1	
TC20102	1	1	1		1		
TC 20188	1	1			1		
TC20256	1	1	1	1	1		
TC20370	1		1	1	1	1	
Totals	**8**	**7**	**7**	**5**	**8**	**5**	**5**

Lessons learned regarding various testing efforts:

- A testing environment that doesn't truly reflect Production is highly problematic, especially given the complexity of security demanded.
- The completeness of the test scenarios and a larger body of test data would have been beneficial.
- The inability to perform complete end-to-end testing, including Internet access and Security device deployment, was troubling. Because of these constraints, expected end-to-end scenarios were absent.

Performance and Stress Testing

The performance of the CT-HIX application and the supporting environment had some issues once in production in October 1, but BEST technical staff and the Deloitte project team were able to utilize load balancing functionality implemented for Access Health such as Akamai. Some performance and penetration testing continues being conducted for the security environment, but this does not seem to be factor in system performance at this time. An enhanced reporting process being put in place provides better communications of defects and underlying causes allowing BEST to determine any impact on infrastructure performance due to these defects.

Technical Operations

The operational support of the CT-HIX technical environment was adequate for the October 1 production Go Live in part because additional technical staff were put "on alert" during this time and the technical teams kept in close communications during the initial implementation of CT-HIX. Since October 1 there has been an effort to improve communications between the various operations supporting CT-HIX, including the Maximus call center and the Xerox call center. Access Health is developing a tracking mechanism process for collecting defect information, defect prioritizing as well as closing the communication loop by reporting to the defect identifier, thus better ensuring all involved in operational support are informed.

Once this process is put in place to track and resolve defects, change control procedures governing technical infrastructure issues need to be finalized. The combined process and procedures can be followed to ensure communication is maintained across the CT-HIX technical environments. Adhering to the process should aid in documentation currency and may require additional staff training.

Lessons learned for technical operations from an IV&V perspective:

- Operational management across a complex technical environment with multiple organizations requires a clear understanding of roles and responsibilities.
  In addition, there needs to be formal operational procedures and communication tools. CT-HIX go-live was made possible through a Herculean effort by the teams involved, but this kind of effort cannot be sustained for long.
  Improvements in clarifying roles and responsibilities needs to include adequate documentation and training to better ensure that in the future, if additional staff resources are brought for systems support, disruption will be minimal.
- A Technical Continuity Plan and subsequent test of the plan would provide valuable insight into what happens when specific technical components fail, what contingencies need to be put in place and how to recover successfully from that failure. This effort will go a long way to minimizing recovery time for outages and ensure adequate restoration procedures for situations that would be difficult to predict and plan for otherwise.

BEST Assessment

At the request of Access Health CT, the First Data team verified and updated documentation of hardware and software assets acquired by ahCT, and determined where each component was physically located and by environment (User Acceptance / Staging / Production) installed. The team identified State contracts under which assets were acquired, but could not document discounts or pricing models applied to demonstrate appropriate pricing

paid. Where available, multi-year hardware support and software licensing options were obtained to lower long-term costs.

DAS/BEST furnished utilization reports to document server occupancy and identify any other agency sharing that server. In a few cases, storage and WebSphere hardware and software are shared with its partner agency, the Department of Social Services' ConneCT System. And in a single case, ahCT paid to expand the State's central IBM-FileNet repository to meet its needs. BEST's Uptime reports depicted both VMware and LINUX server activity for the ahCT solution in early September, on October 1, and on October 3. Based on these reports, ahCT plans to obtain regular periodic utilization reports as part of its performance monitoring. The IV&V team recommended a process be instituted to keep this information updated and to provide better financial information related to ongoing support costs and commitments. AHCT is now planning to institute improved procedures for supporting the technical environment, clarifying roles and responsibilities between DAS/BEST and Deloitte.

The First Data team strongly recommends Access Health, BEST and Deloitte work together on a Technical Continuity Plan with subsequent testing to probe the current technical environment for vulnerabilities and identify needed additional operational procedures for quick recovery and restoration of systems.

IV&V Status Report for Release 3 of CT-HIX

The following is an update of the previous assessments of Release 2 of CT-HIX provided by the First Data team in each monthly IV&V Status Report. The focus of this report will be the implementation of Release 3 of the CT-HIX application and the associated services supporting it. Risks associated with past assessments have been updated for the month of October if the First Data team has determined that they are still a risk for the December 6, 2013 Go Live of CT-HIX. Risks that are considered to be resolved have been moved to the Appendix section of this report to provide continuity between reports.

Project Management Assessment

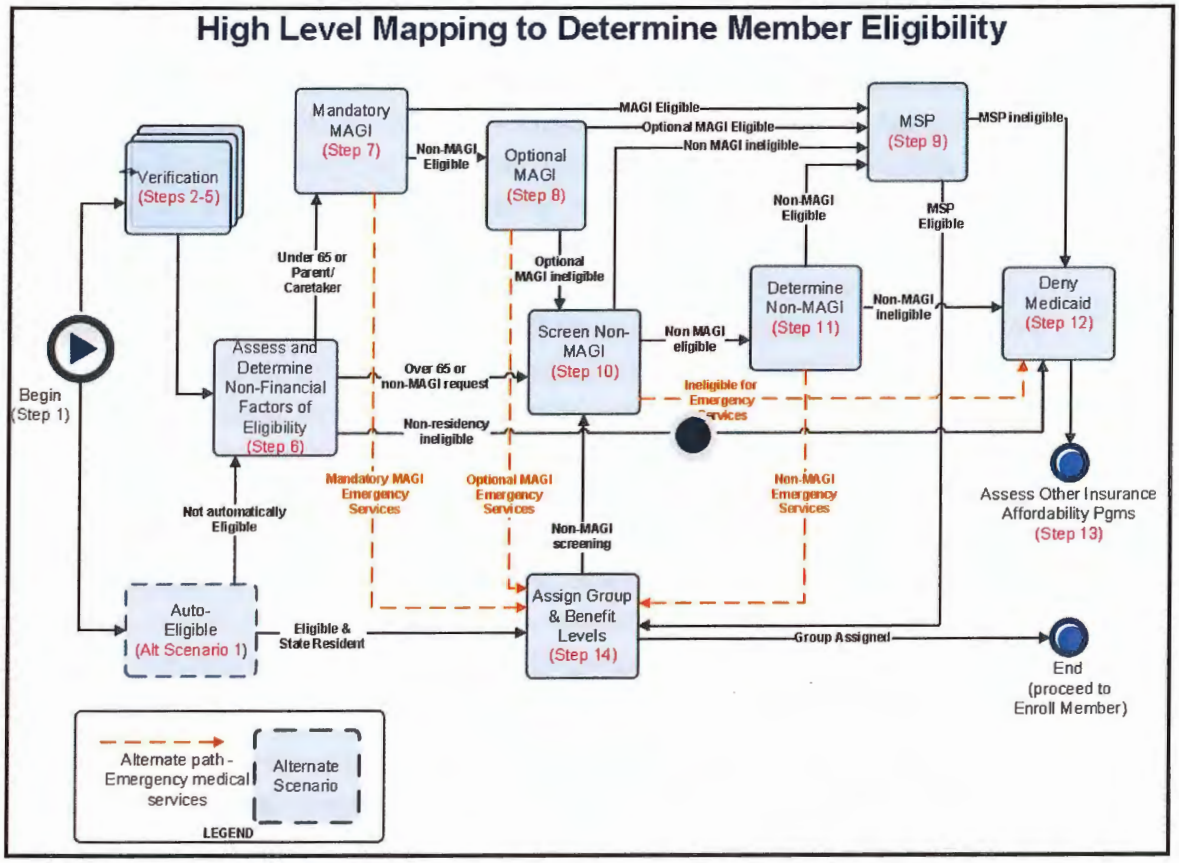
The project management of Release 2 of CT-HIX was organized and executed well by Deloitte and ahCT considering the number of parties involved. A case can be made that the effort would have benefited from improved communication between DSS and AHCT regarding tasks outside of the CT-HIX implementation. Examples include requirements and tasks needed for DSS ConneCT, a separate project by Deloitte. The SHOP vendor would have benefited greatly had testing expectations been communicated earlier. In the end, the testing went well, but required the vendor to commit greater resources because of delayed notification.

Going forward with the testing and implementation of requirements for Release 3 of CT-HIX the coordination with the DSS ConneCT project will be critical to ensure the synchronization of the two projects. Program requirements and business process synchronization is mandatory because of the need for interoperability between the two agency's staff for:

- eligibility,
- verification,
- enrollment, and
- re-determination.

An important purpose of Release 3 of CT-HIX is to implement and enhance workflows and business rules required for CT-HIX in conjunction with ConneCT to address ACA expectations. The IV&V team recommends that to ensure the level of interoperability needed between agencies, the project teams at both agencies should utilize the Medicaid eligibility determination rules defined in Appendix C – Business Process Model Details section of Medicaid Information Technology Architecture (MITA) 3.0 published in June 2013. The workflow needed to determine eligibility across the Medicaid and other programs is laid in sufficient detail to be a baseline for what needs to be in place for the two

agencies by January 1, 2014. The following graphic is taken from the Medicaid Information Technology Architecture (MITA) 3.0 published in June 2013.



Medicaid Information Technology Architecture 3.0 published in June 2013.

This coordination of projects being managed at Access Health and DSS is important enough that the IV&V Status Report will include the following section to focus on this topic.

Coordination with ConneCT

The coordination between ahCT and DSS in terms of data transmission has been well understood for some time. Granted CT-HIX was operational on October 1, but the real coordination effort begins when individuals use CT-HIX to apply for Medicaid eligibility. At that time, ahCT will be responsible for Medicaid eligibility determination. The workflow that is presented in the proceeding graphic requires thorough testing. Given the importance of the process, end-to-testing is essential. The IV&V team raised this subject as a risk (Risk 1.1) some months ago. DSS is also releasing new functionalities to its environment prior to January1. The two efforts must have regular meetings specific to the subject of synchronization of the CT-HIX and ConneCT. This synchronization concerns not only the technological components, but the business processes the technology supports.

Risk 1.1 Limited synchronization of CT-HIX requirements with ConneCT requirements

The IV&V team has been concerned with the coordination of requirements development, testing and implementation for functions that both Access Health and DSS staff share to determine eligibility and process enrollment of health plans by clients for some time. While CT-HIX and ConneCT are being implemented by Deloitte, there has not been enough coordination of the project teams across these agencies to synchronize the automation of workflow and document management functions involving tasks that require involvement by both agencies. This was caused in part by the differences in project timelines and the pressures of having to adhere to these timelines, but the lack of synchronization of these requirements has led to manual workarounds and passing tasks off to the other agency without the benefit of system support. This situation will slow down some process flows after October 1, but the impact of failing to synchronize these system requirements will be much more significant after January 1 when MAGI and other eligibility rules are implemented and the integration needs across these systems increase significantly.

October Update: The project team recently published a schedule for Release 3 of CT-HIX that includes three distinct iterations; iterations that include their own testing and implementation cycles. (See Release 3 Iteration Scope on page 22.)

Release 3 Iterations	User Acceptance Testing End Date	Implementation Date
Release 3.1	November 4	November 6
Release 3.2	November 27	December 4
Release 3.3	December 13	December 18

This approach has risks given the tight timeframe allocated. For the purposes of synchronizing ahCT functionalities with DSS ConneCT functionalities, it makes coordination more challenging. The IV&V is currently researching when the next release of ConneCT will be available to test end-to-end scenarios; specifically scenarios requiring eligibility determination processes between Access Health and DSS. This will be important to ensure that appropriate testing across the two systems is conducted.

Risk 1.1 Details and Previous Updates in Appendix

Technical Assessment Overview

The Technical Assessment of the IV&V Report is comprised of four separate reviews.

- *Technical Architecture Review* – covers infrastructure, hardware, software, and interfaces with other systems for data exchange.
- *Solutions Architecture Review* – covers solutions to ensure interoperability, operational support and change management of the service solutions components in the future.
- *Security Architecture Review* – covers ID management, authentication, authorization, role-based access management and digital signatures.
- *Technical Operational Support Capability Review* – covers change management, performance capabilities, system restoration and recovery, SLA/MOU's and training.

Technical Architectural Review

The Technical Architecture Review includes the technical infrastructure components to support CT-HIX and the interfaces with other systems for data exchange. Areas of particular interest are the Service Oriented Architecture (SOA) based infrastructure components such as the Enterprise Service Bus (ESB) and the interfaces with State systems such as the DSS Eligibility Management System (EMS) and ConneCT. The objective of this review is to ensure that the Technical Architecture and its components are logical, feasible, well documented, and adequately tested. Note that the IV&V team has identified a new finding and potential risk based on the many significant additions and changes to the technical environment supporting CT-HIX without formal architecture reviews to assess their impact.

Technical Architectural Findings:

Finding 3.9 Lack of Technical Architecture Reviews and Updates

Since the initial Technical Architecture document and corresponding diagrams for CT-HIX were developed by Deloitte and reviewed by BEST in November 2012, there have been many changes and additions without any reviews of their impact on the original architecture design or updates of the technical architecture diagrams since January 2013. These changes continued into September 2013 and made testing of the CT-HIX and its technical environment difficult. Changes to the security components in particular were made partly in response to the IRS security review, but never assessed as to the strategic impact on the overall technical architecture and its performance.

Recommendation: Access Health should have all technical architecture diagrams updated and work with Deloitte and BEST to determine the impact of the changes on the technical architecture. This architecture review should be formalized for any significant changes or additions to the technical architecture going forward.

Technical Architectural Risks:

Risk 3.1 Contingency Planning for the Technical Environments

The technical architecture and environment supporting CT-HIX is complex and new to many of the technical staff supporting it. While operational role, responsibilities and procedures are being worked out for the various organizations providing this support, consideration should be given to developing a Technical Continuity Plan with subsequent testing of that plan. This plan would address the appropriate actions necessary in various, technical outage scenarios, including; who should be notified, who is responsible for what actions, and what are the business consequences of each technical malfunction scenario. Technical Continuity testing would also ensure that the Service Registry in the Enterprise Service Bus has adequate interface expectations and remediation instructions for each interface disruption. More detail on Technical Continuity planning and testing is provided in the appendix (Findings 3.1 and 6.4).

October Update: The October 1 Go Live implementation of the Exchange portal has provided the technical support staff experience on what technical components are vulnerable and what the dependencies are between components. However, this experience is only a small subset of the overall environment and the complexities of the technical architecture supporting CT-HIX. Access Health technical staff have expressed to the IV&V team an appreciation of the value of doing a Technical Continuity Plan that formalizes contingency planning when critical components are not working properly. As things settle down for supporting the initial implementation of CT-HIX, they plan on developing and testing a Technical Continuity Plan.

Risk 3.1 Details and Previous Updates in Appendix

Solutions Architectural Review

The Solutions Architecture Review includes the proposed service solutions and their integration with other service solutions. The Solution Architecture that Deloitte is using for CT-HIX is based on the Service Oriented Architecture framework that is being utilized for the ConneCT system being developed in parallel by Deloitte. Areas of particular interest are the integration of CT-HIX solution services with the DSS application services such as document management, workflow management, the business rules engine and the call centers.

Workflow Interoperability and MITA Compliance

In addition to the above areas of interest in the Solutions Architecture Review, the IV&V team is researching the level of CMS MITA 3.0 compliance that will be required as of January 1, 2014. June 2013 updates to the CMS MITA 3.0 compliance documents includes details on the new workflow required for processing eligibility and enrollment for Medicaid benefits that may needed in CT-HIX.

Solutions Architectural Risks:

Risk 4.3 Limited Integration with ConneCT

There are several impediments that have been identified in previous IV&V Status Report findings. These speak to the level of integration between CT-HIX and ConneCT needed to provide "no wrong door" access to health benefit determination and streamlined application processing to determine eligibility and complete enrollment promptly.

Account Management - The first outcome of these impediments is the inability to implement account management across the two applications. The lack of a single-sign-on function in the State's infrastructure by October 1 is the first impediment to integrated account management. The other is the differences in the security policies for access to client information required by the ACA that AHCT is administering and those of Medicaid that DSS administers. While these policy differences are not technical, their resolution is critical to any successful eventual implementation of true single-sign-on functionality across these programs.

Streamlined Application Processing – The implementation of workflow integration between AHCT and DSS staff is somewhat limited by where DSS is today in their modernization effort. Decisions have had to be made to delay automation of some workflow functions at DSS to determine eligibility until the next phase of DSS modernization. Online access to EMS information will

not be available until the legacy EMS application is replaced. This has caused temporary workarounds that have led to more manual processing that apparently will affect the prompt activation of benefits through DSS for clients determined eligible by ahCT's automated process for MAGI clients and some processing of paperwork for verification.

This will also result in additional manual work—some for ahCT but primarily for DSS staff—resulting in significant additional costs.

October Update: It has become increasingly clear that, even in the short term, certain HIX Eligibility determinations require action by DSS before they can be resolved. These determinations will require CT-HIX and ConneCT interoperability. This situation will be compounded on January 1, 2014, when MAGI and other eligibility rules are implemented and the integration needs across these systems increases significantly. If the appropriate eligibility workflow requirements needed within and between both agencies are not developed, tested and implemented by January 1 the need for manual workarounds, staff loads and delays in processing health plans will be detrimental to the success of both agency's programs.

Risk 4.3 Details and Previous Updates in Appendix

Security Architectural Review

The Security Architecture and design approach is robust and includes comprehensive identity management and substantial, related improvements to the State's I.T. infrastructure.

With security concerns escalating for ahCT , the First Data IV&V team believes having BEST managing the CT-HIX I.T. infrastructure should work to ahCT's advantage, given the tools and experience of BEST in resisting cyber penetration and detecting hacker behaviors.

While the IV&V team has documented several security concerns in past status reports, we believe the recent review of security by the IRS has addressed them in more detail and with a high level of security requirements.

There remains the matter of data security in the reporting database that is being built in conjunction with the CT-HIX "transaction" database, and the outstanding need to manage reporting roles. Prior to October 1 the IV&V team deferred the urgency of implementing this requirement because there were only a limited number of standard "canned" reports planned initially with limited access to the data. Soon, requirements need to be developed for more custom and ad hoc reporting. These reports should include security role and

privilege assignments, along with policies to ensure privacy of the data being used in these reports.

Previous Report Security Architectural Review Findings

Technical Operational Support Capability Review

The First Data IV&V team reviewed the operations and maintenance documentation and corresponding change management methodologies to ensure the CT-HIX system is adequately supported once in production. Areas of interest include; SLA's and MOU's (with particular focus on clarity of expectations and accountability), change management capabilities and tools, restoration and recovery procedures, and adequate training of technical State staff. The objective of this review is to ensure that the CT-HIX is completely operational once in production with clear support responsibilities, operational documentation and adequate training of technical staff.

To distinguish between Operational Support business and technical issues, this section title was changed to Technical Operational Support Capability Review.

Technical Operational Support Capability Risks:

Risk 6.1 Adequate Documentation and Training for Support of the Technical Environment

Many of the technical components of the supporting infrastructure are new. There needs to be clear coordination with staff supporting these inside state services as well as outside applications and services such as the federal hub and the SHOP application. Operations and maintenance plans to date focus on the support of CT-HIX with minimal references to the operations and maintenance of the infrastructure that BEST will support or technical environments outside the state. It is unclear if the state technical staff has adequate documented procedures or will be adequately trained to support the new technologies being utilized to support CT-HIX. Written documentation would clarify the "who are you going to call" for different technical support scenarios that have not been resolved yet. They would also ensure that configuration management for the technical infrastructure components is managed properly.

Recommendation: Consideration should be given to creating a Technical Continuity Plan and testing it to verify that the technical infrastructure is ready for production and support staff knows what to do for outages, malfunctions, upgrades and configuration changes. More detail on technical continuity planning and testing is provided in the appendix (Findings 3.1 and 6.4).

October Update: The Operations Support Plan and other operations documentation are still being updated to include all components of the technical environment supporting CT-HIX. Training of BEST technical support staff is still being conducted and to some degree is being substituted with specialized support staff from the product vendors. Research is being conducted on what monitoring and configuration tools are available or are needed to document and manage this environment more proactively. The IV&V team will continue to monitor this risk.

Risk 6.1 Details and Previous Updates in Appendix

Risk 6.6 Coordinating Change Management

Originally, Solutions Architectural Risk 4.2, this risk has been moved to Technical Operational Support Capability and assigned Risk number 6.6.

The solution architecture that supports the CT-HIX application, the

infrastructure supporting it and the various supporting application services needed is complex and needs formal management to ensure the provision of services is stable and manages well. These changes include changes and fixes to application code during the system development life cycle, changes in requirements contracted for with Deloitte, upgrades to software and hardware, fixes to the software and hardware that CT-HIX is built on, changes in service providers, technology upgrades, changes to software and hardware configurations, and fixes to infrastructure components to address malfunctions and outages. With so many changes being managed and implemented by multiple parties a formal process is needed to coordinate change management across the application and technical environments.

Change management processes currently being put in place to support CT-HIX include:

- Change Control for the system requirements being implemented contractually (the Change Control Board must approve any contract addendums or change orders).
- Version control of new versions of the CT-HIX application and their fixes as they work their way through testing into production using the Deloitte System Development Life Cycle methodology.
- A configuration management plan and tool being implemented with BEST to manage hardware and software configuration changes in the infrastructure. Note that the configuration management plan assumes that BEST has formal processes in place to manage configuration changes with other changes in the infrastructure.

Change management for new versions of the CT-HIX application (including enhancements and fixes) will be more complicated if changes to the supporting infrastructure continue to be made. While the CT-HIX Change Control processes focus on the changes in the CT-HIX application, the continual changes today and in the foreseeable future in the various technical environments could jeopardize the expected functionality of the production environment unless they are formally managed on an enterprise basis. In other words, changes in the technical environment need to be better coordinated with the changes in the CT-HIX application itself.

October Update: The Coordinating Change Management Risk still needs better communication to all parties on the scope and impact of what is Change Management. Documentation in the Deloitte library on Change Management or requests by the IV&V team for other documentation on the Change

Management Process has provided only documentation on Project Change Management. This documentation states that it is a Change Control Management Plan for reviewing Change Requests, but it is primarily designed to manage major changes to the CT-HIX project requirements being implemented by Deloitte. It does not cover managing how the versions or fixes to CT-HIX releases are managed or how configuration and other changes of the technical infrastructure will be managed. The Coordinating Change Management risk was meant to include all of these forms of change to minimize impact on development, testing and operations of CT-HIX.

There were some temporary procedures put in place to require approval by Access Health IT management for changes across the application and technical environment late in the implementation of Release 2 of CT-HIX. These procedures should be formalized and communicated to all parties involved.

Originally, Solutions Architectural Risk 4.2, the risk has been moved to Technical Operational Support Capability and assigned Risk number 6.6.

Risk 6.6 Details and Previous Updates in Appendix

Testing Assessment

AHCT is scheduling a December 2013 release and a March 2014 release. During the same time period, DSS has a number of scheduled releases relating to its modernization effort. Effective January 1, ahCT will be responsible for all Medicaid eligibility determinations and redeterminations. The understanding of each agency's requirements and releases is essential in order to develop their respective testing efforts. The need for release and testing coordination can't be overstated. Bi-directional information transfer between ahCT and DSS is of paramount importance.

Both agencies need to develop their respective release plans as well as test plans in support of each release. Once these plans developed, a series of coordination sessions is worth serious consideration.

AHCT has to complete its 834 transaction testing, additional MPI testing as well as more comprehensive document management workflow testing. It is expected that during this time period process tuning and refinement will occur. These efforts will require some degree of regression testing.

AHCT's Release 3 requirements need to be documented to ensure traceability and for the development of appropriate test scenarios. There are outstanding (deferred) requirements from Releases 1 and 2 that will be addressed in Release 3. Whereas test scenarios for ahCT's earlier releases focused on the Deloitte solution, greater consideration must be given to DSS requirements when developing test scenarios. DSS needs sufficient time to review ahCT test scenarios. This is essential given the fact that DSS is relinquishing its eligibility determination process and relying solely on information edited and communicated by ahCT.

As previously mentioned, earlier releases were tested in an environment inaccessible to the Internet and where security applications were not deployed. If these constraints remain, true end-to-end testing is impossible. The additional functionalities dictated by the additional Release 3 requirements may require testing from the Internet with the security applications deployed.

Release 3 Implementation Dates

Release 3 Iterations	User Acceptance Testing End Date	Implementation Date
Release 3.1	November 4	November 6
Release 3.2	November 27	December 4
Release 3.3	December 13	December 18

Release 3 Iteration Scope

The following is a listing of expected functionalities being deployed by iteration.

Release 3.1

CR 58: Catastrophic Plans – Primary Care Required Visits

CR 63: Modify Prescription Drug Cost Sharing on Shopping Screens

CR 65: Eliminate Fields and Change Inpatient Copay per Day on Shopping Screens

CR 78: Family Annual deductible display

CR 59: Deductible Display

CR 57: Benefit Section Label Changes on Shopping Screens

PT-275 - Plan Name Change

PT-276 - Plan Variation

PT-297 – Anthem Dental URL

PT-396 – PDF changes

Release 3.2

EDI 820

CR 87: CMS EDI / 834 Changes

2 Batch Jobs

Release 3.3

CR 11: Catastrophic Coverage

CR 31: Postpone Implement Spanish Translation of website

CR 40: Change to Foster Care Screen

CR 44: Two way data transfer between ConneCT and AHCT

CR 48: AHCT Homepage changes

CR 77: Capture Race and Ethnicity in Application

CR 85: Fair Health link off Learn More page

F3.3.1.9: Special Enrollment

T10.3.11 SSO with ConneCT

Outstanding Defects

Since October 1, new defects have been identified and documented. Deloitte is working to fix, test and close these post-October 1 defects. This defect remediation effort is being closely monitored by ahCT. In subsequent monthly reports, IV&V will be providing quantitative information regarding defect numbers and severities.

As of October 1, there were open pre-production defects, the bulk of which fall under the category or Minor or Low. Regardless, IV&V has requested a plan from the vendor that details how and when they intend to fix, test and close these defects. As with the case of post-October 1 defects, IV&V will be providing quantitative information regarding defect numbers and severities in subsequent monthly reports.

Blueprint Scenario Testing

All Blueprint scenarios were submitted by their required dates in August. On September 29 and on October 5, Booz Allen Hamilton (BAH) provided feedback to the Blueprint Test Scenario submissions. The Shop vendor had prepared and uploaded a response on October 4. Deloitte is presently reviewing the comments and will be responding shortly.

User Acceptance Testing

With each CT-HIX release, complexity increases and interoperability becomes increasingly important. The same holds true for test scenarios. Whereas during previous releases, the UAT effort focused strictly primarily on the Deloitte solution, Release 3 will have an increased emphasis on the testing shared ahCT and DSS processes.

Since UAT is no longer occurring at BEST, depending upon the amount of new functionality in Release 3, the amount of spaces for testers at ahCT may be inadequate.

The JIRA/JAMA suite needs to include all business requirements for Releases 1, 2, and 3. IV&V has yet to be provided with complete traceability for Release 2, so that is still an outstanding issue as is the traceability for Release 3. IV&V will need a minimum of two JIRA/JAMA licenses to complete its responsibilities.

The test scenarios should be reviewed independently to ensure the scenarios address the respective needs of DSS and ahCT. The scenarios and the necessary test data must be agreed to by all parties prior to the start of UAT.

Testing Environment

The UAT environment used during Release 2 didn't allow for complete end-to-end performance testing of the total solution. This reality must be addressed during Release 3. The term "end-to-end" is used by both Deloitte and CMS. In both cases, true industry-defined "end-to-end" testing has not occurred. This needs to go beyond integration of

software components to incorporate infrastructure configuration yielding consistently acceptable performance for a web-based solution.

Testing Assessment Risks:

Risk 4.1 Real World UAT and Technical Testing Environment

The SOA environment that supports CT-HIX and ConneCT has many advantages in supporting service solutions from multiple sources, but it is critical that all final testing for business and technical requirements be conducted in an environment that mirrors the production services and infrastructure exactly. In the case of testing outside user functionality via the intranet and not the Internet, the risk is significant because the intranet bypasses the external firewalls and security functions that will be in place in production. This will have consequences for the results of testing business functionality as well as technical functionality.

The impact of testing in an environment that does not adequately reflect the production environment varies with the role each service performs for CT-HIX. In the case of testing outside user functionality via the intranet and not the Internet, the risk is significant because the intranet bypasses the external firewalls and security functions that will be in place in production. This has consequences for the results of testing business functionality as well as technical functionality.

On the infrastructure side of real world testing, the UAT testing of outside user requirements has started using the state's intranet instead of the Internet, this bypassing the testing of some of the key security components that will be in place to support the outside user access by the Internet. This could impact test results including performance testing. We recommend that BEST consider allowing exceptions regarding Internet testing in the Staging environment and that Access Health conduct running a pilot of the CT-HIX application in the Production environment before going live.

This risk was originally in the Solutions Architecture Section and therefore we are using that reference number.

October Update: In preparation for Release 3 and 4, IV&V needs to be more involved than was permitted in Release 2. The team understands the limitations present during Release 3, but given the criticality of Release 3 functionalities as well as the impending January 1 go-live date, IV&V needs to be permitted to review the test scenarios intended for execution in Release 3.

Risk 4.1 Details and Previous Updates in Appendix

Previous UAT Findings

Performance Testing

The purpose of performance testing is to validate the responsiveness, reliability and throughput of the CT-HIX application in the shared technical environment based on various workload scenarios. Adequate workload stressing of the shared technical environment will be critical because of the additional workload by ConneCT users on some components of the infrastructure when it goes into production. The primary question being: *how will CT-HIX perform during these workload scenarios?*

Adequate workload testing requires an estimate of peak loads on the shared environment as well as average or typical loads on the systems. Workload testing would ensure adequate throughput capability during peak hours of outside and inside user usage.

It is also important that performance testing be conducted in a test environment that reflects all components of the production environment, including the security components required to support outside Internet access to CT-HIX.

Previous Report Performance Test Findings

Reference Material Listing

The following table contains the documents reviewed by the IV&V team. The left-hand column identifies the IV&V Project Status Report area and the right-hand column contains the document citation.

Report Area	Document Citation
Project Management	Weekly IT PowerPoint Presentations KPMG Weekly Operations PowerPoint Presentations KPMG Excel spreadsheet containing identified requirements and requirement-to-testing information
Technical Review	Affordable Care Act (ACA) System Security Plan (SSP) Approach 12/06/13 – Deloitte AHCT FDDR Design Review Presentation to CMS 3/27/13 - KPMG Contingency Recovery Plan version 1.0 04/19/13 – Deloitte CT HIX Component Level Security Roles Matrix Technical Design Document version 1.0 03/15/12 – Deloitte CT HIX Front End – Administration Functionality and Task Workflow Design Document version 1.0 03/15/13 - Deloitte CT HIX Security Solution Design version 1.0 03/15/13 – Deloitte CT-HIX Application Framework TDD v1.0 3/15/13 CT-HIX Batch Jobs TDD v1.0 3/15/13 CT-HIX Contingency/Recovery Plan v1.0 4/19/13 CT-HIX Corticon Business Rules TDD v1.0 3/15/13 CT-HIX Data Management Plan v1.0 3/15/13 CT-HIX Document Management and Notices Technical Design version 1.0 03/15/13 – Deloitte CT-HIX Eligibility – Supplemental Sources Interface Control Document version 1.0 02/08/13 - Deloitte CT-HIX Enrollment and Enrollment Processing TDD v1.0 3/15/13 CT-HIX Enrollment Interface Control Document version 1.0 02/08/13 – Deloitte CT-HIX Financial Management Interface Control Document version 1.0 02/08/13 – Deloitte CT-HIX Front End Individual Account Management TDD v1.0 3/15/13 CT-HIX Implementation Plan v2.0 4/24/13 CT-HIX Interfaces Eligibility Supplemental Sources Technical Design 4/15/13 CT-HIX Master Person Index TDD v1.0 3/15/13 CT-HIX Organizational Readiness Plan v3.0 3/14/13 CT-HIX Organizational Readiness Plan version 1.0 03/14/13 - Deloitte CT-HIX System Architecture Design v2.0 04/03/13 CT-HIX Technical Design Eligibility-Supplemental Sources TDD v1.0 3/15/13

Report Area	Document Citation
	CT-HIX Technical Design Overview and Application Framework 03/15/13 CT-HIX Transition and Knowledge Transfer Plan 04/24/13 Data Exchanges and Interfaces Design Review 12/19/13 – Deloitte Implementation Plan version 2.0 04/24/13 – Deloitte Privacy Security Timelines for IRS version 1.0 April 2013 – CMS Security Plan version 2.0 01/17/12- Deloitte SIT Test Plan version 2.0 04/30/13 SIT Test Plan version 2.0 04/30/13 - Deloitte System Architecture Design version 2.0 04/03/13 – Deloitte System Architecture Design version 2.0 04/03/13 – Deloitte Technical Architecture Document for BEST SDM November 2012 - Deloitte Technical Design Overview 03/13/13 – Deloitte Training Plan version 1.0 03/29/13 – Deloitte Transition and Knowledge Transfer Plan version 2.00 4/24/13 – Deloitte DSS-HIX System Workflows – Final Version 6/28/13 Final CT-HIX Eligibility Business Rules (Business Systems Design) V4 6/28/13 CT-HIX Front End: Individual Account Management (Business Systems Design) V4 6/28/13 CT-HIX 27-R1 Operations and Maintenance Manual V 2 6/21/13 CT-HIX R2 Implementation Plan V3 6/21/13 CT-HIX System Architecture Design V2.1 6/21/13 CT-HIX Contingency/Recovery Plan (all releases) V2 5/30/13 CT-HIX Integrated Requirements Plan for release 2 V2 CT-HIX Security Plan V2 7/1/13 CT-HIX R2 SIT Plan V2 7/10/13 CT-HIX Contingency/Recovery Plan v3.0 7/08/13 CT-HIX System Architecture Design v2.1 7/3/13 CT-HIX Configuration Management Plan v2.1 8/6/13 CT-HIX Operation Support Plan v2.0 7/2/13 CT-HIX R2 Integrated v2 7/8/13 CT-HIX R2 Implementation Plan v3 7/24/13 CT-HIX SSP Workbook 7/9/13 R2 BEST Playbook Master 7/30/13 IBM Service Registry and Repository 7/30/13 Technical Review Board – Design Document 7/30/13 CT-HIX Technical Design Overview and Technical Framework TDD V2 8/21/13 CT-HIX R2 Operation Support Plan v1.0 9/11/13

Report Area	Document Citation
Test Effort Activities	Wave 1 Connecticut State based Exchange FD Test Plan, CMS FDSH Wave 1 Test Strategy March 2013, Deloitte Wave 1 Test Readiness review sign off Check list, CMS Wave 1 Testing Progress, April 2, 2013 and Wave 1 Testing Progress, April 3, 2013, Deloitte Connecticut Daily Defect Tracking Report, CMS FEPS Formal State Testing- Wave 1 CT Test Summary Report, CMS CT HIX Testing Overview submitted 04 10 2013, Deloitte AHCT FDDR Presentation-Design Review, Deloitte March 27- 28th 2013 042313 AHCT ITPMO PowerPoint presentation, KPMG 25 R1 SIT Test Plan_SIT_Plan_Management_Defects_05022013 Testcase_register_R1_v4, Deloitte CT_SBE_to_FEPS_application_Data_3-1-2013, CMS Deloitte System Integration Summary Test Findings CT-HIX R2 SIT Plan V2 7/October 13

Appendix A. Previously Identified Findings (Open)

Date	Area Name	Risk/ Finding Identifier	Statement
	Project Management Assessment	Risk 1.1	**Limited synchronization of CT-HIX requirements with ConneCT requirements** The IV&V team has documented concerns with the coordination of requirements development, testing and implementation for functions that both Access Health and DSS staff share to determine eligibility and process enrollment of health plans by clients. While CT-HIX and ConneCT are being implemented by Deloitte, there has not been enough coordination of the project teams across these agencies to synchronize the automation of workflow and document management functions involving tasks that require involvement by both agencies. This was caused in part by the differences in project timelines and the pressures of having to adhere to these timelines, but the lack of synchronization of these requirements has led to manual workarounds and passing tasks off to the other agency without the benefit of system support. This situation will slow down some process flows after October 1, but the impact of failing to synchronize these system requirements will be much more significant after January 1 when MAGI and other eligibility rules are implemented and the integration needs across these systems increase significantly. **October Update:** See latest update
5/13	Project Management Assessment	Finding 1.1	The process of migrating requirements into the application design for traceability is on-going. There have been some internal project concerns brought to the attention of the IV&V team that the task of traceability to functionality is unfinished with additional concerns about the correctness of the traceability. The IV&V team is reviewing recently provided new requirements traceability and design documentation. Based upon our reviews, recommendations may follow if warranted. **June Update:** KPMG has for some time been raising a concern about the reasonability, accuracy and completeness of the requirement traceability effort that was undertaken by Deloitte. After a series of meetings, Deloitte has brought forth a new schedule for completing the requirement traceability mapping. The final traceability documentation is scheduled to be completed by June 20th. At that time IV&V will be reviewing the final documentation. Deloitte is already producing interim deliverables which indicate that a number of KPMG's concerns are being addressed. **July Update:** IV&V was provided an update requirement traceability documents during the week of July 8th. The document references only those requirements being addressed by Deloitte.

Date	Area Name	Risk/ Finding Identifier	Statement
			IV&V has been reviewing traceability and test mapping. IV&V has reached out to Maximus and HealthPass to be provided with the requirements that the vendors were basing their solution on. In both cases, the requirements provided by the vendors were the requirements provided by AccessHealth to vendors during the proposal process. In both instances, IV&V believes additional requirements have been identified during contract negotiations and during the DDI phase of the project. IV&V has requested additional meetings with both vendors to address our concerns. In the case of HealthPass, IV&V has also reached out to bswift (HealthPass's technical partner) to see the requirements they've been provided. IV&V would like to see greater transparency into the SHOP solution. This will be a topic of our discussions with HealthPass as we refine our testing plan for SHOP. **August Update:** Deloitte continues to update the traceability matrix and expects to complete the updating no later than August 26th. The IV&V team is concerned that this update will still be incomplete because the Business Systems Documents (BSD) and the Technical Design Documents (TDD) have not been completed or accepted yet. There is serious concern that developing a final traceability matrix of requirements may not happen until late in the UAT testing period. Verifying traceability of requirements is further complicated because of the lack of a single comprehensive BSD or TSD to verify from. In the case of HealthPass, the IV&V team believes that bswift traceability is forthcoming from bswift. The IV&V team has had several discussions with HealthPass regarding documentation of their business processes, test plan and UAT. Risk 7.1 contains greater details concerning IV&V's concerns regarding HealthPass's capabilities to comply with the IV&V team's need for adequate documentation. **September Update:** HealthPass has submitted a number of documents to AccessHealth relating to the business processes it executes. Deloitte has also been uploading a number of documents into its library. **October Update:** Deloitte is in the process of updating the Business System Design documents (BSDs) relating to the functionalities within Release 3. IV&V has requested a list of the BSDs that Deloitte intends to update.
5/13	Project Management Assessment	1.2	There is concern regarding the amount of time and effort spent on the completion and acceptance of documentation deliverables. Deloitte has responsibility for the delivery of several project deliverables; responsibilities including presenting a deliverable that has been through their internal Q&A process. KPMG is responsible for executing the deliverable review process. In late April, there were 21 deliverables that had not been accepted. Many of these deliverables have direct bearing on current development efforts. The IV&V team has identified this bottleneck

Date	Area Name	Risk/ Finding Identifier	Statement
			as a risk and provides an associated recommendation below. **August Update:** IV&V will continue to monitor the document delivery and acceptance process. **September Update:** Deloitte has uploaded a number of documents into its library this past month. AccessHealth has not accepted the documents, but is in the process of reviewing them. **October Update:** Deloitte is in the process of updating the BSDs relating to the functionalities within Release 3.
5/13	Project Management Assessment	1.4	Business Continuity documentation wasn't found during our initial review. This documentation is an essential component in supporting the business expectations of AHCT. Disaster Recovery documentation is present, but it lacks the specificity necessary to fully support the system. **June Update:** IV&V has verified this finding and recommends a comprehensive business continuity plan be developed. **August Update:** AHCT is working on a Business Contingency Plan as part of their Operational Readiness planning. Please refer to Risk 3.1 for additional updates regarding technical contingency planning. **September Update:** No update **October Update:** No update
6/13	Project Management Assessment	1.10	Beginning in early May, it became apparent that 100% of the necessary functionality expected to be delivered by the system integrator by May31st was not going to be met. An agreement was struck to deliver 90% of the expected functionality by May 31st and the remaining 10% by June 14th. Since the time of the agreement, weekly updates have continued to show slippage, far exceeding the expected 10%. A comprehensive plan was presented to AHCT by Deloitte that addresses the slippage. First Data has requested a copy of the plan as well as the most recent project plan and will report its finding in the July IV&V Status Report. **July Update:** The solution proposed by Deloitte was accepted by AHCT and is now reflected in the Master Project Plan. All indications are the Deloitte development effort is now on track, based on the updated plan. **August Update:** Deloitte is adhering to the update project plan. IV&V will continue to monitor in that there are scheduled releases in December, 2013 and March 2014. Another reason for monitoring has to do with the fact that all Deloitte releases may impact the on-going modernization efforts at DSS.
Return to Project Management Assessment			
5/13	Technical	2.6	The proposed technical environment is complex, with many pieces

Date	Area Name	Risk/ Finding Identifier	Statement
	Assessment Overview		being built in parallel. This could lead to differences in technical design that may affect interoperability between CT-HIX and ConneCT. **June Recommendation:** Even though there are only two agencies (AHCT and DSS) now using or planning to use this SOA environment, more HHS-related agencies could leverage these two solutions in the future, and putting a process in place now is highly advised, even if for now it is just used to coordinate changes to CT HIX and ConneCT. **August Update:** This finding is being addressed in Risk 4.2 Coordinating Change Management. **September Update:** Access Health is in the process of setting up a change management governance process that will address the coordination of changes in the SOA infrastructure with changes in the CT-HIX application. We recommend that a similar governance process be put in place that includes DSS (for ConneCT) and all agencies sharing this technical environment in the future. **October Update:** The impact of implementing in parallel the technical environments supporting CT-HIX and ConneCT on interoperability between systems has been relatively minimal to date, but will be more of an issue on January 1, 2014. The Technical Architecture Review Section of this report has added a new finding that recommends an architecture review to assess this impact
5/13	Technical Assessment Overview	2.7	The complexity of the technical environment will also require closely managed testing between CT-HIX and ConneCT in a testing environment that accurately reflects production - this may affect the very tight project delivery schedule. **June Recommendation:** Given the complexity of the technical environment, First Data suggests the development of a Technical Continuity Plan (TCP), to accompany the Business Continuity Plan (BCP). **October Update:** This finding is being taken up by Risk 4.1 Real World UAT and Technical Testing Environment which is now being tracked in the Testing Assessment section of this report.

Return to Technical Assessment Overview

Date	Area Name	Risk/ Finding Identifier	Statement
	Technical Architectural Review	3.1	**Contingency Planning for the Technical Environments** The SOA technical architecture environment will require synchronization of actions within and between the following: 1. Access Health CT and the CT-HIX solution 2. Department of Social Services and the ConneCT solution 3. CT DAS BEST for shared Internet and Security services as well as for the underlying infrastructure for solutions 1&2 above (processing / storage / interagency network) 4. HealthPass and its infrastructure and applications 5. Xerox and its CT DSS HUSKY services 6. Maximus and its Call Centers (especially off-site) 7. Federal Hub and its various service interfaces Many of the CT-HIX functions at the customer and staff level will require successful operation of these technical environments and their interfaces. The contingency planning that is being developed to ensure business continuity for CT-HIX operations must include technical contingency planning for what happens when technical component of these environments malfunction. While a technical malfunction will require a business work-around, thought needs to be given to what the technical staff must do in each circumstance of system failure. **Impact**: If there is an outage or interruption in any of the technical environments involved with supporting the Exchange it is important that the technical support staff know what to do to resolve the system malfunction, and how to successfully recover operations in the shortest time possible to restore services. **Recommendation:** Consideration should be given to developing a Technical Continuity Plan with subsequent testing of that plan. This plan would address the appropriate actions necessary in various technical outage scenarios, including; who should be notified, who is responsible for what actions, and what are the business consequences of each technical malfunction scenario. Technical Continuity testing would also ensure that the Service Registry in the Enterprise Service Bus has adequate interface expectations and remediation instructions for each interface disruption. More detail on Technical Continuity planning and testing is provided in the appendix (Findings 3.1 and 6.4). **August Update:** The Release 2 Operations and Maintenance Plan is still being developed with participation from ahCT, Deloitte, KPMG and BEST staff. While the Release 1 Operations and Maintenance Plan did not address this risk completely, the IV&V team is hopeful that its recommendations will be fully addressed in

Date	Area Name	Risk/ Finding Identifier	Statement
			the Release 2 plan. The IV&V team has not seen any evidence of our recommendation to develop a Technical Continuity Plan being implemented yet. Given the tight timeframes of the CT-HIX project, the recommendation to test different technical outage scenarios may not be practical by the October 1 production date. However, we still recommend that it be considered for implementation by January 1, 2014 to ensure contingencies for various technical outages have been addressed before they occur. **September Update:** The R 2 Operations and Maintenance Plan was updated to include additional procedures for recovery and restoration of the CT-HIX application and the batch processes that support it. There still are no recovery and restoration procedures for the following components of the technical environment being implemented to support CT-HIX: Websphere Application Server (WAS), HTTP (portal content), the Enterprise Service Bus, the TIBCO Patterns and Informatica. **October Update:** The Access Health technical management is now planning on developing a Technical Continuity Plan. This will be part of improving documentation of operations and monitoring capabilities for the technical environment supporting CT-HIX.
			See latest update
5/13	Technical Architectural Review	3.2	Interfaces with systems inside and outside the State need to be clearly defined in terms of interface standards, number and type of data requests and their performance impacts on the network and these systems, and the security of data exchanged. Many of these interfaces still need to be defined and contracted for via Service Level Agreements (SLA's) and MOU's. **June Update:** We are waiting for the completion of documentation on interface standards and the Service Level Agreements being contracted for service delivery. **Recommendation:** We recommend that documentation of interfaces and their standards be completed soon so that adequate testing scenarios and support roles for operational support are clear and can be tested. We also recommend the testing of interfaces and this operational support be done via Technical Continuity Testing. **August Update:** This finding is being addressed in Risk 4.1 Real World UAT and Technical Testing Environment and Risk 3.1 Contingency Planning for the Technical Environments.
5/13	Technical Architectural Review	3.3	The interface with the DSS EMS system is of particular concern because the need for many "real time" calls for data are being requested of a system that was designed primarily for batch data interfaces. The EMS technical support staff at DSS is already

Date	Area Name	Risk/ Finding Identifier	Statement
			stretched because of retirements and the difficulty to find trained IMS COBOL staff to replace them. **June Update:** At the 5/22 meeting with Deloitte, the issue of "real time" calls was brought up. Deloitte assured us that they would minimize the impact on EMS in the Tier 1 design by leveraging a "real time" call that is in existence for ConneCT. **Recommendation:** First Data believes that the project would benefit from additional documentation being published that details how what appears to be real-time calls to the EMS database are to be executed without impacting the current "limited" support of EMS by DSS. **August Update:** This finding is being addressed by Risk 4.3 Limited Integration with ConneCT.
5/13	Technical Architectural Review	3.5	The implementation of the CT-HIX and ConneCT systems on the same Enterprise Service Bus (ESB) platform needs to be carefully planned and implemented or the capabilities of the SOA approach will not be leveraged, and could in fact become unnecessarily more complex to use and support. **Resolution:** This finding will continue to be tracked by IV&V. **August Update:** It is also being tracked as part of Risk 3.1 Contingency Planning for the Technical Environments.
5/13	Technical Architectural Review	3.7	The internal interfacing between the Batch Ingestion Services for CT-HIX and ConneCT, the workflow rules in separate areas of the FileNet Content Engine and the workflow rules in the shared Corticon Business Rules Engine, and the eligibility rules in the "backend" could make routing of documents and workflow between HIX and DSS workers more difficult to implement and manage over time. It will also require careful testing between systems and well documented restoration and recovery procedures. This will be explored more in the following Solutions Architecture and Operations Capability Review sections. **Resolution:** The first concern of this finding will be addressed in the Change Management Potential Risk. The second part of this finding (testing) will be addressed in the Potential Testing Risk. **August Update:** This finding is being addressed in Risk 4.3 Limited Integration with ConneCT and Risk 6.1 Adequate Documentation and Training for Support of the Technical Environment.
5/13	Technical Architectural Review	3.8	The complexity of managing ID security in multiple places with multiple products should be looked at closely to ensure true seamless "No Wrong Door" functionality between CT-HIX and ConneCT systems. While the Security Plan is very detailed, the complexity of the environment will make having a single client ID across systems difficult. This concern will be also discussed in the Security Architecture Review section.

Date	Area Name	Risk/ Finding Identifier	Statement
			Resolution: The concerns in this finding will be addressed in the Security Architecture Review section under 5.2. **August Update:** This finding is being addressed in Risk 4.3 Limited Integration with ConneCT, Risk 3.1 Contingency Planning for the Technical Environments and Risk 5.1 Security Policy.
Return to Technical Architectural Review			
	Testing Assessment Review	4.1	**Real World UAT and Technical Testing Environment** The SOA environment that supports CT-HIX and ConneCT has many advantages in supporting service solutions from multiple sources, but it is critical that all final testing for business and technical requirements be conducted in an environment that mirrors the production services and infrastructure exactly. There are several service solutions being finalized such as the services provided by the Federal Hub. A harness is being used in conjunction with the hub to mimic the service interface. This dependence on mimicking the interfaces and results required for service delivery could have significant impact on the UAT testing currently being conducted. On the infrastructure side, the current plan to conduct UAT testing in a Staging environment that allows testing only from the intranet and not via the Internet is an example of testing in an environment that does not reflect production. In the case of testing outside user functionality via the intranet and not the Internet, the risk is significant because the intranet bypasses the external firewalls and security functions that will be in place in production. This will have consequences for the results of testing business functionality as well as technical functionality. **Impact:** The impact of testing in an environment that does not adequately reflect the production environment varies with the role each service performs for CT-HIX. In the case of testing outside user functionality via the intranet and not the Internet, the risk is significant because the intranet bypasses the external firewalls and security functions that will be in place in production. This will have consequences for the results of testing business functionality as well as technical functionality. **Recommendation:** In the case of testing the security services of BEST, one option is to change current BEST practices to allow testing via the Internet to the environment currently be used for UAT. Another option is to conduct final UAT in the unused production environment as pilot testing before going live on October 1. **August Update:** The services provided by the Federal Hub which are still being "mimicked". The anticipated date for the harness's

Date	Area Name	Risk/ Finding Identifier	Statement
			removal is August 26th. At the August 1st. CMS meeting it was mentioned that ahCT may have to "pilot" the application using the "unyoked" version of the Federal Hub immediately before the actual Go Live production cutover. If the Federal Hub services are not made available until this late in the testing process we recommend that contingency planning be completed and formalized for how to process applications through the Health Exchange without these services. On the infrastructure side of real world testing, the UAT testing of outside user requirements has started using the state's intranet instead of the Internet, this bypassing the testing of some of the key security components that will be in place to support the outside user access by the Internet. This could impact test results including performance testing. We recommend that BEST consider allowing exceptions regarding Internet testing in the Staging environment and that Access Health conduct running a pilot of the CT-HIX application in the Production environment before going live. **September Update:** Although BEST has not formally changed its policy regarding not testing in the Staging technical environment, the end-to-end testing of the Federal Hub is being conducted within this environment. This provides the outside Internet access that is not available in the UAT environment. However, the other UAT testing continues to be conducted in the UAT environment with outside access being provided through VPN tunneling into CT-HIX without any testing of the security functions that will be used by outside users once in CT-HIX is in Production. In addition, the document management and workflow functionality has not been tested adequately in the UAT environment because the FileNet servers needed are not connected in the UAT environment. **Recommendation:** The IV&V team recommends that the testing of functions of outside users to CT-HIX be conducted in the Staging environment immediately because this environment is the only place outside of Production that real world testing can be conducted at this time. Note that this assumes that the final additions and configurations to the infrastructure components be completed in Staging.
			See latest update

Date	Area Name	Risk/ Finding Identifier	Statement
	Solutions Architectural Review	Risk 4.3	**Limited Integration with ConneCT** There are several impediments that have been identified in previous IV&V Status Report findings that speak to the level of integration between CT-HIX and ConneCT needed to provide "no wrong door" access to health benefit determination and streamlined application processing to determine eligibility and complete enrollment promptly. Account Management - The first outcome of these impediments is the inability to implement account management across the two applications. The lack of a single-sign-on function in the State's infrastructure by October 1 is the first impediment to integrated account management. The other is the differences in the security policies for access to client information required by the ACA that AHCT is administering and those of Medicaid that DSS administers. While these policy differences are not technical, their resolution is critical to the successful eventual implementation of true single-sign-on functionality across these programs. Streamlined Application Processing – The implementation of workflow integration between AHCT and DSS staff is somewhat limited by where DSS is today in their modernization effort. Decisions have had to be made to delay automation of some workflow functions at DSS to determine eligibility until the next phase of DSS modernization because online access to EMS information will not be available until the legacy EMS application is replaced. This has caused temporary workarounds that have led to more manual processing that apparently will affect the prompt automated determination of eligibility for MAGI clients and some processing of paperwork for verification. This will also result in additional manual work, some for AHCT but primarily for DSS staff, resulting in significant additional costs. **August Update:** While the implementation date of single-sign-on functionality has not been determined, sooner would be better than later. The longer it takes to enable this function the more difficult it will be to implement, because of the need to transition clients with two account access codes to one in the future. Improving workflow integration with ConneCT depends on the next phase of modernization of DSS (Tier 2) which is in the planning process at this time. In the meanwhile DSS, AHCT and KPMG are working on single stream processing of applications to minimize delays and manual intervention. Planning for Tier 2 of DSS modernization will include requirements to expedite the workflow functionality needed to support integration with Ct-HIX and AHCT staff. Given the likelihood at this point that these impediments to

Date	Area Name	Risk/ Finding Identifier	Statement
			integration with ConneCT will not be resolved by October 1 the IV&V team will continue to monitor the impact this risk will have on eligibility determination. **September Update:** It has become increasingly clear that, even in the short term, certain HIX Eligibility determinations require action by DSS before they can be resolved. These determinations will require CT-HIX and ConneCT interoperability. This situation will be compounded on January 1st, 2014 when MAGI and other eligibility rules are implemented and the integration needs across these systems increases significantly. If the appropriate eligibility workflow requirements needed by both agencies are not developed, tested and implemented by January 1 the need for manual workarounds, staff loads and delays in processing health plans will be detrimental to the success of both agency's programs.
			See latest update
5/13	Solutions Architectural Review	Finding 4.3	Currently it appears that the workflow design will require AHCT and DSS workers to rekey the data embedded in forms as opposed to using forms management software to pre-populate the CT-HIX and EMS screens. It is unclear to IV&V if this is only temporary for the initial Tier 1 implementation. **Recommendation:** A forms management software package that aids the extraction of data from paper forms should be considered in future versions of the application. This would allow for the automatic extraction of data from the form for onscreen verification by staff. It is our understanding that this topic has been discussed internally and it was determined that, at the present time, automation of data entry into EMS is not practical. **July Update:** This finding will be tracked as Risk 4.3 Limited Integration with ConneCT.
5/13	Solutions Architectural Review	4.6	There are separate Deloitte teams working on the two projects with different constraints and timetables so keeping these two projects in synch given the tight timetables for both projects will be difficult. It will also be difficult to plan and implement the needed integration of functions between CT-HIX and ConneCT. If CT-HIX goes ahead too far with implementing their system to meet timelines without sufficient planning and testing with the ConneCT system the advantages of sharing technical architecture could be diminished and require extra time and effort to rebuild components or services prior to planned future changes such as the replacement of the DSS Eligibility Management System (EMS). **August Update:** The IV&V team requested documentation from Deloitte on how they will coordinate the requirements and deliverables between the AHCT and DSS projects. We have not received any documentation to date. The need to synchronize

Date	Area Name	Risk/ Finding Identifier	Statement
			these two projects seems to be impacting DSS more than ahCT, but we will continue to request the documentation on Deloitte's project management methodology to ensure minimum impact on CT-HIX functionality. **September Update:** This finding will be tracked as Risk 1.1 Limited synchronization of CT-HIX requirements with ConneCT requirements.
5/13	Solutions Architectural Review	4.7	Integration requirements between the document workflow rules, staff workflow rules, the eligibility rules between CT-HIX and ConneCT systems, and ID management is still being defined. This integration of internal system services will be critical to providing a seamless client experience and staff support environment when both systems are being utilized. Requirements and workflow issues need to be resolved soon to ensure adequate time to implement and test this integration of services. **June Update:** Some of the system design requirements that require integration and interoperability between CT-HIX and ConneCT are still be finalized and approved. **Recommendation:** The impact on the seamless client experience should be assessed closer once these design requirements are finalized. The testing scenarios should also be assessed at that time to ensure adequate testing of client and staff functions across these systems. **August Update:** This finding is being addressed in Risk 4.3 Limited Integration with ConneCT.
Return to Solutions Architectural Review			
Return to Security Architectural Review			
	Technical Operational Support Capability Review	6.1	**Adequate Documentation and Training for Support of the Technical Environment** Many of the technical components of the supporting infrastructure are new and there needs to be clear coordination with staff supporting these inside state services as well as outside applications and services such as the federal hub and the SHOP application. Operations and maintenance plans to date focus on the support of CT-HIX with minimal references to the operations and maintenance of the infrastructure that BEST will support or technical environments outside the state. It is unclear if the state technical staff has adequate documented procedures or will be adequately trained to support the new technologies being utilized to support CT-HIX. This would clarify the "who are you going to call" for different technical support scenarios that has not been resolved yet. It would also ensure that configuration management

Date	Area Name	Risk/ Finding Identifier	Statement
			for the technical infrastructure components is managed properly. **Impact**: Unless the state technical support staff has adequate training and documentation for operational support and maintenance before the October 1 production dates there is a risk that recovering from the various forms of outages or system errors will not be coordinated and take longer to recover from then necessary. **Recommendation:** Consideration should be given to creating a Technical Continuity Plan and testing it to verify that the technical infrastructure is ready for production and support staff knows what to do for outages, malfunctions, upgrades and configuration changes. More detail on technical continuity planning and testing is provided in the appendix (Findings 3.1 and 6.4). **August Update:** The Release 2 version of the Operations and Maintenance Plan is currently being developed in conjunction with BEST staff. The IV&V team has requested a copy of the draft Plan to determine if it is more thorough than the Release 1 O&M Plan. The IV&V team has also been assured by BEST Operations management that their technical staff received several levels of training for the new components they will be supporting. AccessHealth has instituted a notification process for external and internal incidents. Maximus will be handling all incident calls. AccessHealth will be notified electronically (email, smartphones) Incident tickets will then be triaged by the AccessHealth team and the appropriate team(s) notified. A separate instance of JIRA has been created specifically to retain and track these incidents. Plans are underway for utilizing the BMC Software suite (Numara) by June 2014. This tool suite is currently being utilized and well-understood by Best. Incident notification and tracking are suite components. **September Update**: The Operations and Maintenance Manual has been updated and an Operations Support Plan has been recently published in the Deloitte library. Both of these documents provide useful O&M documentation, but are incomplete. The Operations and Maintenance Manual does not have clear roles and responsibilities for the technical components and some of the technical sections have no documentation for providing guidance on maintaining the technical components that have been implemented specifically to support CT-HIX. The Operations Support Plan documents the incident reporting procedures between Tier 0 and 3 graphically which should help track incidents and resolutions across the technical and application environments. Neither document contains adequate procedures on recovery and restoration procedures. The only other operation documentation related to this is the Contingency Recovery Plan, but this addresses recovery procedures for a full disaster such as moving the data

Date	Area Name	Risk/ Finding Identifier	Statement
			center functions to another data center and does not address procedures for more typical outages and system malfunctions.
			See latest update
5/13/2013	Technical Operational Support Capability Review	6.2	Change management processes and controls need to be put in place for all components of the CT-HIX and ConneCT systems, not just for the application software. IV&V would like to see more documentation supporting that this is being adequately addressed. **June Update:** The change control process for approving changes to the requirements of the original Deloitte statement of work for CT-HIX is still being finalized. Processes for managing fixes to the first release of the CT-HIX system while development of release 2 is being completed and put in place is still being worked out. BEST has requested a process for implementing system changes during the testing process. It is our recommendation that an Operational Plan needs to be put in place to manage changes to the CT-HIX system, changes to systems and services that it interfaces with and changes to the infrastructure that supports it once CT-HIX is in production. **Recommendation:** First Data recommends that change management during development, testing and after production be looked at holistically to ensure that CT-HIX is successfully implemented on schedule and into the future. Change management referenced in the Deloitte technical documents focuses primarily on change control of requirements and enhancements of the system being built. With so many parties involved in managing changes, strong change management leadership is essential. **July Update:** This finding will be tracked as Risk 4.2 Coordinating Change Management.
5/13/2013	Technical Operational Support Capability Review	6.3	An SOA environment such as the federated (multi-agency) environment proposed should have an SOA governance process involving all agencies to ensure its success in the future (industry best practices). **Recommendation:** Even though there are only two agencies (AHCT and DSS) now using or planning to use this SOA environment, more HHS-related agencies could leverage these two solutions in the future, and putting a process in place now is highly advised, even if for now it is just used to coordinate changes to CT HIX and ConneCT.

Date	Area Name	Risk/ Finding Identifier	Statement
10/16/ 2013	Technical Operational Support Capability Review	6.6	**Coordinating Change Management** Originally, Solutions Architectural Risk 4.2, this risk has been moved to Technical Operational Support Capability and assigned Risk number 6.6. The solution architecture that supports the CT-HIX application, the infrastructure supporting it and the various supporting application services needed is complex and needs formal management to ensure the provision of services is stable and manages well. These changes include changes and fixes to application code during the system development life cycle, changes in requirements contracted for with Deloitte, upgrades to software and hardware, fixes to the software and hardware that Ct-HIX is built on, changes in service providers, technology upgrades, changes to software and hardware configurations, and fixes to infrastructure components to address malfunctions and outages. With so many changes being managed and implemented by multiple parties a formal process is needed to coordinate change management across the application and technical environments. Change management processes currently being put in place to support CT-HIX include: • Change Control for the system requirements being implemented contractually (the Change Control Board must approve any contract addendums or change orders). • Version control of new versions of the CT-HIX application and their fixes as they work their way through testing into production using the Deloitte System Development Life Cycle methodology. • A configuration management plan and tool being implemented with BEST to manage hardware and software configuration changes in the infrastructure. Note that the configuration management plan assumes that BEST has formal processes in place to manage configuration changes with other changes in the infrastructure. There are no change management processes that we are aware of to manage upgrades and fixes to hardware and software in the BEST technical infrastructure or changes being made in other supporting technical environments such as Health Pass (bswift) or Maximus. **Impact:** Change management for new versions of the CT-HIX application (including enhancements and fixes) will be more complicated if changes to the supporting infrastructure continue to be made. While the CT-HIX Change Control processes focus on the changes in the CT-HIX application, the continual changes today and in the foreseeable future in the various technical environments

Date	Area Name	Risk/ Finding Identifier	Statement
			could jeopardize the expected functionality of the production environment unless they are formally managed on an enterprise basis. In other words, changes in the technical environment need to be better coordinated with the changes in the CT-HIX application itself. **August Update:** There has not been an update on how configuration management will be accomplished in this environment since December or whether these configuration management tools have actually been installed and the staff trained in their use. How configuration management will be conducted in conjunction with changes to the CT-HIX application or other infrastructures supporting CT-HIX has not been addressed, but should be part of the revised Operations and Maintenance Plan being developed by Access Health, BEST and KPMG. The IV&V team has requested access to the current draft of the Release 2 Operations and Maintenance Plan for our review since the R1 Operations and Maintenance Plan does not include the level of comprehensive change management that the IV&V team feels is needed to support the CT-HIX application. The IV&V team has been informed that the Release 2 Operations and Maintenance Plan will be available on August 23rd. **September Update:** Change management procedures for new releases, builds and patches to CT-HIX are being documented in the recently published Operational Support Plan with a plan for a governance structure for these changes. However, there is still little documentation or formal processes on change management on the technical infrastructure side that supports CT-HIX or the other systems and services used by CT-HIX. This allows changes to the technical environments used to support and test CT-HIX to be made (including configuration changes) without an understanding on its impact on the CT-HIX application during testing or production.
			See latest update

Return to Technical Operational Support Capability Review

Appendix B. Previously Identified Risks and Findings (Closed)

Date	Area Name	Identifier	Statement
Risks - Closed			
9/13	Security Architecture Review	5.1 Risk	**Security Policy** The First Data IV&V team biggest concern at this point is the lack of documented state security policies. Many of BEST's security practices are known and understood only by BEST security staff. Without clear security policies written in business language it is difficult to determine if adequate security functionality is being provided. Unless the BEST practices have been disclosed and their implications understood by Deloitte and ahCT, the solution is likely to reveal some conflicts during testing or early production phases. A limited number of ahCT-specific security policies have been drafted. Additional security policies are necessary in order to give direction to AHCT partners and providers, such as HealthPass and Maximus, along with limited policies specific to Navigators. **August Update:** Recent documentation provided in the Deloitte library documents a much more granular role-based security structure for access to documents and workflow functions. AHCT has stated that similar rules for access to information such as that in the reporting database have been delayed until after October 1, 2013 (only standard "canned" reports will be extracted from this database for now). The First Data IV&V team will assess the development of security requirements and policies for access to information in the reporting database when they are developed to ensure adequate security of this information. **September Update: Closed**
9/13	Technical Operational Support Capability Review	6.2 Risk	**Service Level Agreements for Operations, Maintenance and Service Expectations – CMS Level 1** MOU's and SLA's with outside service providers (including BEST, HealthPass, Maximus, and Xerox) are still being developed and finalized. We are concerned that they be sufficiently detailed and clarify responsibilities for operational support and maintenance of infrastructure and services. The SLA records a common understanding about services, priorities, responsibilities, guarantees, and warranties. Undefined and unclear Service Level Agreements for operations, maintenance and service expectations can lead to issues later in production support and possible additional unplanned expenses. SLA's can also be a critical source of what SOA best practice documentation refers as to Service Contracts for interfaces being supported by the SOA infrastructure. These Service Contracts are used in the Service Registry of the Enterprise Service Bus to manage interfaces with these providers, including what are the consequences

Date	Area Name	Identifier	Statement
			arising from any interruption in the expected response from that provider. **August Update:** The MOA between AHCT and BEST incorporates several SLA benchmarks. For example, it sets a goal of "four nines" or 99.99% uptime for network and servers with less than one millisecond latency. At the same time it defines Service Availability with 10 hours of defined maintenance plus a Downtime allowance per month of 12¼ hours, which it concludes is 98.3% minimum server performance. Additional SLAs are expected to be defined between BEST and AHCT in the future. Similar service expectations should be incorporate into MOU's with the other service providers before the October 1, 2013 production date. We will review these MOU's as they are drafted. **September Update: Closed**
7/13	Technical Operational Support Capability Review	Risk 6.3	**Adequate Supplemental Support of the Technical Environment** Many of the infrastructure components being supported are new to the technical support staff at BEST and are critical to the successful operation of CT-HIX. The O&M support being contracted for from Deloitte does not cover this support and contracts should be put in place to ensure the specialized support needed can be obtained on short notice to avoid the risk of significant system disruptions. **August Update:** Operational management at BEST has responded verbally to this risk by stating that contracts are being put in place for the support of all critical service and infrastructure components. Based on this reassurance we are closing this risk. September Update: Access Health has procured additional technical expertise from IBM to help BEST prepare the IBM sourced components of the technical infrastructure for October 1 production of CT-HIX. This in part was in response to concerns that some of the components such as the FileNet workflow and content management servers were not adequately performing for ConneCT recently and this would be a shared technology platform with CT-HIX. The IBM technical staff have found specific settings that have negatively affected ConneCT performance and are working with DSS on changes in procedures to alleviate this problem. **September Update: Closed**
9/13	Testing Assessment	7.1 Risk	**HealthPass Testing** HealthPass hasn't provided any testing materials for IV&V review. Although HealthPass is already executing SHOP-like functionalities, First Date believes HealthPass should still submit the necessary test plans for review and then execute its system integration and user acceptance test plan. As part of our IV&V role, the First Data team plans to evaluate the test plan, review test findings, observe portions of User Acceptance Testing and where appropriate, re-execute test cases. **Impact:** The inability to provide test plans of sufficient detail, the

Date	Area Name	Identifier	Statement
			perceived inability to respond to requests for documentation or to establish SIT and UAT test environments brings into question HealthPass's ability to function successfully as AccessHealth's SHOP vendor. As stated, bswift provides the technical component on behalf of HealthPass. bswift has submitted Blueprint Scenario test findings to CMS. Still, there are a number of testable or observable non-technical processes that fall directly to HealthPass. In addition, documentation covering business continuity, disaster recovery or daily operations has yet to be provided by HealthPass for its processes and facilities. **Recommendation:** HealthPass must provide a detailed test plan that encompasses SIT and UAT as well as provide a document detailing how it intends to demonstrate to IV&V and ahCT management team that it can execute the necessary SHOP functionalities that can't be tested traditionally such as the HealthPass Call Center. The amount of documents relating to business operations need to be supplied. **September Update: Closed**

Date	Area Name	Identifier	Statement
	Performance Testing	Risk 8.1	**Adequate Stress Testing of the Shared CT-HIX and ConneCT Environment** Performance testing should include an adequate stress test of the CT-HIX application based on estimated peak loads of activity. It should include some estimate of the impact on shared components of the technical infrastructure with ConneCT. **Impact:** With the estimated number of Exchange customers accessing CT-HIX and the supporting service applications, it is reasonable to presume there is a realistic risk that the environment will be stressed to maximum capacity early in the program rollout. Subsequent system slowdowns or possible outages would be detrimental to the initial customer experience and could have impact on the success of the program implementation overall. **Recommendation:** Consideration should be given to using the production environment to conduct "pilot" testing that would stress the shared technical components with DSS and others. **August Update:** The Release 2 SIT test plan recently published in the Deloitte library provides much more detail on how stress testing will be conducted for the CT-HIX application. While the test tool being utilized has a limitation of simulating up to 5,000 concurrent users, the new SIT plan (which includes UAT testing) has adequately addressed how the CT-HIX application will be stressed as part of performance testing in the Staging environment. Note that by not conducting outside user testing via the Internet in the Staging test environment we will not know what impact the outside security "firewalls" and related tools will have once in production. There is still a risk of how the shared infrastructure components supporting the CT-HIX application will affect performance once in the production environment. Several of the key components, including the mainframe, are already being stressed as DSS implements the ConneCT application. While it would be difficult to simulate this additional load on the supporting technical environment in Staging, the potential risk on CT-HIX performance should be factored into the stress test results. Consideration should be given to using the production environment to conduct "pilot" testing that would stress the shared technical components with DSS and others. **September Update:** Performance testing has been conducted in the Staging technical environment using a testing tool that can mimic up to 3000 users. While the 3,000 user limit does not provide the stress of thousands of possible users that could be accessing the Exchange on October 1, the addition of extra technical expertise and the ability of BEST to expand capacity via a virtualized technical environment is probably as good as can be expected for ensuring that the CT-HIX application will perform adequately on October 1. Return to Performance Testing

Date	Area Name	Identifier	Statement
Findings - Closed			
5/13	Project Management Assessment	1.3 Finding	Since First Data wasn't engaged until after the requirement gathering sessions were completed, it is impossible for the IV&V to confirm that the documentation is 100% accurate and a complete representation of all necessary requirements. IV&V can state that the published requirements identified are being tracked through design, development and testing. This ultimately represents a potential risk that the IV&V team will fully document as we further research traceability of requirements through Design, Development and Testing. **June Update:** Delolitte has documented 646 functional requirements that are currently being mapped through design and development to an appropriate number of test cases. In all, Deloitte expects to develop an estimated 2,000 test cases. From First Data's perspective, this is an acceptable requirement to test case ratio. **August Update: Closed**
5/13	Project Management Assessment	1.5 Finding	The HIX project management team is working effectively while dealing with the additional complexity of integration with the ongoing DSS ConneCT project. PM roles and responsibilities are generally clear, although there is some overlap between the PMO vendor and the State. We do not see this as a risk at this point but noted for further evaluation in our ongoing project management IV&V reviews. **August Update: Closed**
5/13	Project Management Assessment	1.6 Finding	Project meetings generally follow a clear agenda, are well run and efficient with results (action items, risks, decisions) well documented. **August Update: Closed**
5/13	Project Management Assessment	1.7 Finding	Project Protocols and Controls such as Risk Management, Change Control and Communication Planning are fully documented. The IV&V team is still evaluating how well these have been implemented and their effectiveness, however initial reviews indicate no current issues with project controls. **August Update: Closed**
5/13	Project Management Assessment	1.8 Finding	The Master Project Plan is updated regularly and is documented at a highly granular level. Tasks are defined intuitively and seem to follow a good PMI best practices structure with dependencies and milestones clearly identified. IV&V project management plan concerns are related to the project schedule (a well-known risk) and a better defined critical path. The IV&V team will provide specific schedule recommendations beginning in our first full monthly report. **Resolution:** Given the slippage in the development timeline, IV&V continuing to monitor the master project plan as well as the plan to correct the slippage. **August Update: Closed**
5/13	Project	1.9	The IV&V team considers the integration of multiple call centers and

Date	Area Name	Identifier	Statement
	Management Assessment		the associated supporting vendors, applications and data a potential problem. **August Update:** As part of the UAT effort, IV&V will review the respective call center documents with a particular focus on the integration among the various call centers with documentation supporting the integration. **September Update:** The IV&V team has been on-site to the Maximus, bswift and HealthPass call centers. During our visits we had meetings with management to review operations policies and practices with particular emphasis on how calls are handled among the three facilities. **October Update:** Closed
Return to Project Management Assessment			
5/13	Technical Assessment Overview	2.1 Finding	The overall design is based on the integration of services via an SOA infrastructure framework: o It is built on proven principles, not "cutting-edge" theory. o It is conceived to meet the seven CMS conditions and standards. It appears to meet the State's strategic direction, which should improve interoperability with other agency's needs and solutions. The proposed technical environment is complex, with many pieces being built in parallel. **Resolution:** This finding is addressed in section 1.5 of the May status report. **August Update: Closed**
5/13	Technical Assessment Overview	2.2 Finding	Many detailed technical documents have been developed for the various technical components and solutions. To obtain a top-down view of how these components interoperate is usually accomplished with graphical overviews that do not always provide enough detail to assess interoperability. **Resolution:** This finding is taken up in the Technical Architecture and Solution Architecture review sections of the May report. **August Update: Closed**
5/13	Technical Assessment Overview	2.3 Finding	Many drafted design documents have been submitted for review and approval "pending approval", but work is proceeding with the assumption approval of the submitted design is forthcoming. **Resolution:** This finding is addressed in section 1.6 of the May report. **August Update: Closed**
5/13	Technical Assessment Overview	2.4 Finding	The overall Solution Architecture may not be as adaptable or 'agile' as it will need to be: o There appears to be Eligibility Rules embedded in JAVA that should be the Corticon Rules Engine. **This finding is addressed in section 4.1 of the May report.**

Date	Area Name	Identifier	Statement
			o Multiple Security components and ID directories may need to be synchronized. **This finding is addressed in section 6.4 of the May report.** o Integration between CT-HIX and ConneCT may not be tightly coupled enough. **August Update: Closed**
5/13	Technical Assessment Overview	2.5	There is little in-house (ahCT, DSS or BEST) expertise available to support many of the new infrastructure components or the application code. **June Recommendation:** A decision on outsourcing O&M should be made soon so that technical staff either way can be ready to support the system during UAT. Consideration should be given to provide BEST additional O&M staffing as part of the contract change order. It is unlikely that BEST technical staff will have the availability for mentoring that is required in the Transition and Knowledge Transfer Plan. If outsourcing is not chosen, AHCT (and possibly BEST) will need time to staff up internally to be mentored and trained adequately. **August Update:** This finding is being addressed in Risk 6.1 Adequate Documentation and Training for Support of the Technical Environment and Risk 6.3 Adequate Supplemental Support of the Technical Environment. **September Update:** AccessHealth has executed contracts with several vendors (including IBM) to provide additional technical support for the first six months of operations.
5/13	Technical Assessment Overview	2.8	There does not appear to be enough documentation of expectations between State agencies, outside agencies or outside service providers to ensure operational management of the system or manage changes in the future. For example best practices for an SOA solution requires "contract" level SLA's registered in the Service Registry of the Enterprise Service Bus to clarify expectations and accountability, and guide future replacement. **June Recommendation:** The IV&V team would welcome the opportunity to review the SLA component of MOUs being developed for the services utilized by CT-HIX to assess clarity and thoroughness of expectations and procedures. **August Update:** This finding is being addressed in Risk 6.2 Service Level Agreements for Operations, Maintenance and Service Expectations. **September Update:** Risk 6.2 has been moved to the closed section of the Appendix for September.
Return to Technical Assessment Overview			
5/13	Technical Architectural Review	3.1	The complexity of the technical architecture and the infrastructure being implemented to support it will require careful planning, testing in a staging environment, and implementation with appropriate

Date	Area Name	Identifier	Statement
			technical staff training for operational support capability. Many of the technical solutions being deployed are also new to most of the State staff in DSS and BEST, making appropriate planning, testing and operational preparedness critical to the success of CT-HIX. **Recommendation:** To ensure that that there is adequate testing of the technical environment and operational readiness to support that environment, Technical Continuity Testing should be added to the testing process. This could also be done in conjunction with Business Continuity Testing. **July Update:** This finding will be tracked as Risk 4.1 Real World UAT and Technical Testing Environment, Risk 4.2 Coordinating Change Management, and Risk 3.1 Contingency Planning for the Technical Environments. **September Update:** Recently Access Health has contracted additional technical staff to be available after 10/1 to ensure adequate support is available and additional training is conducted to support the technical environments
5/13	Technical Architectural Review	3.4 Finding	There are separate Deloitte teams working on the two projects with different constraints and timetables so keeping these two projects in synch given the tight timetables for both projects will be difficult. **July Update:** This finding will be researched and reported on in the August IV&V Report. **August Update:** This finding will be combined and followed up with Finding 4.6 in the Solutions Architecture Review section in Appendix A.
5/13	Technical Architectural Review	3.6	The number of interfaces with systems and services will require sufficient stress testing of the new system to ensure that the projected number of users, especially when the CT-HIX exchange is first opened, can be supported with the infrastructure being built. **Resolution:** This finding will be taken up in the 6.1 section of the report. **August Update:** This finding is being addressed in Risk 8.1 Adequate Stress Testing of the Shared CT-HIX and ConneCT Environment. **September Update:** This finding is being closed along with the associated Risk 8.1 Adequate Stress Testing.
Return to Technical Architectural Review			
5/13	Solutions Architectural Review	4.1 Finding	There appears to be eligibility rules embedded in the application in Java code instead of the Corticon business rules engine. This will make it more difficult to make changes to the eligibility rules in the future (need a Java programmer, and substantial time to find the rule(s) in question). At the request of First Data, a meeting was held at the AHCT offices on May 22 to address this finding. The meeting was attended by Deloitte PM and Technical Architects and the First Data IV&V Team. Deloitte provided additional information on how eligibility business rules as

Date	Area Name	Identifier	Statement
			well as other rules are being incorporated into the Corticon Rules engine presently. This discussion alleviated First Data's concern regarding this finding. First Data has requested that the clarification and resolution to business rule concerns that were discussed will be documented by Deloitte and provided to First Data. **Resolution:** Deloitte has provided a clarification document regarding the use of rules in Java and Corticon that met our request to document what eligibility processing rules will be moved from the Java Eligibility Determination Service to Corticon (two in total) and why they are being moved. They also documented what single eligibility processing rule will remain in the Java Eligibility Determination Service. These changes are consistent with "the project's architecture principle to put policy rules in Corticon while keeping data collection from the database and external interfaces in Java" (as documented in the clarification document). **August Update: Closed**
5/13	Solutions Architectural Review	4.2	There is a Service Registry identified to support the ESB infrastructure, but we will need to take a closer look at this to ensure that there are adequate "service contracts" defined for each service being interfaced. This is an important best practice for developing an SOA based environment because it will be critical for understanding what is expected from each service interface and how it will be supported by the service provider if there are problems or enhancements to the systems. **June Update:** The use of MOU's for this purpose should be reviewed to ensure that adequate service levels are being documented and adhered to from all outside service providers. The Service Registry and Repository does not need to include the actual SLA, but does need to document what the ESB is transforming, where data is being routed, and who will be notified if there is a failure in service. **Recommendation:** While an SLA should include this detail of documentation to clarify expectations, the expectations for use of the ESB still need to be in the Service Registry. The IV&V team would like an opportunity to investigate this further. To date, no documentation has been provided as to what resides in the Service Registry and Repository. The lack of documentation may indicate a potential risk that the IV&V Team is continuing to research. **July Update:** This finding will be tracked as Risk 6.2 Service Level Agreements for Operations, Maintenance and Service Expectations and Risk 6.1 Adequate Documentation and Training for Support of the Technical Environment. **September Update:** This finding has been closed based on the closing of associated risks 6.1 and 6.2.
5/13	Solutions Architectural Review	4.4	It is important that the staging environment must reflect all the components and services that constitute the final system design because of the number of interfaces and services that must be integrated to meet the business requirements of AHCT and DSS.

Date	Area Name	Identifier	Statement
			Decisions are still being made on some of the components and their utility in the system which could impact the amount of time available for adequate testing. Consideration should be given to testing whether the Service Registry has adequate information to aid in recovering from system service disruptions. **June Update:** BEST practices have not allowed outside Internet access to the UAT environment, now assumed to be the Staging Environment; UAT testers would need to access their environment through the State's intranet or utilize VPN keys. Neither of these approaches will adequately test the production infrastructure for outside users. The Development testing environment is not hosted at BEST and will not provide an adequate platform for end testing. **Recommendation:** Given the probable volume of activity by individuals outside the state's intranet, First Data recommends that BEST provide an appropriately accessible UAT environment including outside Internet access by testers. **August Update:** This finding is being addressed in Risk 4.1 Real World UAT and Technical Testing Environment and Risk 3.1 Contingency Planning for the Technical Environments. **September Update:** BEST has completed the Staging environment and provided a policy exemption to allow testing of CT-HIX in the Staging environment so this finding is being closed.
5/13	Solutions Architectural Review	4.5	There are still unresolved issues with some of the services being used such as the SHOP application, and the Symantec VIP cloud service. These "loose ends" need to be resolved soon to ensure that an adequate "system test" environment can be created for comprehensive testing before production. As pointed out in the Technical Architecture Review, the integration of services internal to the CT-HIX and ConneCT systems is as important to look at as the integration of services outside these systems. **Resolution:** The SHOP and Symantic VIP Cloud service have been finalized as solutions. Concerns described in this initial finding regarding adequate testing of these and other services will be addressed in the Testing Assessment Review and Adequate Potential Risk sections of this report. **August Update:** This finding is being addressed in Risk 4.1 Real World UAT and Technical Testing Environment.
Return to Solutions Architectural Review			
6/13	Security Architectural Review	5.1	Role based access to applications and documents are not granular enough. For example, there should be different role-based access for the different roles of AHCT and DSS staff workers and their supervisors. **June Update:** It is our understanding that Deloitte has been working with AHCT to develop more granular roles and privileges for access to documents and workflow functions. The IV&V team is waiting for documentation demonstrating the extent to which roles and

Date	Area Name	Identifier	Statement
			responsibilities are being created for the respective entities (AHCT, Maximus, HealthPass, DSS, Xerox, and BEST). **Recommendation:** First Data recommends that AHCT develop specific security policies that will guide creation of user roles based on applications or information needed. As part of the proposed policy, provide documented instances of improved roles definition including examples of privileges assigned to these roles. **August Update:** This finding is being addressed in Risk 4.2 Coordinating Change Management and 5.1 Security Policy. **September Update:** This risk is being closed as more role based security issues have been addressed for CT-HIX.
5/13	Security Architectural Review	5.2	Testing of the entire security environment (including the ID Proofing through the Federal Hub) must be made in the staging environment that reflects production, or be in a special testing environment that incorporates all of the operational infrastructure and application solution, including being open to web access. **June Update:** BEST was made aware by AHCT in the UAT-kickoff meeting that testing needed to be accessible via the Internet. BEST practice does not normally provide Internet access for outside testers in their Staging environment (which is required for true end-to-end testing), but will review this with their security staff. **Recommendation:** Because of the numerous sub-systems and appliances being utilized for CT HIX, the IV&V team recommends holistic testing of all security devices are conducted consistently throughout the UAT process to reveal any anomalies. **August Update:** This finding is being addressed in Risk 4.1 Real World UAT and Technical Testing Environment. **September Update:** This finding has been closed now that BEST is allowing testing of security functions through the Internet in the Staging environment, and the recent IRS security approvals for CT-HIX.
5/13	Security Architectural Review	5.3	Possible limitations or constraints to usage of these components experienced in similar environments are less well described. Most of the components will be supported primarily by BEST; many of these appear to be new or little used to date, based on the documents. Expected operational demands on AHCT and/or DSS such as administration of ID directories and procedures for "remediation" of security issues and who is responsible for which components are not included in the documents. **Resolution:** Sufficient testing at the highest level with Web access should reveal limitations on utilizing or supporting the various components. **August Update:** This finding is being addressed in Risk 4.1 Real World UAT and Technical Testing Environment, Risk 6.2 Service Level Agreements for Operations, Maintenance and Service Expectations, and Risk 6.1 Adequate Documentation and Training for Support of the Technical Environment.

Date	Area Name	Identifier	Statement
5/13	Security Architectural Review	5.4 Finding	While each component service is well documented, the environment is complex and relationship(s) across and between such services is not clear enough. With the complexity of the security components utilized for inside and outside security, it is important that these relationships are clear, logical, accountable and tested. **August Update: Closed:** The relationships between various component services utilized for external versus internal security have been clarified in recent documents.
5/13	Security Architectural Review	5.5	Support resources are not thoroughly detailed, and if the same resources are expected to support many components, the "ramp-up" time to learn and support new services during stress testing or operational stress is a potential concern. Examples of new security components include the Open LDAP solution with ISIM and ISAM, the IBM WEBSEAL QRadar and Data Power security in the "DMZ", and the Adobe digital signature solution. **Resolution:** We have combined this section with Operational Support 6.5 covering technical training and supplemental contractual resources. **August Update:** This finding is being tracked as Risk 6.1 Adequate Documentation and Training for Support of the Technical Environment.
Return to Security Architectural Review			
5/13/ 2013	Technical Operational Support Capability Review	6.1	Several service components of the CT-HIX system are still being finalized and SLA's and MOU's are still being developed for services and interface exchanges of data. We have found no documentation of any finalized SLA for any of the services or interfaces, which would normally be a best practice of a Service Oriented Architecture (SOA) approach to a system. Well documented SLA's are critical for setting expectations and articulating operational procedures (automated or manual) when experiencing service failures or performance issues. These service expectations and failover procedures are utilized in the Service Registry and Repository of the Enterprise Service Bus to automate much of the Enterprise Service Bus management of the SOA environment. **June Update:** The MOU with BEST is currently being reviewed by the attorneys for AHCT. **Recommendation:** The IV&V team would welcome the opportunity to review the SLA component of MOUs being developed for the services utilized by CT-HIX to assess clarity and thoroughness of expectations and procedures. **July Update:** This finding will be tracked as Risk 6.2 Service Level Agreements for Operations, Maintenance and Service Expectations.
5/13/	Technical Operational Support Capability	6.4	We have found no Operation Manual or documentation of technical operational planning across the CT-HIX or DSS systems, or across ACH CT, DSS and BEST. This is required to ensure that the responsibilities for each component of the infrastructure and each service being

Date	Area Name	Identifier	Statement
	Review		interfaced are clear and expectations for what that component does in the system is understood. It should also articulate alternative support plans should resources become unavailable; while there is a disaster-recovery plan, it does not deal with lower-level interruptions, expected intervals for replacement of failed key infrastructure components and tools, or any inability to provide knowledgeable technical staff to support a service. **June Update:** Deloitte has indicated that such a manual does exist and once available, IV&V will be reviewing the document. The clarity of roles and responsibilities for technical operational support will be taken up in section 6.1 as documentation needed for SLA's. We are still looking for more documentation on restoration and recovery procedures. **Recommendation:** Given the complexity of the technical environment, First Data suggests the development of a Technical Continuity Plan (TCP), to accompany the Business Continuity Plan (BCP). The purpose of the TCP is to decide ahead of time what to do when key infrastructure components lose functionality while in operational mode. Such loss can range from reduced capacity (measured against demand) to total system failure. In some instances, it is possible to continue to operate without that component; the TCP predetermines the risk and acceptability of doing so based on the risk determination in the Business Continuity Plan. The TCP instructs when it is necessary and appropriate to shut down or slow down system operation, due to technical shortcomings. **August Update:** The IV&V team has requested a copy of the Release 2 Operations and Maintenance Plan. This finding will be tracked as part of Risk 6.1 Adequate Documentation and Training for Support of the Technical Environment and Risk 3.1 Contingency Planning for the Technical Environments. **September Update:** The Operations and Maintenance Manual has been updated and an Operations Support Plan has been published that defines incident reporting workflow. In addition the IV&V recommendation to a Technical Continuity Plan will be completed and tested in November so this finding is being closed.
5/13/	Technical Operational Support Capability Review	6.5	It is not clear if adequate training of the technical staff responsible for supporting the systems has been planned for. There are many new technology components that State staff may be unfamiliar with. The SOA service support environment in particular will require additional training. **June Update:** The CT-HIX Transition and Knowledge Transfer Plan includes technical training of BEST and AHCT staff via a knowledge transfer approach that assumes that the "protégés" being trained at BEST and AHCT are currently performing similar roles and those identified will be immediately available for mentoring with sufficient time to do so. On the other hand the CT-HIX Transition and Knowledge Transfer Plan states that "third party vendors may be best suited for tool specialist roles for specialized products". The Plan also

Date	Area Name	Identifier	Statement
			states that a "contract change order is in discussions that may likely outsource the O&M support". This would "likely lead to a change in the Transition and Knowledge Transfer Plan roles and responsibilities." **Recommendation:** A decision on outsourcing O&M should be made soon so that technical staff either way can be ready to support the system during UAT. Consideration should be given to provide BEST additional O&M staffing as part of the contract change order. It is unlikely that BEST technical staff will have the availability for mentoring that is required in the Transition and Knowledge Transfer Plan. If outsourcing is not chosen, AHCT (and possibly BEST) will need time to staff up internally to be mentored and trained adequately. **August Update:** Access Health is in the process of finalizing a contract with Deloitte for maintenance of CT-HIX. The other concerns stated in this finding will be tracked as part of Risk 6.1 Adequate Documentation and Training for Support of the Technical Environment and Risk 6.3 Adequate Supplemental Support of the Technical Environment at BEST. **September Update:** Access Health has contracted through BEST for additional technical support for October and November and plans on using these resources to also mentor BEST staff.
Return to Technical Operational Support Capability Review			
5/13	System Integration Testing	7.1 Finding	Deloitte adhered to the testing processes in the System Integration Test Plan. **August Update: Closed**
5/13	System Integration Testing	7.2 Finding	Deloitte's testing team conducted two distinct test cycles, the second cycle conducted as confirmation of the first. **August Update: Closed**
5/13	System Integration Testing	7.3 Finding	Identified testing defect are triaged (classified) by the Deloitte team. **August Update: Closed**
5/13	System Integration Testing	7.4 Finding	Deloitte employed capturing reporting processes in order to log defects and designated classifications. **August Update: Closed**
5/13	System Integration Testing	7.5 Finding	Deloitte prepared daily reports for review by Deloitte and AH CT staff. **August Update: Closed**
5/13	System Integration Testing	7.6 Finding	Defect identified in each test cycle of tests were addressed based on severity and retested. **August Update: Closed**
5/13	System Integration	7.7 Finding	Deloitte prepared a defect summary report that listed all defects and their status at the time of publishing.

Date	Area Name	Identifier	Statement
	Testing		**August Update: Closed**
5/13	System Integration Testing	7.8 Finding	No Severity 1 Defects existed at the conclusion of SIT; a limited number of Severity 2 defects remain, this was agreed to by Deloitte and AH CT management. **August Update: Closed**
5/13	System Integration Testing	7.9 Finding	Regression testing was performed throughout the SIT and is being extended into UAT when outstanding defects being fixed and to ensure existing functionality is working as expected. **August Update: Closed**
5/13	System Integration Testing	7.10 Finding	NAIC was unable to provide SERFF test data for Release 1 SIT. Once NAIC can provide the test data, additional testing will be necessary. **August Update: Closed**
5/13	System Integration Testing	7.11 Finding	SERFF and plan data were not available for Release 1 SIT. Required additional testing could produce new defects. **August Update: Closed**
5/13	System Integration Testing	7.12 Finding	CT-HIX inability to secure SERFF test data was due to changes to the existing data extract specifications. **August Update: Closed**
Return to System Integration Testing			
5/13	Performance Testing	8.1 Finding	Only those components necessary for Release 1 functionalities were tested. **August Update: Closed**
5/13	Performance Testing	8.2 Finding	Performance testing was measured by using a stop watch. **August Update: Closed**
5/13	Performance Testing	8.3 Finding	Performance tests focused on the ability to upload data/information. **August Update: Closed**
5/13	Performance Testing	8.4 Finding	Performance tests focused on the ability to view uploaded information. **August Update: Closed**
6/13	Performance Testing	Recommendation	Additional performance testing is necessary using more realistic volumes of data and a far greater number of simultaneous users
6/13	Performance Testing	Recommendation	Employment of a performance testing tool that can better document findings allowing for the more detailed analyses using industry metrics. **August Update: Closed**
6/13	Performance Testing	Recommendation	IV&V recommends that all performance testing occur in an environment that mirrors the production environment. **August Update: Closed**

Date	Area Name	Identifier	Statement
Return to Performance Testing			
5/13	Wave 1 Testing	9.1 Finding	Testing could not verify what information was send and Via ESB or Test Harness. **August Update: Closed**
5/13	Wave 1 Testing	9.2 Finding	Test results did not distinguish between Open Book and Closed Book tests as indicated in FEPS Test Plan. **August Update: Closed**
5/13	Wave 1 Testing	9.3 Finding	Testing progress reports were inconsistent in terms of identified defects, and pass/fail tests results for each service. **August Update: Closed**
5/13	Wave 1 Testing	9.4 Finding	Testing progress reports do not include all Defect IDs. **August Update: Closed**
5/13	Wave 1 Testing	9.5 Finding	The defect ID's shown does not match between reports. **August Update: Closed**
5/13	Wave 1 Testing	9.6 Finding	Wave 1 testing conducted could not confirm payload 4 results. **August Update: Closed**
6/13	Wave Testing	9.7 Finding	All defects identified in Wave 1 testing have been corrected. **August Update: Closed**
6/13	Wave Testing	9.8 Finding	Five of the seven services have already been certified during Wave 3 Testing. The remaining two services are expected to be certified by 6/14/2013. **August Update: Closed**
6/13	Wave Testing	9.9 Finding	600 test applications will be available for selection during Wave 3. **August Update: Closed**
6/13	Wave Testing	9.10 Finding	In Wave 3 testing, the exchange is to use 100 applications for testing; 25 of the original 25 applications (Wave 1), then selecting 75 "new" applications from the pool of 600 test applications. **August Update: Closed**
Return to Wave Testing			
5/13	User Acceptance Testing	10.1 Finding	The UAT Test Plan does not exist. **June Update:** A UAT Test Plan does exist and is being reviewed by the IV&V Test Team. **August Update: Closed**
5/13	User Acceptance Testing	10.2 Finding	Most of the UAT cases are taken from the SIT Test Plan for Release 1. **August Update: Closed**
5/13	User	10.3	Smoke testing was performed prior to formal UAT testing.

Date	Area Name	Identifier	Statement
	Acceptance Testing	Finding	**August Update: Closed**
5/13	User Acceptance Testing	10.4 Finding	An adequate volume of test data was available at the commencement of testing. **August Update: Closed**
5/13	User Acceptance Testing	10.5 Finding	Deloitte provided tester training in the usage of two testing support applications; JIRA for defect tracking and JAMA Contour for test execution.
5/13	User Acceptance Testing	10.6 Finding	Defects are being logged and triaged with Development teams and escalated based on Severity. **August Update: Closed**
5/13	User Acceptance Testing	10.7 Finding	Daily Test Status is being provided during the UAT testing activity. **August Update: Closed**
5/13	User Acceptance Testing	10.8 Finding	AH CT and DSS are serving as user acceptance. **August Update: Closed**
6/13	User Acceptance Testing	10.9 Finding	If UAT timelines are exceeded, a lack of available testers is realistic, especially if there is a large amount of retesting. An inadequate number of qualified testers could result in delaying UAT completion, thus impacting the CT-HIX Go Live date October 1. At the CMS Weekly Call Meeting, the Test Manager reported a high degree of cooperation by DSS to provide testers for UAT. Tester space is still a concern, but AHCT is aggressively looking for available space. **July Update:** Access Health has secured adequate space for testers during Release 2 of UAT. UAT testers will be located at the BEST facility. Test machines have been ordered and BEST has assured Access that the area will be ready by August 9th. **August Update: Closed**
Return to User Acceptance Testing			

IEDSS IV&V Monthly Management Briefing

JULY 14, 2015

First Data.
beyond the transaction

Agenda

Summary for June 2015

Observations

Future Activities

Performance Measures

Questions

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Summary for June 2015

Deliverables/Artifacts

- Reviews
  - System Test Summary Report
  - Revised System Test Summary Report DED
  - Operational Readiness Plan DED
  - Security Information and Event Management (SIEM) Implementation AED
  - CR PSD for Support IR14 - QC
  - Revised Unit Tested System Code
  - Application Vulnerability Assessment Report AED
  - Midpoint Survey Review for Organizational Change Management activity

© 2015 First Data Corporation. All Rights Reserved.

Summary for June 2015

Deliverables/Artifacts

- Activities
  - JAD Sessions (14)
    - Front Office
    - Interfaces
    - EDBC
    - Correspondence

- BPM (Task Management) Sessions (7)

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Summary for June 2015

Deliverables/Artifacts

- Activities
  - Walkthroughs
    - Revised Data Conversion Load and Test Plan
    - Revised Unit Tested System Code
    - System Test Summary Report DED
    - Security Information and Event Management (SIEM) Implementation AED
    - Operational Readiness Plan DED
    - Conversion Reference Code Mapping
    - Benefit Match for Converted Cases
    - Manual Correspondence

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Summary for June 2015

Deliverables/Artifacts

- Activities
  - Attended Training Team meetings
  - Attended Organizational Change Management (OCM) meetings
  - Attended SOTA call for Achieving Real Time Eligibility Determination webinar
  - Attended DDI Vendor Weekly Stage 2 Defect Triage Meetings
  - Monitored System Testing activities
  - Attended IEDSS Weekly Stage I Defect Management meetings
  - Attended CDMS Requirements/Design sessions

© 2015 First Data Corporation. All Rights Reserved.

Summary for June 2015

Deliverables/Artifacts

- Activities
  - Monitored System Testing
- Attended Touch Point/Document Defect Meetings
  - Self Service
  - Front Office
  - Back Office
  - Interfaces
  - Conversion
  - Correspondence
  - Reports

© 2015 First Data Corporation. All Rights Reserved.

Observations

- Decision #251215 – Conversion of Historical ICES Data
  - Closed in PMC
  - Impacts 18 System Requirements
  - Need to modify/remove
- Correspondence
  - Outstanding IR approvals
  - New CRs
- Project progress
  - Case vs AG
  - Phone Application
  - Task Management
  - Re-planning process
- System Documentation Storage
  - Issue with storing/locating current versions of PSDs

© 2015 First Data Corporation. All Rights Reserved.

Observations

- System Test
  - Defects
  - Change Requests Code Drop 1

- Integration Test
  - No Activities

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Testing

As of 06/30/2015

Cycle	Rel 1	% Comp	Rel 2	% Comp	Rel 3	% Comp	Rel 4	% Comp	CR 1	% Comp
System Test Overall Pass %										
1									20.4	100
2									28.7	100
3	99.9	100	99.9	100	99.8	100	97.6	100	31.0	100

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Future Activities

- Attend Design sessions as scheduled
- Review Design sessions minutes and documentation
- Attend document defect sessions
- Attend IEDSS Steering Committee meetings
- Generate IEDSS Steering Committee Minutes
- Monitor and Evaluate System Testing activities
- Provide System Test observations
- Review Integration Test Scenarios and Test Cases
- Monitor and Evaluate Integration Test activities

© 2015 First Data Corporation. All Rights Reserved.

Future Activities

- Provide Integration Test observations
- Monitor State User Acceptance Test activities
- Attend BPM/Task Management sessions
- Attend Walkthroughs as scheduled
- Attend IEDSS Project related meetings
- Review proposed Change Requests
- Deliver Monthly IV&V Briefings
- Deliver Monthly IV&V Reports
- Review and analyze re-plan results

© 2015 First Data Corporation. All Rights Reserved.

Future Activities

- Review artifacts, work products and deliverables
  - Revised Data Conversion and Load Plan
  - DDI Vendor June, July, August Monthly Status Report
  - System Test Summary Report
  - Security Information and Event Management Solution (SIEM)
  - On-line Help
  - Performance Test Summary Report
  - Operational Readiness Plan DED
  - Integration Test Summary Report

© 2015 First Data Corporation. All Rights Reserved.

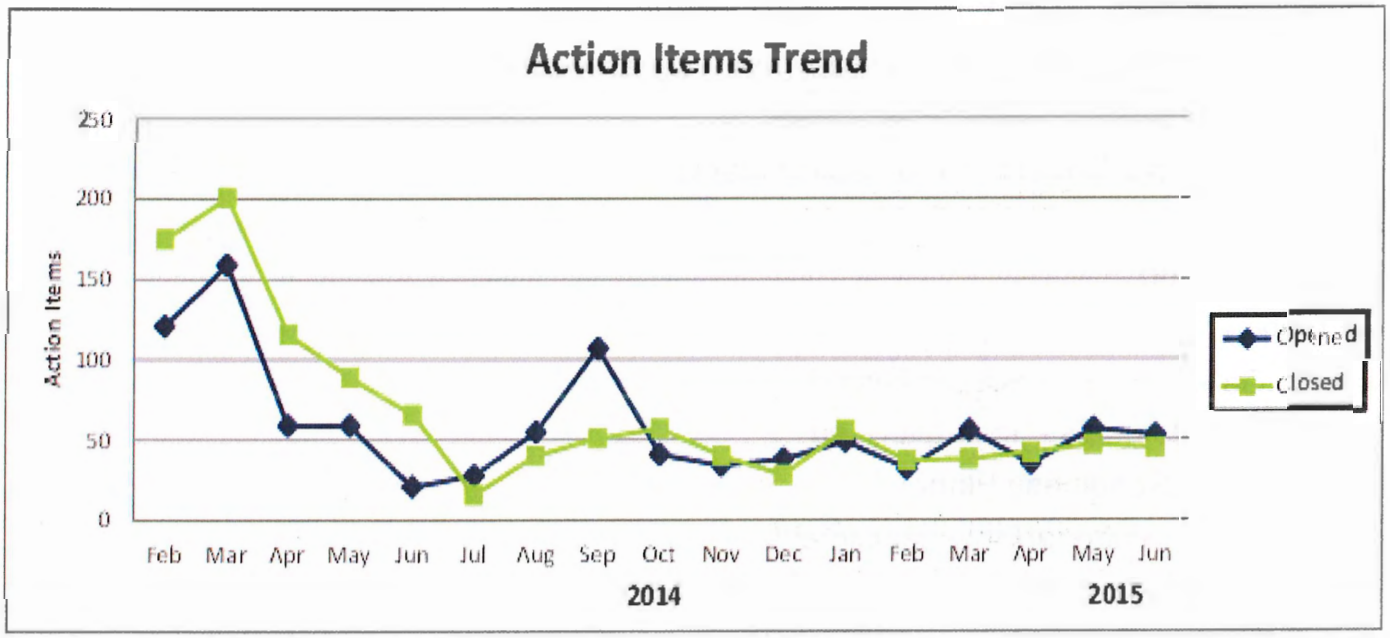
Future Activities

- Review artifacts, work products and deliverables
  - Data Conversion and Load Testing
  - Organizational Transition Plan - Pilot
  - Requirements Database Traceability Matrix
  - Design
  - Construction
  - Testing
  - IRS Safeguard Procedures Report
  - Training Materials – Instructor Led
  - Operation Readiness Plan
  - Application Vulnerability Assessment
  - Implementation Plan
  - CR IRs and Responses

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

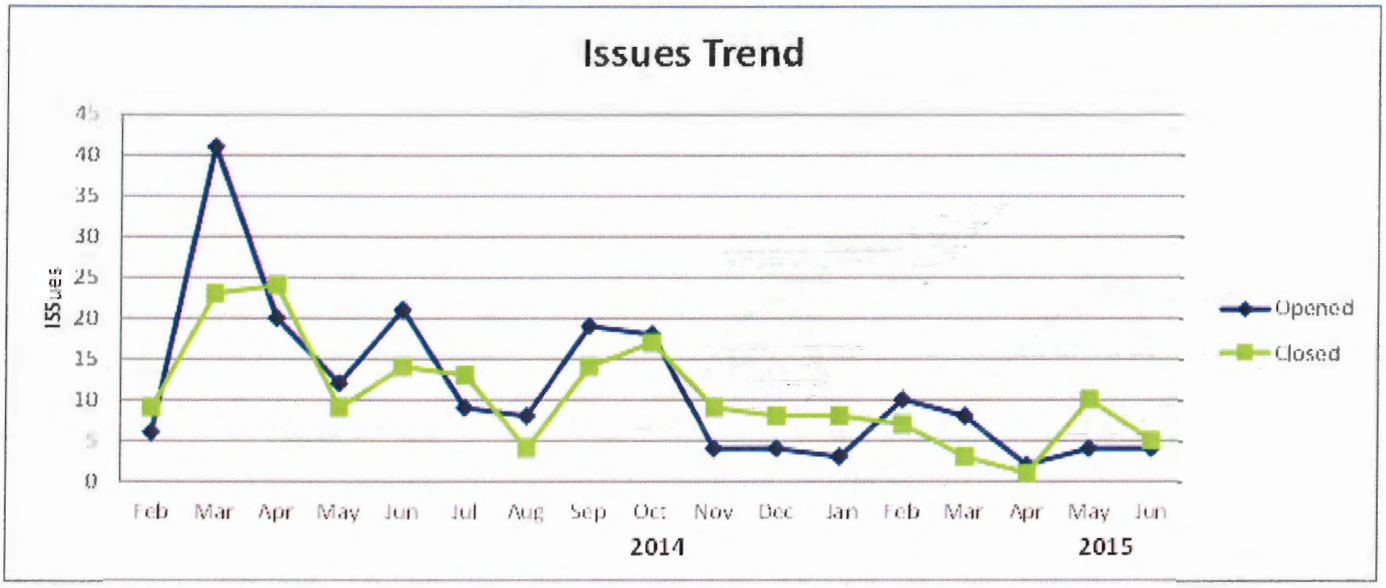
Performance Measures



© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Performance Measures



© 2015 First Data Corporation. All Rights Reserved.

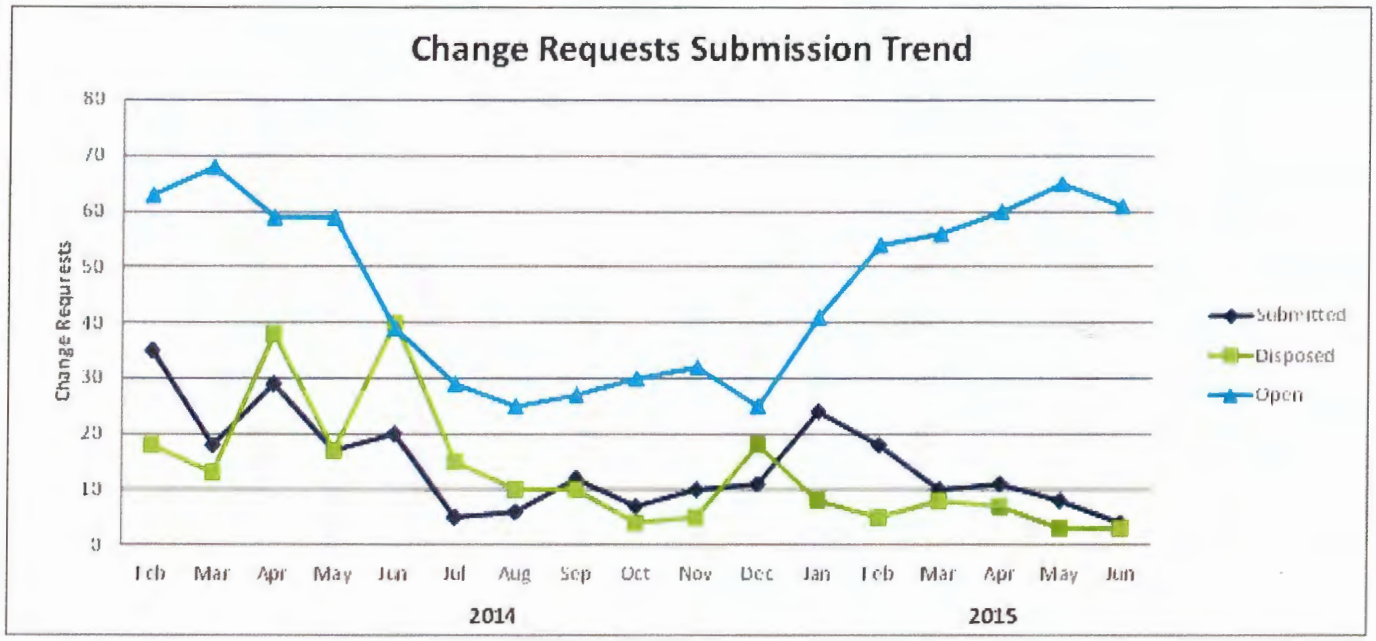
First Data.
beyond the transaction

Performance Measures

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

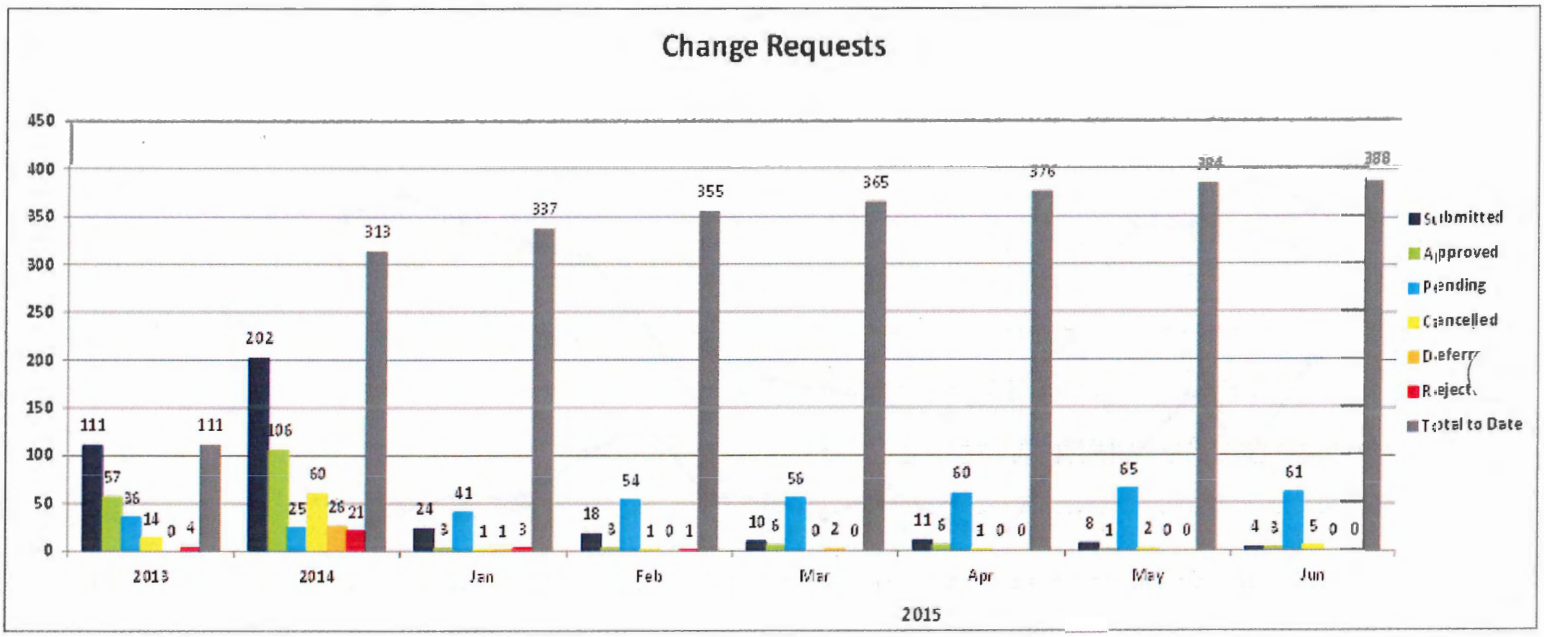
Performance Measures



© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Performance Measures



© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

Questions?

© 2015 First Data Corporation. All Rights Reserved.

First Data.
beyond the transaction

State of Indiana

Family and Social Services Administration, Division of Family Resources (DFR)

IV&V Services for Indiana Eligibility Determination Services System (IEDSS)

Monthly IV&V Report
June 2015

Document History

This document is controlled through the Document Management Process. To verify that the document is the latest version, please contact the First Data Team.

Date	Version	Reason for Revision
07/15/2015	1.0	Initial draft
8/3/2015	1.1	Addressed State Comments
8/10/15	2.0	Final

Table of Contents

Document History 1
Table of Contents 1
1.0 Introduction and Purpose 2
2.0 Summary 3
3.0 Observations 5
4.0 Activities Performed 13
5.0 Planned Activities (Next Two Months) 20
6.0 Performance Metrics 22
6.1 Action Items Metrics 23
6.2 Change Requests 26
6.3 Issue Metrics 27
6.4 Decision Metrics 30
6.5 Schedule Review 32
Appendix A – Current Organizational Chart 37
Appendix B – Project Metrics 38
Action Items, Issues, Decision Items and Change Requests Metrics 38
Appendix C – Action Items Pending Over 120 Days 41
Appendix D – Issues Pending Over 120 Days 42
Appendix E – Decisions Pending Over 120 Days 43

1.0 Introduction and Purpose

This is the Monthly IV&V Report for June 2015. The structure of the report is based on the State's IV&V Services Opportunity Requirements Form and includes:

- Activities performed during the month
- Activities planned for the next two months
- Expected meetings, interviews and documentation needed during the next two months
- Project risks, issues, mitigation strategies and corrective action approaches
- Current IV&V Organizational Chart (Appendix A)
- Project Metrics (Appendix B)
- Action Items Pending Over 120 Days (Appendix C)
- Issues Pending Over 120 Days (Appendix D)
- Decisions Pending Over 120 Days (Appendix E)

2.0 Summary

Activities for the month of June include attending Joint Application Design (JAD) sessions, training meetings, attending various standing project meetings, monitoring system testing and reviewing IEDSS deliverables/artifacts.

The IV&V highlights for the reporting period include:

- Review of Vendor's deliverables/artifacts
  - IEDSS
    - Revised System Test Summary Report DED
    - Reviewed System Test Summary Report
    - Operational Readiness Plan DED
    - Security Information and Event Management (SIEM) Implementation AED
    - Requirement Review for CR 286400 – Adding VAN to SVES
    - CR PSD for Support IR14 - QC
    - Application Vulnerability Assessment Report AED
    - Revised Unit Tested System Code
    - Revised Data Conversion and Load Plan
    - Midpoint Survey Review for Organizational Change Management activity
- Participated in 14 JAD sessions for Front Office, Interfaces, EDBC, and Correspondence
- Attended Touch Point/Document Defect Meetings as scheduled for Back Office, Front Office, Interfaces, Conversion, Correspondence, Reports and Self-Service
- Participated in Joint Training Review Design sessions
- Attended 7 BPM follow-up sessions
- Attended CDMS requirements and design sessions
- Attended comment resolution walkthroughs for:

  - Revised Data Conversion Load and Test Plan
  - Revised Unit Tested System Code
  - System Test Summary Report DED
  - Security Information and Event Management (SIEM) Implementation AED
  - Operational Readiness Plan DED
  - Conversion Reference Code Mapping
  - Benefit Match for Converted Cases
  - Manual Correspondence
- Attended Training Team meetings
- Attended Organizational Change Management (OCM) meetings
- Attended SOTA call for Achieving Real Time Eligibility Determination webinar
- Attended DDI Vendor Weekly Stage 2 Defect Triage Meetings
- Monitored System Testing activities
- Attended IEDSS Weekly Stage I Defect Management meetings

3.0 Observations

- The lack of decisions, guidance and responses from the DDI Vendor, the State and the Federal partners, is impacting the ongoing progress of the project. Items include, level of efforts for outstanding Change Requests, Case vs AG, Task Management, outstanding Federal approvals, State Gate Reviews, and input on other States' experiences. The project is also being impeded by the length of time it is taking to receive the results of the re-planning efforts associated with the proposed Amendment 4 to the DDI contract. (Holdover from May Report)

- As indicated in the May Status Report, Decision 251215, Conversion of Historical Data from ICES, has been closed in PMC. There are 18 system requirements that will need to be modified as a result of this decision; however, the requirements were not identified in the PMC Item when the Decision was created and the requirements were not updated prior to requesting the State to close the Decision.

- As indicated in previous status reports, there continues to be an issue with determining the most recently approved Storyboards/documentation in the State SharePoint. Although the DDI Vendor was reminded to place the most recently approved Storyboards/documents in the System Documentation folder in State SharePoint, this area is not being used by several tracks, and those that are using it are using it inconsistently.

- Several changes have been made on screens based on the design for HIP 2.0 and ABAWDs; however, these changes have not been submitted to the State for approval. When defects have been identified on the prior version of the screen, the unapproved updated version of the screen (updated based on HIP 2.0 and ABAWD) is often being used to correct the defect. IV&V is concerned that this is contributing to the confusion regarding locating the most recent approved version of a document.

- The DDI Vendor has been inconsistent in their design document defect meetings. Some tracks have consistently held meetings to review any design document defects with the appropriate State SME(s), while other tracks have not scheduled meetings at all or infrequently. Design document defect meetings should be held regularly and the meetings should be consistent in content and preparation (i.e., list of defects provided in advance, reason for the defect, supporting documentation for why it is a design document defect rather than an application defect).

- The State has not approved the 18 correspondence IRs submitted in the third quarter of 2014. They were never approved by the prior State Correspondence SME, and the current State SME has been unable to complete them thus far in 2015 due to time constraints, as she is currently involved with the IEDSS Report Track, along with the design and review of FACTS and ICES changes. A session to go over the document defects for correspondence screens in IEDSS was held in late May and

submitted to the State for approval on 5/28; however, the State SME has not approved or given other feedback on the corrections as of the end of June. In addition, the State Correspondence track lead has expressed her intent to review prior State approved PSDDs related to eligibility and non-eligibility notices, but has been unable to do so.

- A former DDI Vendor Correspondence Lead, still assisting with correspondence, left the project in June (with little notice given). Comments submitted by the State on 6/12 on Correspondence IR25 remained unaddressed in June.

- The CCB did not meet in June and this has impacted the State's ability to plan for potential JAD sessions related to change requests. This also impacted several new CRs that were submitted in April and May; ten of these CRs were for the correspondence track.

- BPM follow-up sessions, led by the DDI Vendor Back Office Lead, continued in June. Thus far the Document Processing BPM has been discussed, and in part, the Application Processing BPM. Several gaps in functionality have been identified as a result of these sessions, some of which will be needed for Day 1 implementation and will require input from the Change Control Board.

- The Transformation Team has recently begun to ramp up its effort of coordinating the Organizational Change Management (OCM) activities leading up to IEDSS rollout. With this increased level of effort comes an increased level of staff involvement from a State perspective. However, as verbalized by the State participants within several OCM meetings, there is a lack of State staff to assist with the OCM process overall. After reviewing the Deliverable Expectations Documents (DEDs) for the upcoming OCM deliverables, it has become evident that the State will need to identify a State OCM/Implementation Coordinator that will have the dedicated bandwidth to devote their time to coordination of the IEDSS implementation from both a people and a system perspective.

- The Training Team has started to present course module outlines and storyboards during Joint Training Review meetings. However, concerns have been raised regarding the accuracy of the IEDSS page information being utilized in the training design. At times, the information being presented isn't always based on the most current approved design document. While it is true that the Training Team is only allowed to use approved documentation for their design, there appear to be gaps or inaccurate information being incorporated into the coursework. Components of the design for the courses have been completed based on the functionality within the DEV environment which isn't always accurate. This leads to a greater concern about how the Training Team plans on staying current with design changes, defects, and CRs. As the project gets closer to rollout, time will not allow for substantial rework. The Vendor would benefit from a more structured method of information share between the track leads and the Training Team.

- The RCR CDMS Team reported issues with access to the IEDSS environment for the purpose of conducting unit and system testing. Numerous emails have been exchanged, and while there is some limited access, they do not have the full access that they require. Failure to provide this access could have a negative impact on their testing schedule.

- The DDI Vendor has not provided any Integration Test cases to the State or IV&V to begin the review process prior to the start of Integration testing. With Integration testing scheduled to start within the next few months, it is critical that DFR be provided with sufficient time to review the test cases prior to the start of Integration Testing to assure that there is adequate test coverage.

General Testing Observations

- There continues to be no documentation in RQM as to why test cases are being de-scoped. Because of this lack of documentation, test case de-scoping by the DDI Vendor remains a concern. There are currently 638 test cases de-scoped for Release 1-4. The DDI Vendor did provide a definition for "de-scoped" test cases in the System Test Summary Report submitted in June. The definition is limited to a general understanding of what a de-scoped test case is, rather than provide specifics as to why each test case was classified as "de-scoped".

- Due to the low test case pass percentages for Change Request Code Drop 1, as noted below, IV&V continues to strongly recommend the State request a Quality Assessment by the DDI Vendor of their development and unit test processes. Deloitte's development and unit test processes appear to be ineffective as demonstrated by the poor quality of code being promoted to the System Test environment.

System Test

- System test defect remediation and re-testing continued through June for the first four code releases and CR-1.

- In June, the DDI Vendor provided IV&V a list of the change requests associated with CR-1. IV&V is reviewing this list and other change requests to insure they are tested accordingly.

Below is the end of month snap shot of the Stage 2 System Test progress.

Release	Scheduled Completion	Actual Completion	Comments
Release 1	01/09/2015	March 2015	Test case execution completed in March. Retesting continues in June as defects are corrected.
Release 2	02/04/2015	April 2015	Test case execution completed in April. Retesting continues in June as defects are corrected.
Release 3	02/20/2015	April 2015	Test case execution completed in April. Retesting continues in June as defects are corrected.
Release 4	02/27/2015	April 2015	Test case execution completed in April. Retesting continues in June as defects are corrected.
System Test Phase	02/27/2015	April 2015	Test execution was reported as complete for the first four code drops (R1-R4); defect remediation is ongoing. With the exception of CR1 noted below the DDI Vendor has not, however, provided the scope and time frame for testing the remaining modules for system testing.
System Test CR1	Not yet designated	May 2015	Change Request Release 1 code testing commenced in April. The DDI Vendor completed Cycle 1, 2, and 3 at the end of May. The completed test case results reported were remarkably low, as noted below. Retesting continues in June as defects are corrected.

- The DDI Vendor stated in project steering committee meetings, they plan on executing test cases in System Test until each Cycle 3 pass rate is 100%, resolving any Critical, High and Medium defects. However, the DDI Vendor has not committed in writing any plans to resolve 'Medium' defects for future test phases (INT and UAT). Current pass rates indicate an effort is being made to reach the 100% goal. Of the 6,160 defects logged, only 13 remain unresolved.

- IV&V remains concerned the CR Code Drop 1 pass percent results are remarkably low for each of the three CR 1 test cycles. The highest pass percent was for Code Drop 1, Cycle 2, at only 31%; Cycle 1 and Cycle 3 were lower at 30% and 23% respectively. These low pass percent numbers are troubling and are indicative of issues within the DDI Vendor's development and unit test processes.

The table below displays the DDI Vendor reported results for system testing at the end of June compared to the end of May, indicating defect remediation is an ongoing effort by the DDI Vendor.

Cycle	Pass Rate Rel 1	Test Case Exec % Comp	Pass Rate Rel 2	Test Case Exec % Comp	Pass Rate Rel 3	Test Case Exec % Comp	Pass Rate Rel 4	Test Case Exec % Comp	Pass Rate Rel CR1	Test Case Exec % Comp
System Test Results										
1 (May)									22.9	100
(June)									20.4	100
2 (May)									31.3	100
(June)									28.7	100
3 (May)	97.2	100	96.2	100	90.8	100	79.5	100	30.3	100
(June)	99.9	100	99.9	100	99.8	100	97.6	100	31.0	100

Defect Reporting

- The DDI Vendor reported on June 30th-99.7% (6,147) of the 6,160 identified System Test application defects were mitigated or repaired, leaving 0.3% (13) to be resolved. This is the fourth month where improvement in the number of defects being resolved is observed.

- Of the 13 unmitigated defects, 12 are at least 30 days old. This number has decreased from 119 at the end of May. There is only 1 unrepaired application defect at least 12 days old. The following chart depicts the number of application defects that are at least 30 days old and unmitigated.

Defect Aging	Critical	High	Medium	Low	Total
30+ Days Old	0	0	10	2	12

- The number of open Stage 2 "design document defects" has again decreased slightly this month. At the end of May there were 748 document defects opened, and for

June, the number decreased to 585. These are in addition to the 13 unresolved application defects noted above.

Design Defects	January	February	March	April	May	June
Number Open	412	817	1,084	1,067	748	585

- The document defects are attributed to design defects discovered in either a PSDD or DSDD. The DDI Vendor has documented a process on how design document defect remediation recommendations will be reviewed and/or approved by the State. The design and document defects are reviewed during track touch point meetings for those tracks that have design document defects. Once reviewed, an action item is opened in Project Management Control (PMC) for the SMEs to approve the changes to the design document. The DDI Vendor reports they are reviewing and resolving these on a track by track basis. IV&V met with the DDI Vendor in June to confirm the process is being followed. IV&V will continue to monitor the remediation of the design document defects.

IV&V is concerned with the high number of design document defects still open and the rate at which they are being addressed. Development of invalid test scenarios and test cases for Integration Test and User Acceptance Test could be possible due to incorrect design documents being used. There is an additional concern that there may not be enough State resources allocated to reviewing these defects. Additionally, we have found that defects initially determined to be application defects are changed to design document defects without sufficient documentation for the reason for the change. While this may be appropriate in some cases, it is not always apparent why the change was made due to lack of documentation in the project tracking tool (RTC).

Integration Test

- No testing activity has transpired in the Integration Test environment since mid-March.

Other Testing

- Conversion unit testing is underway. Conversion update meetings are being held with the State to provide the status of the testing activities.

Master Test Plan

- IV&V continues to monitor any actions in regards to our review conducted in November of whether the processes and associated artifacts with Stage 2 System Test are in compliance with the Stage 2 Master Test Plan, and other project deliverables. We also verified Stage 2 testing compliance with the IEDSS Stage 2 project planning effort and integration with the IEDSS Project Management plan.

- A report of similar content of what follows was provided to State Project Leadership in February. IV&V will continue to monitor the DDI Vendor's remediation effort of these items. Since February, IV&V has indicated that "A draft of the proposed changes should be provided by the DDI Vendor before a decision is entered"; however, Deloitte has not provided any proposed changes.

  1. The DDI Vendor is using statuses to track defects other than what has been approved in the Stage 2 Master Test Plan.
     a. The DDI Vendor still needs to correct the Stage 2 Master Test Plan.
  2. Rational Jazz Suite has multiple incidents where defect attributes cannot show traceability, are incorrectly identified, or the release code is not identified.
     a. This item is still outstanding.
  3. The DDI Vendor is not recording the cycle a defect is detected in Rational Jazz Suite
     a. This has been partially corrected. The DDI Vendor has added a drop down box for 'cycle' in Rational Jazz Suite, but the DDI Vendor uses it sporadically.
  4. The DDI Vendor is not following the defect lifecycle process as stated in the Stage 2 Master Test Plan.
     a. This item is still outstanding. The DDI Vendor has assigned a decision item (#268804) in PMC to the State for the changes to occur. A draft of the proposed changes should be provided by the DDI Vendor before a decision is entered.
  5. The DDI Vendor is not following the Test Case Creation and Test Case Preparation process as outlined in the Master Test Plan
     a. This item is still outstanding. The DDI Vendor has assigned a decision item (#268804) in PMC to the State for the changes to occur. A draft of the proposed changes should be provided by the DDI Vendor before a decision is entered.
  6. The System Test scope as outlined on pages 32-34 in the Stage 2 Master Test Plan is not in alignment with the Master Project schedule and other information provided by the DDI Vendor, such as project weekly statuses, and the expectations of what is included in each of the four System Test code releases.
     a. This item is still outstanding. The DDI Vendor has assigned a decision item (#268804) in PMC to the State for the changes to occur. A draft of the proposed changes should be provided by the DDI Vendor before a decision is entered.
  7. The various test phases Entrance and Exit Criteria conflicts with the Master Project Plan/Schedule.
     a. This item is still outstanding. The DDI Vendor has assigned a decision item (#268804) in PMC to the State for the changes to occur. A draft of the proposed changes should be provided by the DDI Vendor before a decision is entered.
  8. The expected Test Reports identified in the Stage 2 Master Test Plan are not being delivered as Expected.

   a. This item is still outstanding. The DDI Vendor has assigned a decision item (#268804) in PMC to the State for the changes to occur. A draft of the proposed changes should be provided by the DDI Vendor before a decision is entered.

9. The defect escalation/triage process, as outlined in the Stage 2 Master Test Plan is not being followed.
   a. This item is still outstanding.
10. There is concern the DDI Vendor has not documented what a test cycle is and how it will be used in the planning of test case execution. There is no established entry and exit criterion for each testing cycle.
   a. This item is still outstanding.
11. The Medium Defects logged in RQM are not in compliance with the Stage 2 Master Test Plan.
   - Medium defects are not documented with a 'workaround' as designated by the Stage 2 Master Test Plan

4.0 Activities Performed

The following table describes each activity performed and its status:

Project Component	Activity	Status
Project Management	➢ Attended DFR Help Desk meetings ➢ Attended IEDSS Steering Committee meetings ➢ Attended Eligibility Change Implementation Team (CIT) meeting ➢ Attended IEDSS IAPD update meeting ➢ Reviewed proposed Change Requests ➢ ➢ Provided status of performance metrics for DFR ➢ Attended and participated in CMS IN SOTA calls ➢ Delivered IV&V Monthly Report for May ➢ Held the Monthly IV&V Briefing ➢ Reviewed and provided comments on the proposed CR Tracking Tool	Ongoing
Elaboration: Requirements	➢ Reviewed and provided comments on: ○ DPS005 Notify Documents Received Interface Requirements & File layout ○ DPS004 Document Upload and Save Correspondence Interface Requirements & File layout ➢ Attended DPS 006 Notify Applications Received Requirements Walkthrough ➢ Participated in RRC Review of Requirements for CR 286400 – Adding VAN to SVES ➢ Attended DPS/OHA Decision Document Upload Requirements session (UI Spec also presented)	Ongoing
Elaboration: Design	➢ Attended the following IEDSS JAD Sessions: • Front Office - 2032 Perdue Verification (1 Session) • Interfaces - CDEE File, Case Interface Match Summary Screen, NDNH (6 Sessions) • Super JAD - HIP Lockout (ED/FO/CO) (1 Session) • Correspondence - Authorization for Release of Medical Information, TANF Discontinuance/Apply for SSA, ABAWD,	Ongoing

Project Component	Activity	Status
	Managed Care Form, HIP 2.0 MAPC, HIP Link (6 Sessions) ➢ Reviewed the following session minutes and post session documents and provided comments: • Interfaces - CDEE File, Case Interface Match Summary Screen, NDNH • Super JAD - HIP Lockout (ED/FO only) • Correspondence - TANF Discontinuance/Apply for SSA, ABAWD ➢ Reviewed and provided comments on updated Self Service IR12, Account Retrieval/Password Reset ➢ Attended Comment Walkthrough for EDBC IR14, Change Requests ➢ Reviewed and provided comments on Correspondence IR25, Email and Text Notification Send Notification and Receive Failure ➢ Attended Walkthrough of Draft Requirements / Database Traceability Matrix - Artifact ➢ Attended State Approach for Data Mapping Meeting (Conversion) ➢ Attended Data Conversion and Load Plan Walkthrough ➢ Reviewed and provided comments on Conversion Load resubmission deliverable ➢ Attended Conversion Reference Code Mapping working session ➢ Reviewed IEDSS_AED Application Vulnerability Assessment ➢ Reviewed and provided comments on DPS002 – Retrieve Documents List ➢ Reviewed and provided comments on DPS004 Document Upload and Save Correspondence File Layout v0 04 ➢ Reviewed and provided comments on Support - IR14 - Quality Control ➢ Reviewed and provided comments on DPS – Document Indexing Process Flow diagram v0.09 ➢ Attended Manual Correspondence IR walkthrough/design sessions ➢ Attended BPM Sessions ➢ Attended weekly Touch Point/Defect meetings per track as scheduled	

Project Component	Activity	Status
Construction: Development	➢ Attended and participated in IEDSS Infrastructure meetings ➢ Attended and participated in Configuration Management Status meetings ➢ Attended IEDSS Weekly Stage I Defect Management Meetings ➢ Participated in track specific Touch Point meetings ➢ Reviewed and commented on UTSC resubmission	Ongoing
Construction: Test	➢ Monitored System Testing execution and results ➢ Attended System Test Summary Report - Walkthrough ➢ Attended the weekly Defect Triage meeting	Ongoing
Transition: UAT	➢ No activities this month	Ongoing
Transition: Training	➢ Attended weekly training meetings ➢ Attended Joint Training Review Design Meetings ➢ Reviewed Training Modules Course Outlines and Storyboards	Ongoing
Transition: Deploy	➢ Attended Organizational Change Management meetings ➢ Attended Organizational Change and Transition Support (OCTS) DED Comment Walkthrough ➢ Participated in Change Network Working Session ➢ Participated in Operational Readiness Plan DED Walkthrough ➢ Reviewed/commented on Operational Readiness Plan DED ➢ Reviewed Midpoint Survey ➢ Attended Conversion update meetings	Ongoing

The following table describes the IV&V tasks and the progress for each:

Task #	Task Item	Task Summary	IV&V Activity
Project Planning			
3	Systems Environment	Verify appropriate system environments are in place and updated.	IV&V observed that the DDI Vendor & IOT changed Stage I SFTP file exchanges (VLP, Account Transfer, VCI, HIP Link and eDRS) from mysftp server to securesftp server. IV&V noted that FSSA directed the DDI Vendor to monitor all the sixteen JVM's logs of Corticon Application Server in Stage 1 post code deployment after occurrence of the COMMERRs incident on June 29th, 2015.
4	Detailed Project Work Plan	Verify that the DDI Contractor's Detailed Project Work Plan addresses each phase of the System Development Life Cycle (SDLC).	IV&V has noted that the DDI Contractor's Detailed Project Work Plan is no longer accurate and is not being updated at this time. Awaiting the re-planning effort once final agreement is reached for what functionality is to be included for delivery on Day 1. The DDI Vendor was expected to deliver a high level schedule no later than June 30; however, they failed to meet that deadline. A new date for delivery has not been provided, putting the August 14 date for delivery of the detailed WBS/MS Project schedule at risk..
System Design Verification			
12	Design	Verify that the DDI Contractor's design and analysis process is in place and used to develop the design.	This has been verified. The concerns with aspects of the design and analysis process are documented in Observations earlier in this report.
13	Interfaces	Verify data interfaces and integration with the overall system design.	Interface change request design sessions continued in June and have included discussions regarding the impacts to other system components. The Account Transfer Preliminary System Design (PSD) final approval is pending with FSSA -OMPP. IV&V noted that correspondence is not required to be triggered for FFM Account Transfer Interface and the PSD was updated accordingly.

Task #	Task Item	Task Summary	IV&V Activity
14	Requirements Traceability	Verify that business and technical requirements can be traced forward to system and business area design elements.	During the review of the Detailed System Design Documents, traceability of requirements is verified. The Requirements Traceability Database Matrix is also reviewed and verified when delivered after each SDLC phase. A preliminary version of the RTDM for Design and Construction was provided in June with an expectation that the official deliverable will be provided in July.
15	Requirements Traceability	Verify that required processes and tools are in place in accordance with the appropriate RFP business and technical requirements, as updated through requirements validation and design phases of the project.	The DDI Vendor continues to use RRC as the requirements repository and traceability tool.
17	Design Standards	Verify DDI Contractor design standards, methodology and tools used to develop the design are in place and appropriate for the tasks at hand.	IV&V continues to monitor the design standards as the project moves forward. The DDI Vendor has provided a link to other internal documents being used for the data fields being used in the development of Correspondence and Reports. These documents should be formally submitted to, reviewed and approved by the State.
18	Security Requirements	Validate the project policies and procedures for ensuring that the system is secure meets the State's IT security requirements, and ensure that the privacy of client data is maintained through these policies and procedures.	IV&V has noted that the DDI Vendor, the DFR and the FSSA Privacy Office are evaluating the client information (HIPAA/PHI) that needs to be protected.
19	Security Requirements	Verify the DDI Contractor's project security plan and risk analysis processes comply with the State's IT security requirements.	IV&V participated in QRadar AED discussion and reviewed Application Vulnerability Assessment Report Artifact Expectations Document (AED) and Security Information and Event Management (SIEM) Implementation Artifact Expectations Document (AED).

Task #	Task Item	Task Summary	IV&V Activity
21	Gap Analysis	Verify that the agency hosting the IEDSS system (Indiana Office of Technology - IOT) is implementing IT security processes as required, and that there are no deficiencies in IOT's security processes for the IEDSS where Federal (e.g. HIPAA) and State laws might impose security requirements.	FSSA decided and directed the DDI Vendor to mask production data if it is leveraged for Conversion or Functional Testing.
Construction and Testing			
22	Master Test Plan	Verify that the Master Test Plan meets IEDSS requirements, is appropriate for the IEDSS project, and is being used by the DDI Contractor to actively guide the DDI Contractor's approach to testing throughout the life cycle of the project.	IV&V continues to monitor the responses to the findings regarding the Master Test Plan. This month's status is discussed in the Observations Section.
23	System Integration Test	Verify the software artifacts, system documentation, test data, and the test plan confirms a robust and complete migration capability.	No activities for this month.
24	Test Results	Validate that the results of the test are providing solutions as expected.	System Test is continuing. IV&V continues to monitor and report on those activities. Details are provided in the Observations Section.
25	Interface Testing	Verify adherence to Application Architecture Standards as outlined in the RFP.	Interface integration testing has not started for Stage 2.
26	Technical Reviews	Verify the contractor is monitoring activities during the Construction and Unit Testing task using technical reviews and audits.	IV&V Reviewed the Unit Tested System Code revised submission and provided comments. Participated in preview of Code Browsing in RTC meeting.

Task #	Task Item	Task Summary	IV&V Activity
27	Test Scenarios	Verify the contractor's prepared comprehensive set of test scenarios, with applicable test cases and expected test results to test the migration, and conversion of all data and files.	Working with the DDI Vendor to identify and access the Test Scenarios to be verified, when submitted. IV&V's concerns relative to the non-submittal of Integration Test scenarios is documented in the Observations section.
28	Data Conversion Verification	Verify that DDI Contractor has demonstrated that all data required to support processing is available, accurate, and ready for operations.	IV&V reviewed the Data Conversion and Load Plan deliverable and provided feedback. IV&V participated in comment walkthrough resolution meetings.
Integration and System Testing			
29	System Integration Test	Validate the plans, requirements, environments, tools, and procedures used for unit, integration and system testing of system modules.	IV&V continues to monitor and report on System Test. Details are provided in the Observations Section No activities occurred for Integration Test during the month. Reviewed and commented on the UTSC. Attended walkthrough of the UTSC comments.
34	Operational Readiness Review	Verify the functional area checklist for Operational Readiness has been applied and go/no-go criteria have been met.	IV&V participated in the Operational Readiness Plan DED Walkthrough. IV&V reviewed Operational Readiness Plan Deliverable Expectations Document (DED) and provided comments.

5.0 Planned Activities (Next Two Months)

Project Component	Activity
Project Management	➢ Attend IEDSS Steering Committee meetings ➢ Attend IEDSS Project Status meetings ➢ Attend DFR Help Desk meetings ➢ Attend Eligibility Change Implementation Team (CIT) meetings ➢ Review Change Requests ➢ Attend Hybrid Steering Committee meetings ➢ Attend IEDSS Change Control Board meetings ➢ Review the DDI Vendor Monthly Status Report Deliverables (April, May, and June) ➢ Prepare and deliver monthly IV&V Reports ➢ Hold IV&V Monthly Management Briefings ➢ Attend IEDSS IAPD update meetings ➢ Review re-baseline Project Work Plan
Elaboration: Requirements	➢ Participate in requirements sessions as scheduled ➢ Review requirements documented as a result of the requirements sessions ➢ Review any work products submitted during the next two months
Elaboration: Design	➢ Participate in the design sessions as scheduled ➢ Participate in the design defects review meetings ➢ Review and comment on minutes and documentation from the JAD sessions ➢ Review Requirements Database Traceability Matrix ➢ Review any work products scheduled to be submitted during the next two months ➢ As requested by the State, complete a Quality Assessment of the development and unit test processes
Construction: Development	➢ Monitor the development phases for the various Systems Partners ➢ Participate in track specific Touch Point meetings ➢ Review Requirements Database Traceability Matrix ➢ Review Software Stage 2: Unit Tested System Code
Construction: Test	➢ Monitor System Test activities and results ➢ Monitor Integration Test activities and results ➢ Review System Test Summary Report ➢ Attend Integration Go/No Go meetings ➢ Review Integration Test Summary Report ➢ Review Performance Test Summary Report

Project Component	Activity
	➢ Review Test Scenarios and Test Cases ➢ Review updated Requirements Database Traceability Matrix ➢ Monitor and evaluate testing phases for IEDSS and the various Systems Partners
Transition: UAT	➢ Monitor any activities that occur
Transition: Train	➢ Review Training Related DEDs and Deliverables/Artifacts ➢ Participate in Stage 2 training related activities and Joint Training Design Meetings ➢ Review Online Help ➢ Review Training Materials – Instructor Led
Transition: Deploy	➢ Attend comment walkthroughs as scheduled ➢ Review Organizational Change Management DEDs and Deliverables/Artifacts ➢ Review revised Business Impact Analysis ➢ Review Updated Operations Documentation ➢ Review Security Information and Event Management Solution (SIEM) ➢ Review IRS Safeguard Procedures Report ➢ Review Operational Readiness Plan
Expected Meetings, Interviews, Needed Documentation	➢ Monthly Management Briefing

6.0 Performance Metrics

The following table lists the Performance Metrics as outlined in the Indiana Performance Measurement Plan based upon data currently available. See Appendix D – Project Metrics for the additional details.

Performance Measure	Source/Type of Data	Report Method	Frequency Collected/ Reported	Status
Open Action Items - Length of time to close action items , Past Due Aged (Average exceeds 30 days past due)	PMC	Monthly Status Report	Monthly	See Section 6.1.
Change Request Tracking - Number of Change Requests month over month, may be a key indicator of a potential negative impact on the budget and/or schedule	PMC	Monthly Status Report	Monthly	See Section 6.2.
Issues Aging – The number of days a critical or high issue is pending	PMC	Monthly Status Report	Monthly	See Section 6.3.
Deliverables % - Deliverables Completed / Planned	Project schedule	Monthly Status Report	Monthly	See Section 6.5.
Deliverables Review – Deliverables reviewed with defects	Deliverable Review worksheet	Monthly Status Report	Monthly	Defects were reported by IV&V for the reviewed deliverables during the reporting period.
Decisions - The status of Decisions by Priority, the average time to close a Decision, and the Decisions pending more than 30 days that were due in the reporting period	PMC	Monthly Status Report	Monthly	See Section 6.4.

6.1 Action Items Metrics

The table below shows the status of Action Items by Priority from project inception through June 30, 2015. The purpose of this metric is to track the number of Action Items that are being created and worked, specifically the Critical and High priority items. As depicted in the chart below, Action Items are being worked, as 2,479 of the 2,558 (97%) have been disposed (Cancelled or Closed). There were 53 new Action Items opened in June and 45 Closed or Cancelled. 41 of the 79 Action Items listed as In Progress, On Hold or New below had a due date prior to June. Additionally, the numbers depicted in the table below are the counts reported on June 30, 2015.

Status	Critical	High	Medium	Low	Grand Total
Cancelled	**1**	**16**	**106**	**1**	**124**
DDI Vendor	0	14	96	1	111
State	1	2	10	0	13
Closed	**34**	**224**	**2047**	**50**	**2355**
DDI Vendor	17	151	1502	42	1712
State	17	73	545	8	643
In Progress	**2**	**8**	**36**	**1**	**47**
DDI Vendor	1	4	24	1	30
State	1	4	12	0	17
New	**1**	**8**	**21**	**0**	**30**
DDI Vendor	1	1	9	0	11
State	0	7	12	0	19
On Hold	**0**	**0**	**2**	**0**	**2**
DDI Vendor	0	0	2	0	2
State	0	0	0	0	0
Grand Total	**38**	**256**	**2212**	**52**	**2558**
DDI Vendor	19	170	1633	44	1866
State	19	86	579	8	692

Note that there is a discrepancy between the actual New Action Items received during the month and the number designated as New in PMC as there are items that are labeled New in PMC that were received in months prior to June. The following Action Items have a status of 'New'; however, they have a Create Date of prior to June 2015:

Action Item Number	Create Date
279332	1/22/2015
301911	4/23/2015
257831	10/16/2014
260388	10/28/2014
270138	12/8/2014
297126	4/2/2015
269403	12/4/2014
290032	3/4/2015
305555	5/11/2015
305551	5/11/2015
309533	5/27/2015
309535	5/27/2015
309964	5/29/2015

The table below provides the number of days in which Action Items are resolved. As the table below depicts, almost half of the all Action Items to date have been resolved in 15 days or less and two thirds were resolved within 30 days.

Days to Resolve	Count	Percentage	Cumulative
0-5 Days	564	23%	23%
6-10 Days	365	15%	37%
11-15 Days	214	9%	46%
16-20 Days	145	6%	52%
21-30 Days	335	14%	65%
31-60 Days	425	17%	83%
61-90 Days	200	8%	91%
+91 Days	231	9%	100%
Totals	2479	100%	

The table below shows the average number of days to close an Action Item from project inception through June 30, 2015. In addition to the number of Action Items being worked, it is critical that they be worked in a timely manner. There were thirty-four Action Items identified as Critical and the average closure was 58 days.

Status	Critical	High	Medium	Low
Closed	58 Days	40 Days	33 Days	34 Days

The table below shows the Action Items pending over 120, 90, 60 and 30 days with a due date prior to June. Critical and High Action Items that pend for over 30 days could have a negative impact on the project schedule. Currently, there are 40 Action Items with Priority of Critical, High or Medium with a past due date of over 30 days, up from 34 last month. The Action Items pending over 120 days are contained in Appendix C and should be reviewed as they may be able to be closed or have the due date moved out.

Priority	Over 120	Over 90	Over 60	Over 30	Grand Total
Critical	**2**	**0**	**0**	**0**	**2**
DDI Vendor	2	0	0	0	2
State	0	0	0	0	0
High	**9**	**1**	**1**	**0**	**11**
DDI Vendor	3	0	0	0	3
State	6	1	1	0	8
Medium	**14**	**2**	**0**	**11**	**27**
DDI Vendor	8	2	0	6	16
State	6	0	0	5	11
Low	0	0	0	1	1
Deloitte	0	0	0	1	1
Grand Total	**25**	**3**	**1**	**12**	**41**
DDI Vendor	13	2	0	7	22
State	12	1	1	5	19

6.2 Change Requests

The table below shows the status of Change Requests by month.

Status	Tot 2013	Tot 2014	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Tot
Submitted	111	202	24	18	10	11	8	4							388
Approved	57	106	3	3	6	6	1	3							185
Pending	36	25	41	54	56	60	65	61							61
Cancelled	14	60	1	1	0	1	2	5							84
Deferred	0	26	1	0	2	0	0	0							29
Rejected	4	21	3	1	0	0	0	0							29
Total to Date	111	313	337	355	365	376	384	388							388

6.3 Issue Metrics

The table below shows the status of Issues by Priority from project inception through June 30, 2015. The purpose of this metric is to track the number of Issues that are being created and worked, specifically the Critical and High priority items. As depicted in the chart below, Issues are being worked, as 266 of the 293 (91%) have been disposed (Cancelled or Closed). There were 6 new issues added to the Issue Log in June and 5 Issues were closed during the month. 20 of the 27 Issues listed as In Progress or New below had a due date prior to June. The numbers depicted in the table below are the counts reported on June 30, 2015.

Status	Critical	High	Medium	Low	Grand Total
Cancelled	**4**	**13**	**6**	**0**	**23**
DDI Vendor	3	11	6	0	20
State	1	2	0	0	3
Closed	**65**	**120**	**57**	**1**	**243**
DDI Vendor	44	96	52	1	193
State	21	24	5	0	50
In Progress	**7**	**13**	**1**	**0**	**21**
DDI Vendor	4	10	0	0	14
State	3	3	1	0	7
New	**2**	**4**	**0**	**0**	**6**
DDI Vendor	1	3	0	0	4
State	1	1	0	0	2
Grand Total	**78**	**150**	**64**	**1**	**293**
DDI Vendor	52	120	58	1	231
State	26	30	6	0	62

Note that there is a discrepancy between the actual New Issues received during the month and the number designated as New in PMC as there are items that are labeled New in PMC that were received in months prior to June. The following Issues have a status of 'New'; however, they have a Create Date of prior to June 2015:

Issue Number	Create Date
290003	3/4/2015
294809	3/24/2015
290002	3/4/2015
291098	3/10/2015

The table below provides the number of calendar days in which Issues are resolved. As the table depicts, more than 40% of the all Issues to date have been resolved in 20 days or less and nearly 60% were resolved within 30 days.

Days to Resolve	Count	Percentage	Cumulative
0-5 Days	37	14%	14%
6-10 Days	24	9%	23%
11-15 Days	34	13%	36%
16-20 Days	14	5%	41%
21-30 Days	40	15%	56%
31-60 Days	47	18%	74%
61-90 Days	31	12%	85%
+91 Days	39	15%	100%
Totals	266	100%	

The table below shows the average number of days to close an Issue from project inception to June 30, 2015. In addition to the number of Issues being worked it is critical that they be worked in a timely manner.

Status	Critical	High	Medium	Low
Closed	62 Days	51 Days	34 Days	0 Days

The table below shows the Issues pending over 120, 90, 60 and 30 days with a due date prior to June. There are currently nineteen Issues pending over 30 days (versus 16 last month). See Appendix D for a list of all Issues pending over 120 days.

Priority	Over 120	Over 90	Over 60	Over 30	Grand Total
Critical	**5**	**0**	**1**	**1**	**7**
DDI Vendor	3	0	1	1	5
State	2	0	0	0	2
High	**7**	**0**	**1**	**3**	**11**
DDI Vendor	6	0	1	3	10
State	1	0	0	0	1
Medium	**1**	**0**	**0**	**0**	**1**
DDI Vendor	0	0	0	0	0
State	1	0	0	0	1
Grand Total	**13**	**0**	**2**	**4**	**19**
DDI Vendor	9	0	2	4	15
State	4	0	0	0	4

6.4 Decision Metrics

The table below shows the status of Decisions by Priority from project inception through June 30, 2015. The purpose of this metric is to track the number of Decisions that are being created and worked, specifically the Critical and High priority items. As depicted in the chart below, Decisions are being worked, as 511 of the 539 (95%) have been disposed. There were 12 new Decision Items opened in June and 18 Closed or Cancelled. Of the 28 Decision Items listed as In Progress, New, Pending Approval, or On Hold below, 27 have a due date prior to June. The numbers depicted in the table below are the counts reported on June 30, 2015.

Status	Critical	High	Medium	Low	Grand Total
Cancelled	**13**	**11**	**80**	**0**	**104**
DDI Vendor	12	9	50	0	71
State	1	2	30	0	33
Closed	**53**	**112**	**216**	**26**	**407**
DDI Vendor	21	77	110	6	214
State	32	35	106	20	193
In Progress	**2**	**4**	**5**	**0**	**11**
DDI Vendor	0	3	3	0	6
State	2	1	2	0	5
New	**0**	**0**	**2**	**0**	**2**
DDI Vendor	0	0	1	0	1
State	0	0	1	0	1
On Hold	**0**	**0**	**1**	**0**	**1**
DDI Vendor	0	0	0	0	0
State	0	0	1	0	1
Pending Approval	**2**	**10**	**2**	**0**	**14**
DDI Vendor	1	10	0	0	11
State	1	0	2	0	3
Grand Total	**70**	**137**	**306**	**26**	**539**
DDI Vendor	34	99	164	6	303
State	36	38	142	20	236

The following Decisions have a status of 'New'; however, they have a Create Date of prior to June 2015:

Decision Number	Create Date
224190	5/23/2014
309138	5/26/2015

The table below provides the number of days in which Decisions are resolved. As the table depicts, more than half of all Decisions to date have been resolved in 30 days or less and more than three quarter were resolved within 60 days.

Days to Resolve	Count	Percentage	Cumulative
0-5 Days	104	20%	20%
6-10 Days	82	16%	36%
11-15 Days	35	7%	43%
16-20 Days	23	5%	48%
21-30 Days	56	11%	59%
31-60 Days	91	18%	77%
61-90 Days	57	11%	88%
+91 Days	63	12%	100%
Totals	511	100%	

The table below shows the average number of days to close or cancel a Decision from project inception to June 30, 2015. In addition to the number of Decisions being worked it is critical that they be worked in a timely manner.

Status	Critical	High	Medium	Low
Closed	46 Days	71 days	35 Days	23 days

The table below shows the Issues pending over 120, 90, 60 and 30 days with a due date prior to June. There are 27 Decisions pending over 30 days; 18 of which are Critical or High. The Decisions pending over 120 days are contained in Appendix E and should be reviewed as they may be able to be closed or have the due date moved out.

Priority	Over 120	Over 90	Over 60	Over 30	Grand Total
Critical	**4**	**0**	**0**	**0**	**4**
DDI Vendor	1	0	0	0	1
State	3	0	0	0	3
High	**12**	**0**	**2**	**0**	**14**
DDI Vendor	11	0	2	0	13
State	1	0	0	0	1
Medium	**7**	**0**	**2**	**0**	**9**
DDI Vendor	2	0	2	0	4
State	5	0	0	0	5
Grand Total	**23**	**0**	**4**	**0**	**27**
DDI Vendor	14	0	4	0	18
State	9	0	0	0	9

The table below shows the number of Action Items, Issues, and Decisions Closed/Cancelled by month for the previous 13 months.

Closed/Can	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun 15
Action Items	66	16	40	51	57	40	28	56	37	38	42	47	45
Issues	14	13	4	14	17	9	8	8	7	3	1	10	5
Decisions	12	8	3	19	15	13	8	17	18	8	12	9	18

6.5 Schedule Review

During June, the following past due Deliverables/Artifacts were submitted:

- System Test Summary Report

The following Deliverables/Artifacts were past due:

- Requirements Database Traceability, Design and Construction
- Security Information and Event Solution (SIEM)
- Performance Test Summary Report
- Integration Test Summary Report
- Data Conversion and Load Testing

- Organizational Transition Plan – Pilot
- IRS Safeguard Procedures Report
- Training Materials – Instructor Led
- Operational Readiness Plan

The following revised Deliverables/Artifacts were received for re-review:

- Unit Tested System Code
- DDI Vendor's March Monthly Project Status Report
- Data Conversion and Load Plan
- DDI Vendor's April Monthly Project Status Report

The table below show deliverables planned and completed for the month. The table only reports on the initial delivery or initial response of the deliverable.

Deliverable	Planned Submission Date	Revised Submission Date	Actual Submission Date	State Response Due Date	State Requested Response Date	State Actual Response Date
Monthly Status Report – May	6/1/15					
Integration Test Summary Report	6/5/15					
Data Conversion and Load Testing	6/12/15	8/7/15				
Organizational Transition Plan – Pilot	6/12/15	7/2/15				
Updated Requirements Database Traceability Matrix – Testing	6/19/15	8/28/15				
IRS Safeguard Procedures Report	6/19/15	8/4/15				
Training Materials – Instructor Led	6/26/15					
Operational Readiness Plan	6/26/15	7/24/15				
Metrics	**Planned**	**Completed**	**Percent**			

Deliverable	Planned Submission Date	Revised Submission Date	Actual Submission Date	State Response Due Date	State Requested Response Date	State Actual Response Date
Monthly Deliverables	8	0	0%			
Metrics	On Time	Late	Percent On Time			
Deliverable Timeliness	0	8	0%			
Metrics	On Time	Late	Percent On Time			
State Response Timeliness	0	0	0%			

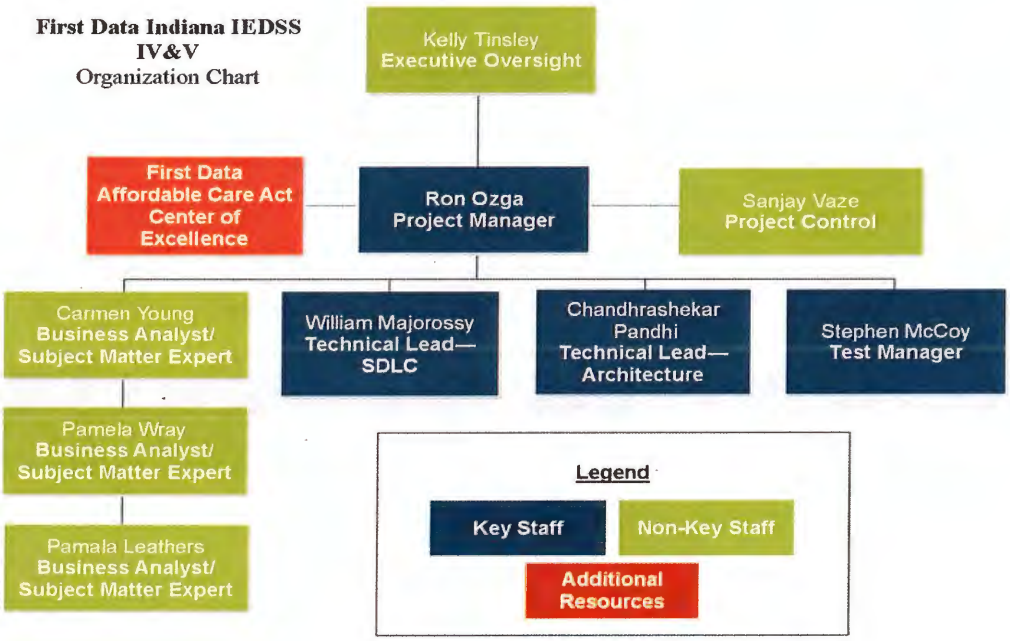
The table below lists milestones or critical path tasks that were scheduled for completion during this or prior reporting periods that were not completed per schedule and still show as being active in the work schedule as of the end of the reporting period. This is based upon the Baseline Start and Finish Dates.

Task	Name	Scheduled Start	Scheduled Finish	Baseline Start	Baseline Finish
	Milestones				
5688	Submit RDTM Artifact (11/14/2014	06/26/2015	06/26/2015	11/14/2014	11/14/2014
5691	Re-submit RDTM Artifact for Approval	07/21/2015	07/21/2015	12/09/2014	12/09/2014
5693	State Acceptance of RDTM	07/28/2015	07/28/2015	12/16/2015	12/16.2014
5760	Stage 2 Design Complete	04/01/2015	04/01/2015	01/13/2015	01/13/2015
5888	Re-submit UTSC for Approval	6/10/2015	06/10/2015	02/13/2015	
5896	Submit RDTM Artifact (2/6/2015)	07/10/2015	07/10/2015	02/06/2015	02/20/2015
5912	AED Submission (Security Operations Documentation(SEIM)	06/10/2015	06/10/2015	03/06/2015	03/06/2015
5918	Submit SEIM Artifact for State Review (4/3/2015)	06/10/2015	06/10/2015	04/03/2015	04/03/2015
5920	Milestone – Security Operations Documentation (Procedures) Complete	06/24/2015	06/24/2015	03/06/2015	03/06/2015
5988	IRS SGP Submit to IRS (6/19/2015)	8/4/15	8/4/15	6/19/15	6/19/15
5989	Artifact - SPR Update for Stage 2 IEDSS Application Security Controls	8/3/15	8/3/15	6/18/15	6/18/15
5992	Go/No Go Phase (Development) Exit Decision	07/20/2015	07/20/2015	01/19/2015	03/06/2015

Task ID	Name	Scheduled Start	Scheduled Finish	Baseline Start	Baseline Finish
5993	Stage 2 Development Complete	07/20/2015	07/20/2015	01/19/2015	01/19/2015
6876	Submit System Test Sum. Report Deliverable (3/20/2015)	07/1/2015	07/1/2015	03/20/2015	03/20/2015
6879	Re-submit System Test Sum. Report Deliverable for Approval	07/24/2015	07/24/2015	04/10/2015	04/10/2015
7519	Submit Integration Test Summary Report DED	06/01/2015	06/01/2015	03/20/2015	03/20/2015
7524	Submit Integration Test Summary Report Deliverable (6/5/15)	6/5/2015	6/5/2015	6/5/2015	6/5/2015
7527	Re-submit Integration Test Summary Report Deliverable for Approval	6/26/2015	6/26/2015	6/26/2015	6/26/2015
7535	Submit RDTM Artifact (6/19/2015)	6/19/2015	6/19/2015	6/19/2015	6/19/2015
7545	Milestone - Qradar Integration Testing Complete	6/10/2015	6/10/2015	6/5/2015	6/5/2015
7549	Submit Performance Test Sum. Report DED	02/19/2015	02/19/2015	06/02/2014	06/02/2014
7612	Submit Performance Test Sum. Report Deliverable (5/29/2015)	05/29/2015	05/29/2015	05/29/2015	05/29/2015
7615	Re-submit Performance Test Sum. Report for Approval	6/19/2015	6/19/2015	6/26/2015	6/26/2015
7621	Submit Information Security Risk Assessment DED	04/17/2015	04/17/2015	03/31/2015	03/31/2015
7631	Submit Integrated Software DED	07/2/2015	07/2/2015	03/13/2015	03/13/2015
7636	Submit Integrated Software Deliverable (5/29/2015)	05/29/2015	05/29/2015	05/29/2015	05/29/2015
7639	Re-submit Integrated Software Deliverable for Approval	6/19/2015	6/19/2015	6/19/2015	6/19/2015
7696	Integration test Go/No Go Phase Exit Decision	6/2/2015	6/2/2015	6/2/2015	6/2/2015
7698	Start Stage 2 UAT Sub-Phase	03/30/2015	03/30/2015	03/30/2015	03/30/2015
7713	Submit Acceptance Confirmation DED	6/1/2015	6/1/2015	6/1/2015	6/1/2015
7736	Submit DLT&A(Data Load Tested and Approved) DED	5/14/2015	5/14/2015	5/15/2015	5/15/2015
7783	Submit Application Vulnerability Assessment Report DED	05/15/2015	05/15/2015	05/18/2015	05/18/2015
7805	Start Stage 2 Training Sub-Phase	06/29/2015	06/29/2015	12/23/2014	12/23/2014
7810	Submit Security Awareness Training DED	03/31/2015	03/31/2051	03/10/2015	03/10/2015
7816	State Approval of Training Materials Overall Package	6/2/2015	6/2/2015	6/2/2015	6/2/2015
7817	Milestone - Security Awareness Training Materials	6/2/2015	6/2/2015	6/2/2015	6/2/2015
7820	Milestone - Security Awareness Training	6/9/2015	6/9/2015	6/9/2015	6/9/2015
7856	Start Stage 2 Pilot	09/21/2015	09/21/2015	05/22/2015	05/22/2015

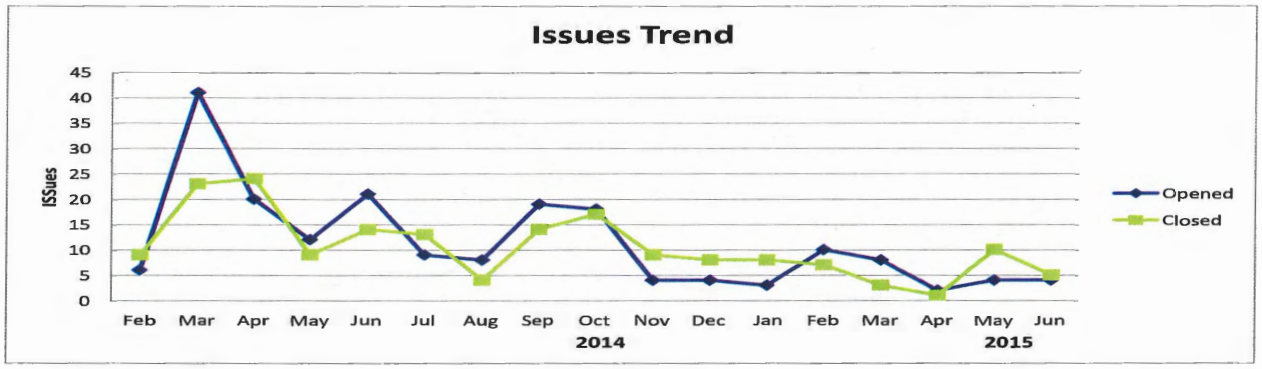
Task ID	Name	Scheduled Start	Scheduled Finish	Baseline Start	Baseline Finish
7865	Prod. Databases DED Submission	05/01/2015	05/01/2015	05/01/2015	05/01/2015
7897	Prod. Software DED Submission	05/01/2015	05/01/2015	05/01/2015	05/01/2015
7957	Submit OTP-Pilot Deliverable (6/12/2015)	8/4/2015	8/4/2015	6/12/2015	6/12/2015
8138	Submit Implementation Plan DED	08/07/2015	08/07/2015	04/17/2015	04/17/2015
8152	OR Plan DED Submission	06/22/2015	06/22/2015	04/16/2015	04/16/2015
8157	Submit OR Plan Deliverable (6/26/2015)	8/31/2015	8/31/2015	6/26/2015	6/26/2015
8247	Submit Training Materials Deliverable (6/26/2015)	8/28/2015	8/28/2015	6/11/2015	6/11/2015
8287	Submit WBT Training Materials Deliverable (9/25/2015)	8/26/2015	8/26/2015	6/10/2015	6/10/2015
8593	State Acceptance of Second Revised Data Conv. & Load Plan Deliverable	7/7/2015	7/7/2015	6/19/2015	6/19/2015
8600	Data Conv. & Load Testing (DC&LT) DED Submission	06/02/2015	06/02/2015	01/22/2015	01/22/2015
8601	DC&LT DED Approval	06/02/2015	06/02/2015	01/22/2015	01/22/2015
8605	Submit DC&LT Deliverable (6/12/15)	8/21/2015	8/21/2015	6/12/2015	6/12/2015
8606	State DC&LT Deliverable Review	8/21/2015	8/21/2015	6/12/2015	6/12/2015
8608	Re-submit DC&LT for Approval	8/28/2015	8/28/2015	6/19/2015	6/19/2015
09	Revised DC&LT State Review	8/28/2015	8/28/2015	6/19/2015	6/19/2015
8610	State Acceptance of DC&LT	8/28/2015	8/28/2015	6/19/2015	6/19/2015
Critical Path					

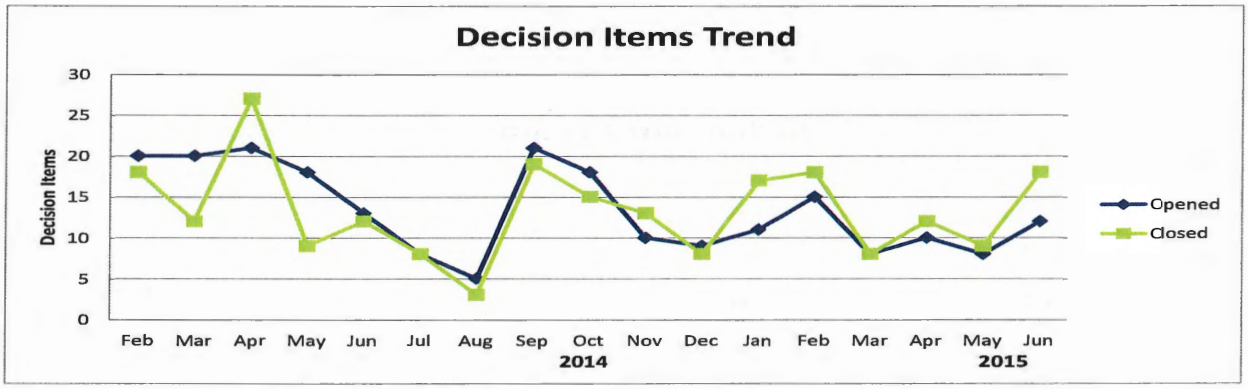
Appendix A – Current Organizational Chart

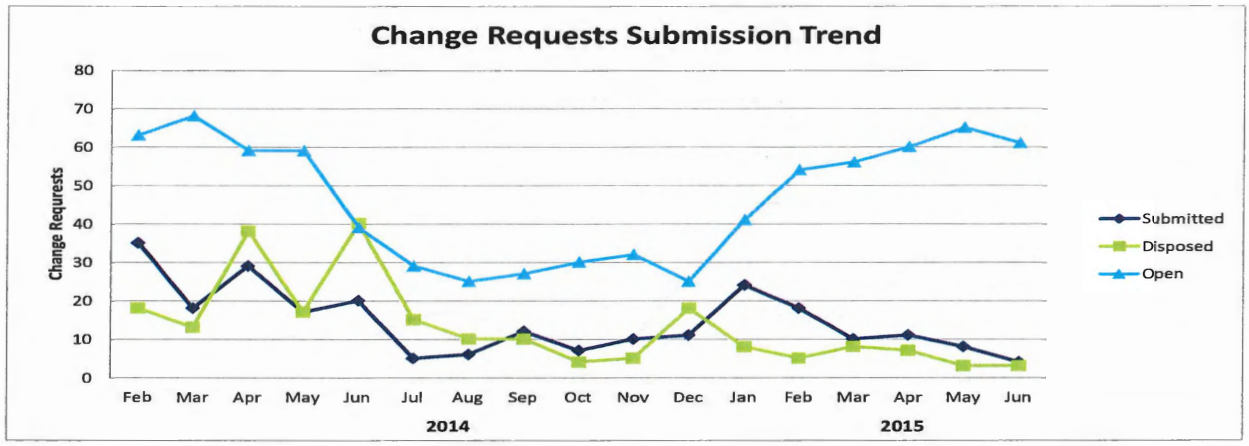


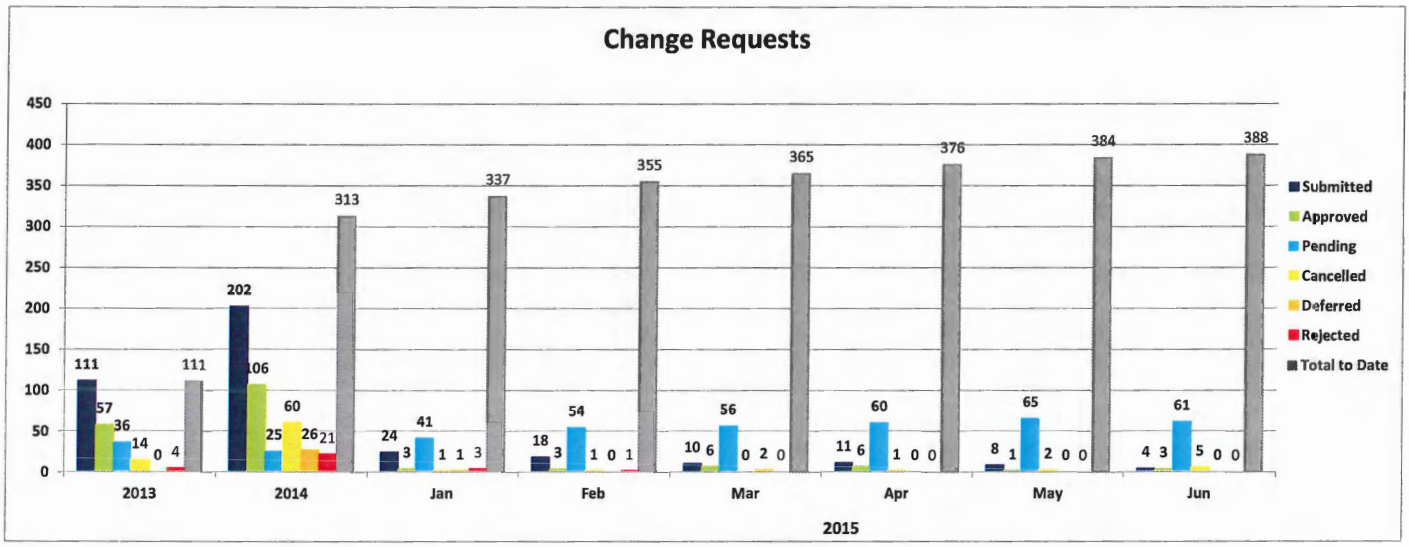
Appendix B – Project Metrics

Action Items, Issues, Decision Items and Change Requests Metrics




Decision Items Trend
Decision Items
30
25
20
15
10
5
0
Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun
2014
2015
Opened
Closed


Change Requests Submission Trend
Change Requrests
80
70
60
50
40
30
20
10
0
Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun
2014
2015
Submitted
Disposed
Open


Change Requests
450
400
350
300
250
200
150
100
50
0
111
57
36
14
0
4
111
202
106
25
60
26
21
313
24
3
41
1
1
3
337
18
3
54
1
0
1
355
10
6
56
0
2
0
365
11
6
60
1
0
0
376
8
1
65
2
0
0
384
4
3
61
5
0
0
388
2013
2014
Jan
Feb
Mar
Apr
May
Jun
2015
Submitted
Approved
Pending
Cancelled
Deferred
Rejected
Total to Date

Appendix C – Action Items Pending Over 120 Days

No.	Created On	Assigned To	State/Vendor	Priority	Status	Due Date	Days Pending
248152	9/8/2014	Abhinav Siriguri	Deloitte	Critical	In Progress	9/24/2014	279
270138	12/8/2014	Sreshta Wickramasinghe	Deloitte	Critical	New	12/12/2014	200
235649	7/16/2014	Sreshta Wickramasinghe	Deloitte	High	In Progress	7/30/2014	335
257709	10/16/2014	Sreshta Wickramasinghe	Deloitte	High	In Progress	10/30/2014	243
284207	2/12/2015	Matthew Vallorano	Deloitte	High	In Progress	2/25/2015	125
178274	10/24/2013	Leigh Van brecht	Deloitte	Medium	In Progress	4/4/2014	452
180680	11/4/2013	Kshama Chopra	Deloitte	Medium	In Progress	9/30/2014	273
251776	9/23/2014	Sreshta Wickramasinghe	Deloitte	Medium	In Progress	10/10/2014	263
286754	2/20/2015	Matthew Vallorano	Deloitte	Medium	In Progress	2/27/2015	123
285910	2/18/2015	Emil Hessel	Deloitte	Medium	In Progress	2/25/2015	125
279332	1/22/2015	Abhinav Siriguri	Deloitte	Medium	New	2/22/2015	128
283857	2/10/2015	Matthew Vallorano	Deloitte	Medium	In Progress	2/18/2015	132
272687	12/16/2014	Matthew Vallorano	Deloitte	Medium	On Hold	12/19/2014	193
236886	7/22/2014	Matthew Rager	State	High	In Progress	7/31/2014	334
257831	10/16/2014	Matthew Rager	State	High	New	10/21/2014	252
257411	10/14/2014	Sunshine Beam	State	High	In Progress	10/22/2014	251
262855	11/6/2014	Matthew Rager	State	High	In Progress	11/13/2014	229
260388	10/28/2014	Matthew Rager	State	High	New	11/26/2014	216
269403	12/4/2014	Sunshine Beam	State	High	New	12/12/2014	200
241725	8/11/2014	Sunshine Beam	State	Medium	In Progress	8/25/2014	309
252356	9/24/2014	Matthew Rager	State	Medium	In Progress	10/8/2014	265
253961	10/1/2014	Virginia Taylor	State	Medium	In Progress	10/15/2014	258
266445	11/24/2014	Sunshine Beam	State	Medium	In Progress	2/28/2015	122
281807	2/3/2015	Sunshine Beam	State	Medium	In Progress	2/6/2015	144
281989	2/3/2015	Sunshine Beam	State	Medium	In Progress	2/6/2015	144

Appendix D – Issues Pending Over 120 Days

No.	Created On	Assigned To	State/Vendo	Priority	Status	Due Date	Days Pending
179532	10/30/2013	Sreshta Wickramasinghe	Deloitte	Critical	In Progress	4/11/2014	445
221888	5/14/2014	Akhil Dayal	Deloitte	Critical	In Progress	6/13/2014	382
263900	11/11/2014	Matthew Vallorano	Deloitte	Critical	In Progress	12/12/2014	200
193075	1/16/2014	Marat Bleykhman	Deloitte	High	In Progress	7/31/2014	334
245810	8/27/2014	Sreshta Wickramasinghe	Deloitte	High	In Progress	9/19/2014	284
284944	2/13/2015	Sreshta Wickramasinghe	Deloitte	High	In Progress	2/27/2015	123
290003	3/4/2015	Jamieson Ogle	Deloitte	High	New	2/20/2015	130
242459	8/13/2014	Jim Perez	Deloitte	High	In Progress	10/17/2014	256
254874	10/2/2014	Vishwa Halaharvi	Deloitte	High	In Progress	10/10/2014	263
283974	2/11/2015	Sunshine Beam	State	Critical	In Progress	2/17/2015	133
283501	2/10/2015	Sunshine Beam	State	Critical	In Progress	2/12/2015	138
130301	1/17/2013	Matthew Rager	State	High	In Progress	1/17/2014	529
215080	4/9/2014	Matthew Rager	State	Medium	In Progress	6/20/2014	375

Appendix E – Decisions Pending Over 120 Days

No.	Created On	Assigned to	State/ Vendor	Priority	Status	Due Date	Days Pending
213521	4/3/2014	Matthew Vallorano	Deloitte	Critical	Pending Approval	5/21/2014	405
175506	10/8/2013	Michelle Jang	Deloitte	High	Pending Approval	10/30/2013	608
181603	11/8/2013	Kevin Rollins	Deloitte	High	In Progress	11/22/2013	585
179759	10/30/2013	Kevin Rollins	Deloitte	High	Pending Approval	11/22/2013	585
179757	10/30/2013	Kevin Rollins	Deloitte	High	In Progress	11/22/2013	585
276729	1/12/2015	Vishwa Halaharvi	Deloitte	High	In Progress	1/23/2015	158
231298	6/24/2014	Michelle Jang	Deloitte	High	Pending Approval	12/31/2014	181
270544	12/9/2014	Sreshta Wickramasinghe	Deloitte	High	Pending Approval	12/16/2014	196
254618	10/2/2014	Nagendra P C R Panuganti	Deloitte	High	Pending Approval	10/10/2014	263
252727	9/25/2014	Sreshta Wickramasinghe	Deloitte	High	Pending Approval	10/10/2014	263
252654	9/25/2014	Vishwa Halaharvi	Deloitte	High	Pending Approval	10/10/2014	263
236233	7/19/2014	Rajesh Shanmugam	Deloitte	High	Pending Approval	7/25/2014	340
224190	5/23/2014	Abhinav Siriguri	Deloitte	Medium	New	10/20/2014	253
228483	6/13/2014	Matthew Vallorano	Deloitte	Medium	In Progress	6/27/2014	368
262746	11/6/2014	Matthew Rager	State	Critical	In Progress	11/12/2014	230
250324	9/16/2014	Sunshine Beam	State	Critical	Pending Approval	10/16/2014	257
177291	10/18/2013	Matthew Rager	State	Critical	In Progress	2/28/2014	487
284841	2/13/2015	Sunshine Beam	State	High	In Progress	2/20/2015	130
281808	2/3/2015	janet sanford	State	Medium	On Hold	2/13/2015	137
281806	2/3/2015	janet sanford	State	Medium	In Progress	2/6/2015	144
281805	2/3/2015	Katie Hunter	State	Medium	In Progress	2/6/2015	144
268804	12/3/2014	Virginia Taylor	State	Medium	Pending Approval	1/31/2015	150
222500	5/16/2014	Sunshine Beam	State	Medium	Pending Approval	5/23/2014	403

Appendix 8

First Data™
b›yond the transaction

Department of Children and Family Services

One DCFS Modernization Project

Go/No-Go Process

Contents

Go/No-Go Process 3
Readiness Checklist 3
Readiness Meetings 4
Release Readiness Checkpoints 4
Go/No-Go Meeting 5
Final Go/No-Go Meeting 5
Post Implementation Checkpoint Meetings ..... **Error! Bookmark not defined.**

Go/No-Go Process

The Go/No-Go decision process serves as the catalyst for Project Sponsors, Department Executives, Project Team Leaders and Integration Partners to validate that the system is stable and ready to be operational for implementation, staff are prepared to work in the new system and they have adequate tools to facilitate the transition. The Go/No-Go Process allows executives to evaluate implementation readiness from the perspective of all stakeholders and discuss the implications of outstanding items, and the impacts of not resolving them prior to Implementation.

The Go/No-Go Process involves both the monitoring of critical task progress and completion prior to implementation, as well as the assessment of incomplete tasks and project issues and risks. The monitoring of critical tasks in the months leading up to implementation will keep a pulse on the major arteries of the project. This will help prevent the late identification of incomplete tasks that "must" be completed prior to implementation. A Go/No-Go Meeting including the State Teams, PMO, Implementation Vendor(s) and the Quality Assurance Vendor will occur two weeks prior to implementation to confirm the overall readiness of the project. The vendors will evaluate why each project section is ready, and provide their professional recommendation for Go/No-Go to the State. The emphasis of this meeting is to evaluate the impact of tasks that were not completed, review Transformation Project issues and risks, and measure the impact of proceeding with the implementation. A Final Go/No-Go Meeting will occur 1-2 days in advance of the start of cutover activities to re-confirm entrance into implementation activities.

The Go/No-Go Process is the evaluation of the culmination of efforts from all of the functional teams, vendors, workers and project stakeholders to determine if the level of risk associated with unfinished tasks is acceptable to the State to proceed with the Transformation Release. The inputs to the Go-No Go decision include:

- **The Readiness Checklist** – An Excel Spreadsheet used to track the progress and completion of key or critical tasks.
- **DCFS Risk and Issue Report** – A project wide repository of risks and issues.
- **MS Project Work Plan**– A list of tasks that have not yet been completed, or will be completed prior to Implementation.

Readiness Checklist

A new process First Data is recommending to the State is the implementation of a Readiness Checklist. For each Transformation Release a Readiness Checklist should be created to track the progress or completion of key tasks (metrics). The metrics identified in the Readiness Checklist can define the criterion or thresholds acceptable for entrance to implementation. These metrics are reviewed at defined intervals (6 months, 5 months, 4 months, 3 months, 2 months, 1 month, 3 week, 2 week and/or 1 week) leading up to implementation. If a metric is marked as 6 months, it should be reviewed 6 months prior to

implementation. The frequency of reviews can vary depending on whether monitoring the progress of a metric is needed, or just validate that it completed.

The items included on the Readiness Checklist are metrics that can impact the overall success of the implementation, and the progress or status of these items are tracked using stoplight reporting incrementally leading up to Go Live. The PMO will assist the State in defining parameters around each metric that will show the measures of acceptability and will help the teams with evaluating whether the metric will have a Green, Yellow or Red status. In addition to the stoplight reporting the teams will need to evaluate the metrics attributed to their teams for a specific reporting period to provide a Comment/Status, the Evidence if a metric was completed, and any other relevant updates. There is not an exact science to determining the stoplight status of a metric, as there are both qualitative and quantitative aspects that can impact the effectiveness of the implementation; the emphasis is on reporting an accurate status.

For the Transformation Project *each* Release should have its own Readiness Checklist. This will allow the State to compartmentalize the readiness assessment respective to the functionality implemented during a Release. The Readiness Checklist criteria that are defined for each checklist will need to be validated by the State to ensure they are comprehensive and the frequency of the review is as expected.

The Readiness Checklist can help the State determine if they are ready for a Phase or a Release. The checklist will provide the Department with a mechanism to see at a high level any outstanding items and evaluate the risk of proceeding.

	Topic	Metric	Report Used to Measure	Strategy to Measure	Target Threshold	Responsible Tea	Comment/Status	Recommended Assessment Point(s)	Recommended Assessment Points										Evidence	Issue/Action Item #	Results
									6 Mo n	5 Mo n	4 Mo n	3 Mo n	2 Mon t	1 Mo n	3 Wee k	2 Wee k	1 We e				
	Change Readiness	Has a Change Readiness Action Plan for workers been developed?	Change Readiness Plan	Validate Change Readiness Plan exists		Change Readiness		4 Months			X										
	Change Readiness	Has the Release 1 Change Readiness Plan for CSRs been developed?		Validate Change Readiness Plan exists		ACS		3 Months				X									
	As is/To be	Have Business Processes for Release 1 been assessed?		Gap Analysis		Change Readiness		3 Months				X									
	As is/To be	Identify the Gap between the "As Is" and "To Be" processes for Release 1		Gap Analysis		Change Readiness		4 Months			X										
	As is/To be	Have new business process documents been developed to prepare staff for the changes identified in the Gap Analysis?		Business Process Guides		Change Readiness		3 Months, 2 Months, 1 Month				X	X	X							

***The status of the metrics provided in the Figure are not representative of the status of the actual tasks.*

Readiness Meetings

Tracking Project Readiness is not meant to create additional work or meetings for the project teams but rather be a tool to help facilitate the readiness process. Readiness Checkpoint reviews should be included in regularly scheduled meetings for the project teams to update statuses and presented to ESC so executives receive the statuses.

Release Readiness Checkpoints

The review of the Readiness Checklists will follow the defined intervals for assessment (6 months, 5 months, 4 months, 3 months, 2 months, 1 month, 3 week, 2 week and/or 1 week). The initial creation of the metrics and any ongoing additions will need to be

reviewed with the project teams to ensure the metrics created present a uniform goal of the team. Once the metrics are reviewed, they will be presented according to the assessment interval to the ESC. The ESC will discuss the stoplight metrics outlined for each metric, and any outstanding issues attributed to a disposition. Action Items may be identified by the Project Manger and assigned to Team Leads for follow-up.

Go/No-Go Meeting

The Go/No-Go Meeting will be scheduled approximately two weeks prior to implementation. The meeting should include the Executive Steering Committee, Project Executives and relevant project team members. The Implementation Vendor and QA Vendor should address their overall readiness for implementation by team, any tasks that have not yet been completed, and any risks or issues. This will allow the ESC to understand all issues and risks that exist across the project, and determine if the risks outweigh the benefits of moving forward with implementation.

Final Go/No-Go Meeting

When a "Go" decision is reached during the initial Go/No-Go meeting, a Final Go/No-Go Meeting should occur 1-2 days prior to implementation. Similar to the Go/No-Go Meeting, any outstanding tasks will be addressed, and any updates to risks and issues should be addressed. The State and vendor teams will re-confirm the decision to move forward with entrance in to implementation.

Topic	Metric	Report Used to Measure	Strategy to Measure	Target Threshold	Responsible Team	Comment/Status	Recommended Assessment Point(s)	Recommended Assessment Points: 6 Month	5 Month	4 Month	3 Month	2 Month	1 Month	3 Week	2 Week	1 Week	Evidence	Issue/Action Item #	Results
Change Readiness	Has a Change Readiness Action Plan for workers been developed?	Change Readiness Plan	Validate Change Readiness Plan exists		Change Readiness		4 Months			X									
Change Readiness	Has the Release 1 Change Readiness Plan for CSRs been developed?		Validate Change Readiness Plan exists		ACS		3 Months				X								
As Is/To be	Have Business Processes for Release 1 been assessed?		Gap Analysis		Change Readiness		3 Months				X								
As Is/To be	Identify the Gap between the "As Is" and "To Be" processes for Release 1		Gap Analysis		Change Readiness		4 Months			X									
As Is/To be	Have new business process documents been developed to prepare staff for the changes identified in the Gap Analysis?		Business Process Guides		Change Readiness		3 Months, 2 Months, 1 Month				X	X	X						
Change Readiness	Have the core business function been communicated to staff? And do staff understand their job functions as they relate to Release 1?	Change Readiness Survey	Survey	60%	Change Readiness		2 month, 1 month					X	X						
Change Readiness	Does the communication network effectively disseminate information to staff? Is the communication timely?		Review feedback from Pilot to identify gaps in the communication network or recommendations for improvement		Change Readiness		2 Month (post Pilot)					X							
As Is/To be	Have the baseline measurements for processes affected by Release 1 been identified and documented (# of intakes per day etc)?		DCFS established Baseline metrics		Change Readiness		3 Months				X								
To Be	Have all Business Processes that [illegible] of implementation been identified as Early Adoption Changes?		Review the list of BP [illegible] for completeness.		Change Readiness		4 Month, 3 Month			X	X								
To Be	Have Early Adoption Changes been implemented? If not what % have been completed?		Validation with parish operations that new processes have been implemented.		Change Readiness		2 month, 1 month					X	X						
Change Readiness	Have Change Readiness activities been distributed to all affected users?		Confirm with Change Readiness Lead from each Implementation Team		Change Readiness		1 month						X						
Change Readiness	Have change readiness activities been reviewed in each local office?		Confirm with Change Readiness Lead from each Implementation Team that the activities have been reviewed in each local office.		Change Readiness		1 month						X						
Change Readiness	Have baseline metrics to be used to evaluate success of CAFE been developed?		Review CAFE R1 Baseline Metric Report template.		Change Readiness		3 months				X								
Change Readiness	Have baseline metrics to evaluate success of CAFE been documented and reported?		Review CAFE R1 Baseline Metric Report from Pilot		Change Readiness		2 months (Post Pilot)					X							
Change Readiness	Have Change Agents been identified in local and regional offices?		Review the list of selected Change Agents and determine if adequate support is planned within each region and local office.		Change Readiness		3 months.				X								
Change Readiness	Have staff been identified to execute change readiness activities with region and local office staff?		Validate that the Change Readiness Leads have created lists and are tracking progress.		Change Readiness		4 months, 3 Months			X	X								
Change Readiness	Have system demonstrations been provided to all regions?		Confirm that system demonstration occurred and staff were able to attend.		Core CAFE		2 months					X							
Training	What percentage of trainees have been certified in the course they attended (a) # of people scheduled who attended, (b) # of people who passed who attended, (c) # of people scheduled who did not attend?		Review Moodle attendance tracking	95% attendance	Training		1 Month, 2 Week, 1 Week						X		X	X			
Training	Has a process to validate training was effective for users been developed?	Training survey	Review Training Survey	Department defined	Training		2 Months (Post Pilot), 1 Month				X		X						
Training Site Prep	Have Training Rooms been identified?		Review Training Plan and the list of Training Rooms		Training		3 Month				X								
Training Site Prep	Has Training hardware (PC, Laptop, projectors) been procured?		Validate purchase order(s)		Training		3 Month				X	X							
Training Site Prep	Has training equipment been implemented in classrooms?		Validate that the training equipment has been installed and tested in each classroom		Technical Support		4 Month, 3 Month				X	X							

Topic	Metric	Report Used to Measure	Strategy to Measure	Target Threshold	Responsible Team	Comment/Status	Recommended Assessment Point(s)	Recommended Assessment Points: 6 Months	5 Months	4 Months	3 Months	2 Months	1 Month	3 Weeks	2 Weeks	1 Week	Evidence	Issue/Action Item #	Results
Trainers	Have the trainers been indentified for each region?		Lists of DCFS staff who will be trainers		Training		4 Month			X									
Trainers	Are Trainers adequately prepared to deliver training?		Verify certification in T4T courses. Assess Trainers comfort delivering training and their understanding of their roles		Training		5 Months (2 Month Pre Pilot) , 2 Month Pre Implementation		X			X							
Training Environment	Has the CAFE Training environment been built to support ILT?		Validate content in the training environment		Deloitte		5 Months (2 Month Pre Pilot) , 2 Month Pre Implementation		X			X							
Training Environment	Has the Legacy Training environment been built to support ILT?		Validate content in the training environment		Legacy Technologies		5 Months (2 Month Pre Pilot) , 2 Month Pre Implementation		X			X							
Training Environment	Have training artifacts been loaded in the CAFE training environment?		Validate content in the training environment		Deloitte		1 Month Pre-Pilot, 2 Month Pre-Implementation			X		X							
Training Environment	Have cases are loaded in the Legacy training environment?		Validate content in the training environment		Legacy Technologies		1 Month Pre-Pilot, 2 Month Pre-Implementation			X		X							
Training	Is the curriculum developed?		Review draft materials		Deloitte		2 Month Pre-Pilot, 2 Month Pre-Implementation			X		X							
Training	Has the curriculum been printed?		Review draft materials		Training		1 Month Pre-Pilot, 2 Month Pre-Implementation			X		X							
Training	Has the Sandbox training environment been developed?		Review materials		Training		1 Month Pre-Pilot, 2 Month Pre-Implementation			X		X							
Training	Are workers completing Sandbox training?	Moodle Report	Staff will need to self report using Moodle. Have	90%	Training		2 Month (Pilot) 1 Month, 2 Weeks					X			X				
Training enrollment	Have DCFS regional coordinators scheduled workers to the appropriate courses?	Moodle Report	Verify list of attendees by parish	Target of no more than 25% of staff out of the office	Training		1 Month Pre-Pilot, 2 Month Pre-Implementation				X	X							
Training	Have Training User Ids been created for multiple profiles? Do the users have the appropriate access rights?	List of training Ids	Test training IDs		Conversion		2 Month prior to Pilot			X									
Training Environment	Has the process and schedule to refresh the Training environment been documented?		Review Training Plan and refresh schedule		Emerging Technologies		2 Month prior to Pilot			X									
Training	Have the CBTs been pushed out to Pilot Parish?		Validate with Pilot Parish		Training		2 Month prior to Pilot			X									
Training	Have CBTs been pushed out to all Parishes?		Validate with Parish offices		Training		2 Months					X							
Training	Are the Training Sites set up and the Training Site Checklist completed?	training site checklist	Validate checklist completion with IT regional rep		Training		2 months					X							
Training	Have training materials been printed and delivered to training sites?		validate delivery of materials by each site contact		Training		2 months					X							
Training	Have supplies for the Trainers been secured?		trainers validate receipt of needed trainer supplies		Training		2 months					X							
System Logins	Can Pilot parish staff log in as appropriate?		Validate functionality with select Super Users		Implementation		3 Month (UAT,) 2 Month				X	X							
Cutover	Has the Day 1 Walkthrough plan been developed and stepped through each at each local office?		Review day 1 walkthrough plan with office staff	80%	Business Process Analysis		1 month, 1 week						X			X			
Implementation Support	Has Infrastructure for Implementation Support Staff been identified and installed?(PC, Phone etc)		Review Implementation Plan, validate with implementation Leads		Communications		1 month, 2 week, 1 week						X		X	X			
Implementation Support	Have Down Time Procedures for any instance where an automated solution is not available been created?		Walk through procedures to validate that all processes and required data elements are captured.		Business Process Analysis		3 Month, 1 Month				X		X						
Implementation Support	Has a schedule for daily project calls including phone line and meeting invitation been sent?		Review Calendars and validate conference line availability		Communications		2 week, 1 week								X	X			
System Logins	Is a procedure in place to address staff without a login or a login that does not function correctly?		Review the process		Communications		2 Months, 1 Month, 3 Week, 1 Week					X	X	X		X			
Communication	Validate that a person is designated at each site as the local office Communication Contact		Review Local Office Plans		Communications		1 Month, 2 Weeks						X		X				
Communication	Are there regularly scheduled meetings to update staff?		Review Local Office Plans		Communications		1 Month, 2 Weeks						X		X				
Communication	Is there a process in place in each local office to distribute CT/CRFFs to appropriate staff?		Review Local Office Plans		Communications		1 Month, 2 Weeks						X		X				
Implementation Support	Do all 9 regions have operational implementation teams?		Validate regional staffing plan		Implementation		3 months				X								

Topic	Metric	Report Used to Measure	Strategy to Measure	Target Threshold	Responsible Team	Comment/Status	Recommended Assessment Point(s)	Recommended Assessment Points: 6 Month	5 Month	4 Month	3 Month	2 Month	1 Month	3 Week	2 Week	1 Week	Evidence	Issue/Action Item #	Results
Implementation Support	Does each region have a regional implementation plan?		Review Regional implementation Plans		Implementation		2 months, 1 month					X	X						
Implementation Support	Does each local office have a local office implementation plan?		Review local office implementation Plans		Implementation		2 months, 1 month					X	X						
Implementation Support	Has each region completed their implementation readiness checklist?		Validate implementation Readiness Checklists		Implementation		1 Month, 2 Week, 1 Week						X		X	X			
Implementation Support	Has each local office completed their implementation readiness checklist?		Validate implementation Readiness Checklists	100%	Implementation		1 Month, 2 Week, 1 Week						X		X	X			
Implementation Support	Has each local office identified Super Users?		Review list of Super Users		Implementation		4 Months			X									
Implementation Support	Have Super Users been provided all material needed for Go Live?		Validate materials are created and distributed		Implementation		1 Month, 2 Week, 1 Week						X		X	X			
Implementation Support	ARe Super User preparation tasks complete?		Super Users have attended all modules of CAFE training including CBTs. Super Users have completed X additional practice exercises using cAFE sandbox. Super Users have been trained in Issue Reporting Protocols.	100%	Implementation		1 Month, 2 Week, 1 Week												
Communication	Is the communication plan in place for cutover weekend?	Communication Plan	Review communication plan to validate that for each state agency partner there is a primary and secondary point of contact including emergency contact numbers	100%	Communications		2 Month (Pilot), 1 Week					X				X			
Integration Partners	Identify and validate systems CAFE will integrate with		Review DSD		Core CAFE		3 Month, 2 Month				X	X							
Integration Systems	Define specific data elements per each integration system		Review DSD		Core CAFE		2 Month					X							
Integration Systems	Test system integration		Validate System Test results	100%	Testing		2 Month, 1 Month					X	X						
System Test	Has the Interface Test Plan been approved?		Review Test Plan		Testing		2 Month					X							
System Test	Have parameters for the testing data been defined and communicated to establish testing environments?		Review Test Plan		Testing		5 Month, 4 Month		X	X									
System Test	Has the Batch testing Plan been approved?		Review Test Plan		Deloitte		2 Month					X							
System Test	Do Batch testing results meet threshold targets?		Review batch timings from System Test and compare to anticipated outcomes from Test Plan	Need threshold from Test Plan	Deloitte		1 Month, 2 Weeks						X		X				
Integration Partners	Have Real-time and batch update testing processes been defined and communicated to interface partners (dates or standards are defined)?		Validate integration plan		Integration		2 Months					X							
Implementation	Is the Pilot customer portal redirection front end in place?		Site test		Core CAFE		3 Months (2 Weeks prior to Pilot)				X								
Implementation	Has the customer portal redirection front-end been removed?		Validate cutover plan		Core CAFE		Statewide implementation weekend									X			
Data Conversion	Was the Conversion Plan approved?	Conversion Plan	Review Conversion Plan		Conversion		4 Months			X									
Data Conversion	Were the data elements identified for conversion validated?	Conversion Plan	Review Conversion Plan		Conversion		4 Months			X									
Mock Conversion	Did Mock Conversion results meet data validation standards?		Count of converted user IDs to # of legacy IDs	TBD	Conversion		2 Months				X								
Conversion Planning	Is Manual conversion progress meeting expectations?	Roles and Responsibility matrix Security Profile metrix	Extract existing LAMI user information Confirm CAFE roles for each candidate user Secure field approval Provide final office approval of user information Secure state office approval Provide final approval of all user information		Conversion		2 Months, 1 Month, 2 Weeks					X	X		X				
Conversion Planning	Are Security Profile validation efforts complete?	Data purification reports	Data Conversion Plan		Conversion		3 Months, 2 Months				X	X							
Mock Conversion	Was the Dry Run LDAP load tracked to determine data migration timings?		Record time the file sent		Conversion		2 Months					X							
Mock Conversion	Did the dry Run LDAP test conversion reports?	Conversion Reports	Compare Conversion Reports to baseline		Conversion		4 Months			X									

Topic	Metric	Report Used to Measure	Strategy to Measure	Target Threshold	Responsible Team	Comment/Status	Recommended Assessment Point(s)	Recommended Assessment Points: 6 Months	5 Months	4 Months	3 Months	2 Months	1 Month	3 Weeks	2 Weeks	1 Week	Evidence	Issue/Action Item #	Results
Defect Resolution	Have all Critical Legacy system defects that impact implementation been resolved?	Report from defect tracking tool	Review tickets logged from testing and pilot. Resolution needs to occur prior to system freeze.	100% resolution	Legacy Technologies		4 Months, 3 Months, 2 Months, 1 Month, 3 Weeks, 2 Weeks			X	X	X	X	X	X				
Worker Id's and Worker Profiles	Validate that Worker ID's and Worker Profile function properly	System Test, UAT and Pilot	Review tickets logged from testing and pilot. Resolution needs to occur prior to system freeze.		Testing		1 Month before Pilot, 1 Month				X		X						
UAT Test	Have test cases been created?		Validate test environment		Testing		4 Month			X									
System Test	Do test scripts cover all requirements?		Review Test scripts		Testing		6 Months, 5 Months	X	X										
UAT Test	Have Bill test scripts been generated for UAT?		Review Test scripts		Testing		5 Month		X										
UAT Test	Have the UAT staff been trained on CAFE?		UAT Training	100%	Testing		5 Month, 4 Month		X	X									
UAT Test	Is test script production on target to meet the UAT schedule?		Review the # of scripts needed to the testing schedule		Testing		5 Month, 4 Month		X	X									
System Test	Has 508 Testing been completed?		System Test Results	100%	Testing		4 Month			X									
UAT Test	Has 508 Testing been completed?		UAT Test Results		Testing		3 Month				X								
UAT Test	Have Security Profiles been tested?		System Test Results	100%	Testing		5 Month, 4 Month		X	X									
System Test	Were Testing User ids created?		Validate test environment		Testing		6 Month	X											
UAT Test	Were Testing User ids created?		Validate test environment		Testing		5 Month		X										
Help Text	Have the help text and FAQs been validated?		Validate the screen help functionality in System Test and UAT		Testing		5 Month, 4 Month		X	X									
Customer Portal	Does the Customer Portal function according to requirements?	RTM	Validate the customer is able to perform a redetermination during redetermination window	100%	Testing		5 Month, 4 Month, 3 Month		X	X	X								
Worker Portal	Does the Worker Portal function according to requirements?	RTM	Validate dashboard functionality functions according to requirements Validate workflow functions properly according to Business Rules Validate Interview Wizard functions properly	100%	Testing		4 Month, 3 Month			X	X								
Capacity Planning	Do live results from stress and performance testing meet SLA's?	Stress and Performance Test Summary	Validate that the planned capacity can meet the system requirements		Testing		4 Month			X									
Customer Portal	Are translations for other languages available in Customer Portal?	System Test/ Pilot Test Tickets	System Testing		Testing		4 Month, 3 Month, 2 Month			X	X	X							
Intrusion/Detection	Do the results from Intrusion/Detection testing meet SLA's?	System Test/ Pilot Test Tickets	Validate System Test results		Testing		4 Month, 3 Month			X	X								
Technical Staff Training	Have all technical staff been trained as indicated in the Technical Training Staff Document?	Timely training of all technical staff Document	Staff are trained in HATS Staff are trained in Cotcon Staff are trained in Way	100%	Deloitte		4 Month, 3 Month			X	X								
System Documentation	Was the CAFE System documentation updated prior to implementation? Has it been distributed to appropriate audiences?		Review and validate the system documentation Validate it was sent to the appropriate teams	100%	Core CAFE		3 Month, 2 Month				X	X							
Legacy system enhancements	Have targeted Legacy system enhancements been implemented prior to code freeze?		Legacy release notes	100%	Legacy Technologies		6 Month, 4 Month, 2 Month, 1 Month	X		X		X	X						
Source Code	Were source code updates were correctly prioritized and migrated?	Legacy System Defect Report	View list of outstanding system defects and prioritize them based on system and conversion criticality	Recommend 100% critical, high, medium and low will vary based on direction from Department	Legacy Technologies		5 Month, 3 Month, 1 Month		X		X		X						
Single Sign-on	Does single sign-on in CAFE function as designed?		Validate System Test/Pilot Test results	100%	Testing		4 Month, 3 Month			X	X								
HATS	Does the HATS data populate in LAMI according to design?	System Test/ Pilot Test Tickets	Validate System Test/Pilot Test results		Testing		4 Month, 3 Month			X	X								
Pseudo SSN	Does the pseudo SSN function as designed?		Validate System Test/Pilot Test results		Testing		4 Month, 3 Month			X	X								
Implementation	Is the CAFE Environment set up in preparation for Implementation?		Validate environment is prepared for implementation		Core CAFE		1 Month, 2 Week						X		X				
CAFE	Has the System Design Documented been approved?		DSD is approved		Core CAFE		6 Month	X											

Topic	Metric	Report Used to Measure	Strategy to Measure	Target Threshold	Responsible Team	Comment/Status	Recommended Assessment Point(s)	Recommended Assessment Points: 6 Month	5 Month	4 Month	3 Month	2 Month	1 Month	3 Week	2 Week	1 Week	Evidence	Issue/Action Item #	Results
Sandbox	Is the Sandbox environment associated in the appropriate legacy environment?		Test connectivity		Legacy Technologies		3 Months (after Pilot training)												
Sandbox	Is the Sandbox environment prepared for training?		Validate the sandbox environment is set up		Legacy Technologies		3 Months (prior to Pilot)				X								
System Test	Was the Interface testing environment set up?		Confirm environment		Deloitte		2 Month					X							
System Test	Was the System Test environment setup?		Confirm environment		Deloitte		6 Month	X											
UAT Test	Is the UAT Test environment setup?		Confirm environment		Deloitte		5 Month		X										
System Test	Was test data loaded to the System Test environment?		Validate test environment		Deloitte		6 Month	X											
UAT Test	Is CAFE Test Data loaded to the UAT environment?		Validate test environment		Deloitte		4 Month			X									
UAT Test	Is Legacy Test Data loaded to the UAT environment?		Validate test environment		Legacy Technologies		4 Month			X									
Training	Were applications loaded to the Sandbox environment?		Validate Sandbox environment		Deloitte		2 Month prior to Pilot			X									
Training	Were cases loaded to the Sandbox environment?		Validate Sandbox environment		Legacy Technologies		2 Month prior to Pilot			X									
Training	Were Sandbox user id's created?		Review and validate logics		Conversion		2 Month prior to Pilot			X									
Training	Are the Sandbox refresh procedures documented and scheduled?		Review Refresh Procedure		Legacy Technologies		1 Month prior to pilot				X								
UAT Test	Are Performance testing user id's created?		Load Testing		Testing		2 weeks before								X				
UAT Test	Is the CAFE Load Test environment created?		Load Testing		Deloitte		2 weeks before								X				
UAT Test	Are CAFE Load Test scripts created?		Load Testing		Deloitte		2 weeks before								X				
Customer Feedback	Customer Survey TBD pending clarification from Liz.		Validate client survey is created. Send survey to clients.		Implementation		2 Month, 3 Weeks					X		X					
Forms	Are application forms generated out of the application correctly?		Sight validation from System Test	100%	Testing		4 Month, 3 Month,			X	X								
Forms	Are Redetermination forms generated out of the application correctly?		Sight validation from System Test	100%	Testing		4 Month, 3 Month,			X	X								
Forms	Are Supplemental Forms generated out of the application correctly?		Sight validation from System Test	100%	Testing		3 Month, 2 Month,				X	X							
Customer Notification	Have customers been notified about the Customer Portal including instructions on how to use it?		Review correspondence		Communications		2 Month, 1 Month, 1 Week					X	X			X			
Customer Notification	Were customers notified of timeframes for new functionality?		Review correspondence		Communications		1 Month, 2 Weeks						X		X				
Help Desk	Are Help desk staff prepared for CAFE?	Help Desk support Plan			Core CAFE		1 Month, 2 Week						X		X				
FAQ's	Are FAQ's updated and accessible?		Manually verify		Core CAFE		1 Month, 2 Week						X		X				
Policy question	Is a process to escalate policy questions in place?		Review the workflow and communication plan		Communications		2 Month					X							
MR	Has the list of CSC MR's to change for CAFE been validated?		Documented List		ACS		5 Month, 2 Month				X	X							
MR	Confirm list of CSR information needed to change for CAFE		Validate the list with State team and ACS		ACS		3 Month, 2 Month				X	X							
Call Center	Have the CSC FAQ's that require changes or updates for CAFE been identified?		Documented List		ACS		2 Month					X							
MR	Have the CSC scripts and call flows that must be changed or updated prior to CAFE been implemented?		Review testing outcomes		ACS		2 Month					X							
Training	Was ACS's training plan for CSR's for CAFE approved?		Written training plan reviewed by identified staff; approval signed (plan not a contract deliverable)		ACS		3 Month				X								
MR	Have final approval of CSC MR changes completed for CAFE been implemented?		Signed list of completed changes, MR changes frozen		ACS		1 Month, 2 Week						X		X				
Call Center	Have CSR work sheets, short cuts, etc. been completed for CAFE?		Signed list of completed documents; docs frozen		ACS		1 Month, 2 Week						X		X				
Call Center	Have CSC FAQ's updated for CAFE been implemented?		Signed list of completed documents; docs frozen		ACS		1 Month, 2 Week						X		X				
Call Center	Have CSC call flows and scripts for CAFE been implemented?		Signed list of completed documents; docs frozen		ACS		1 Month, 2 Week						X		X				
Implementation	Has the Communication Plan between the CSC and CAFE been approved?		Review workflow and communication plan		Communications		1 Month						X						
Help Desk	Have Help desk staff been identified and trained as appropriate for Release 1 pilot?		Validate CSRs are trained		Core CAFE		3 Month, 1 Month				X		X						
Help Desk	Has the Help Desk - Level 2 Location been selected?		Validate Level 2 Staffing Plan		Implementation		4 Month (2 month before pilot)			X									
Help Desk	Is Equipment needed for Help Desk operations procured?		Validate hardware procurement		Implementation		4 Month (2 month before pilot)			X									
Implementation	Has the Command Center location been selected?		Review Command Center Plan		Implementation		4 Month (2 month before pilot)			X									

	Topic	Metric	Report Used to Measure	Strategy to Measure	Target Threshold	Responsible Team	Comment/Status	Recommended Assessment Point(s)	Recommended Assessment Points: 6 Month	5 Month	4 Month	3 Month	2 Month	1 Month	3 Week	2 Week	1 Week	Evidence	Issue/Action Item #	Results
	Implementation	Have phone lines and computers been secured for Command Center?		Review Command Center Plan		Implementation		4 Month (2 month before pilot)			X									
	Implementation	Has the Command Center Schedule for assignments been developed and distributed?		Review Command Center Plan		Implementation		3 Month (1 month before pilot), 1 Month				X		X						
	Pilot	Have the Redetermination notices been changed for pilot area?		Site test		Core CAFE		3 Month				X								
	Testing	Were the CAFE Load Test results within acceptable SLA's?		Validate against contract SLA's		Testing		3 Months (prior to Pilot)												

R Red: Urgent attention needed

Y Yellow: Some concern, issues to address

G Green: Progress meets or exceeds expectations

N Gray: Not assessed

Appendix 9

Your Health IDAHO

IV&V Services for Idaho Health Insurance Exchange

Deliverable: M6_1

Operational Readiness Review Assessment
October 23, 2014

FINAL

First Data
beyond the transaction

This Page Intentionally Left Blank

FINAL

Revision History

This document is controlled through the Document Management Process. To verify that the document is the latest version, please contact the First Data Team.

Date	Version	Responsible	Reason for Revision
10/7/2014	0.1	P. Harris	Initial Draft
10/17/2014	0.1	P. Shergill	content

FINAL

This Page Intentionally Left Blank

FINAL

Table of Contents

Revision History i
1.0 Introduction and Purpose 2
2.0 Roles and Responsibilities 2
3.0 Operational Readiness Review (ORR) 2
4.0 Project Artifacts and Comments 13
5.0 Assumptions/Constraints/Risks (if applicable) 16
6.0 Appendix A: ORR Agenda 17

FINAL

1.0 Introduction and Purpose

The Operational Readiness Review (ORR) assessment provides a review of project artifacts, process work products as well as on-site witness of the Operational Operational Readiness demo held on October 15 and 16, 2014.

2.0 Roles and Responsibilities

The following table documents the roles and responsibilities associated with the development, review and approval of the deliverable.

Role	Responsible Individual	Responsibility
First Data Approval Representative	Patricia Harris	IV&V Project Manager
First Data Deliverable Owner	Premjeet Shergill	Responsible for ORR Process / Assessment
Your Health Idaho Health Insurance Exchange	Rick Moran	Responsible for feedback and approval of the Deliverables.

Table 2.1 Deliverable Roles and Responsibilities

3.0 Operational Readiness Review (ORR)

The purpose of the ORR is to satisfy the Center for Medicare and Medicaid Services (CMS) oversight groups the system is operationally ready and prepared to support the requirements for implementation of a State Based Marketplace (SBM). To that end, a formal checklist was provided to ensure all areas of concern are reviewed and the system is ready for deployment. The checklist is provided here and is organized by business area. IV&V comments are associated with each checklist item and where needed, reference to other associated artifacts is also included.

Business Area			
Individual Eligibility and Enrollment			
Functionality	Single, Streamlined Application for Health Coverage	*Questions/Items to Look for:* Single, streamlined application: Does online functionality support collection of application information in accordance/compliance with CMS guidance on single, streamlined application (*defer to CCIIO and CMCS application subject matter experts*) and allows for automated processing of application information collected.	**First Data Observations:** • The ability to view single sign-on functionality was not available for the ORR demo. This is functionality which CMS would like to view prior to "go-live". **Recommendation:** • Provide CMS a view of this functionality in a demo prior to "go-live".
Scenarios	No financial assistance (not requested or not eligible)	*Questions/Items to Look for:* Are verification calls made to the HUB? Plan Selection – • Does the system have filtering criteria? • Does the system display Deductible, Coinsurance, and Copayment? Can an individual enroll in Plan?	**First Data Observations:** • The demo provided all features with the exception of NOA generation. • NOA hard copies are provided on CALT for review by CMS. **Recommendation:** • Provide a demonstration to CMS of NOA generation from YHI Exchange system which identifies the NOA triggers.

		Is an 834 transaction generated? Can the system generate Notices related to eligibility determinations and QHP enrollment?	
	Stopping work in the application without creating an account	Does the system allow for "browsing" without creating an account/submitting an application? At what point in the application process is an individual expected to create an account?	**First Data Observations:** • Demonstrated and met for ORR. **Recommendation:** • None
	Persist an application, if a Federal Partner is either down or in a maintenance window	Does the system allow for "holding" an application and returning later to complete?	**First Data Observations:** • Demonstration showing the ability to stop and start an application. This item was satisfactorily met. **Recommendation:** • None
	Does the system have functionality in place to handle unexpected results? (e.g., error responses or invalid responses)	How are errors communicated, is the functionality automated, e.g.:, if the system requires a field with 10 alpha-numeric characters and an individual inputs 10 alpha characters, what communication is generated, is the functionality automated?	**First Data Observations:** • The specific error communication cited by CMS was not part of the demo but error messages were described. • Page error messages DO pop-up in Idalink and login error messages are shown in YHI Exchange. • Unexpected results were not part of this

			demo. **Recommendation:** • Clarity around the questions for incorrect results should be provided. How are they is handled when they occur, can they occur and what the types of errors are. • Provide a demonstration other than 'happy path' functionality.
	Document Management	Is the system able to accept, store, associate and process documentation received from individual applicants and enrollees electronically? Does the system have the ability to image, store, associate, and process paper documentation received from individual applicants and enrollees via fax/mail?	**First Data Observations:** • Demonstration provided good overview of how documents are uploaded. • Good explanation provided on how items are associated in the application. **Recommendation:** • None
	Eligibility for Financial Assistance – APTC/CSR Determination; Individual and Family	*Questions/Items to Look for*: Are verification calls made to the HUB? Are MAGI Rules executed in an	**First Data Observations:** • Demonstration of financial application with APTC and CSR eligibility provided. • Enrollment and 834 criteria demonstrated with a pre-entered

		automated fashion? Plan Selection- • Does the system have filtering criteria? • Does the system display Deductible, Coinsurance, and Copayment? Can an individual enroll in Plan? Is an 834 transaction generated? Can the system generate Notices related to eligibility determinations and QHP enrollment?	case. **Recommendation:** • None.
	Eligibility for Financial Assistance – Medicaid MAGI Determination, Individual and Family	*Questions/Items to Look for:* Are verification calls made to the HUB? Are MAGI Rules executed in automated fashion? Plan Selection- • Does the system have filtering criteria? • Does the system display deductible, Coinsurance, Copayment? Can an individual enroll in Plan?	**First Data Observations:** • Idalink to IBES demonstration. • Pre-entered information from IBES through Account transfer to YHI Exchange was demonstrated **Recommendation:** • Present a written plan to demonstrate Account transfer to CMS • For any perceived lapses in the continuity of processing (such as handoff to a batch

		Is an 834 transaction generated? Can system generate notices related to eligibility determinations and QHP enrollment?	process which occurs overnight), walk through a diagram or process which clearly demonstrates the process from initiation, handoff, and posting the following day. • Provide a two-day session demo for CMS once ATC is received to illustrate a transfer from end to end.
	Mixed Household with Eligibility for Marketplace and Medicaid/ CHIP Coverage	*Questions/Items to Look for:* Are verification calls made to the HUB? Are MAGI Rules executed in automated fashion? Plan Selection- • Does the system have filtering criteria? • Does the system display deductible, Coinsurance, Copayment? Can an individual enroll	**First Data Observations:** • Demonstrated as requested. **Recommendation:** • None

FINAL

		in Plan? Is an 834 transaction generated? Can system generate notices related to eligibility determinations and QHP enrollment?	
	Additional Eligibility Scenarios Applicant change of address Enrolled applicant is now incarcerated Eligibility failed due to incarceration Applicant with a child under 26 Applicant with a child under 26 that is employed Processing paper applications	*Questions/Items to Look for:* Are verification calls made to the HUB? Are MAGI Rules executed in automated fashion? Plan Selection- • Does the system have filtering criteria? • Does the system display deductible, Coinsurance, Copayment? Can an individual enroll in Plan? Is an 834 transaction generated? Can system generate notices related to eligibility determinations and QHP enrollment?	**First Data Observations:** • Multiple addresses were demonstrated for a household. • Incarceration failure was demonstrated for an individual in a mixed household • 26-year-old demonstrated with correct results • 26-year-old with income not demonstrated • Paper processing discussion with use of the CSR discussed. **Recommendation:** • Include a scenario for blueprint which includes a 26-year-old with income as part of review for CMS.
	Exemption Processing – 6 exemptions	*Demo only needed if state is processing its own exemptions in an automated fashion (this*	**First Data Observations:** • Exemptions will be referred to the FFM.

		only applies to CT)	**Recommendation:** • Upload enrollment process to CALT for CMS review.
	Account Creation	Can the system account for processing issues; e.g., individual forgot logon, password, no email or telephone contact information has been identified, no fixed/permanent address has been identified. Can the system account for unlocking a locked account, how are individuals notified that their account has been locked?	**First Data Observations:** • Demonstration provided for YHI Exchange system. **Recommendation:** • Provide Demonstration of how "Single Sign-on" is impacted if locked-out in one system; what happens in the second system.
	QHP Selection Change before payment made during open enrollment Change after payment	Can the system account for QHP changes made by an application before a payment is made to the Issuer if the change is made during the open enrollment period? Change is made after payment is made to the Issuer?	**First Data Observations:** • Demonstrated both scenarios. **Recommendation:** • None.

	made during open enrollment	Is communication in automated fashion, to applicant, to Issuer, to QHP?	
Enrollment			
	834 Generation (We are working with SBMs through this process; as such the demonstrations will be "State specific" depending upon individual, unique State circumstances.) -To issuers -999 receipt and transmission reconciliation processes • Initial and/or Effectuated Enrollments • Changes in enrollment • Disenrollment Monthly reconciliation process with issuers	View 834 that is to be transmitted View 834 that is to be transmitted See logs and reports Understand the process Understand the process and see demo if possible	**First Data Observations:** • Demonstration of 834 files and EDI conversion of file presented. • There was some questions surrounding the version guide updates and completed of 834 testing with CMS. **Recommendation:** • Provide updated states on version coding changes and any outstanding items for CMS. • Provide updated 834 test results to CMS.
Consumer Assistance			
	• Navigator Screens • Navigator Account Creation Process	How an application is submitted on behalf of an individual? How are Navigators identified and certified? How an application is submitted on behalf of	**First Data Observations:** • Assistors and Navigator account creation and system usage demonstrated along with how to edit fields and entries.

	• In-Person Assistors • In-Persons Account Creation Process	an individual? How are In-Person Assistors identified and certified?	**Recommendation:** • None.
Eligibility Determination Appeals Process (No Demo Needed)			
	• Marketplace • Medicaid	*Refer to Appeals discussion in Implementation Review* If an appeal starts in one agency, does it need to be transferred to the other agency? Is this process automated?	**First Data Observations:** • Appeals process flow presented to CMS. **Recommendation:** • None.
Plan Management			
	• State Plan Review Screens • Issuer Plan Review Screens • Loaded into Plan Select Screens – Individual and SHOP	Understand plan error correction process	**First Data Observations:** • Demonstration and discussion of Plan Management given based on status of release in production. **Recommendation:** • None.
Call Center			
	• Logon on • Workflows • Escalation Processes	Role based access Tier 1 to Tier 2 or Tier 3 support	**First Data Observations:** • Call Center plans and process presented and discussed. • RFP assistance for "go-live" presented and discussed.

			Recommendation: • None.
Technical			
	• View logs that show successful calls to HUB and State Sources • View logs for identify management • Validate data base updates		**First Data Observations:** • Database design document and what is proprietary still has some outstanding questions. • Logs were presented during demonstration for various areas of HUB calls and RIDP. **Recommendation:** • Request decision on expected documentation for database design or if what has been submitted will meet CMS approval.
Operations			
	• System Monitoring Process • Disaster Recovery/Continuity of Business Operations	How are system related errors monitored and resolved Review data backup procedures	**First Data Observations:** • Security Presentation and discussion with CMS on how monitoring is done for both DHW and YHI. • Disaster recovery plans and presentation given. • Authority to Connect discussion with impact to schedule and testing discussed. **Recommendation:** • Accelerate where possible to attain ATC approval from CMS.

4.0 Project Artifacts and Comments

In addition to on-site review during formal ORR by GI and DHW, IV&V reviewed project artifacts for confirmation / verification of system capability. Key artifacts reviewed addressing system capabilities are listed below:

Project Artifact	Date Reviewed	Comments
Administration_Level_3_Process_Flows_2014-09-02[1].vsd		• Provides an overview of all project and operations processes.
Idaho_Special_Enrollments_Matrix_v20.xlsx		• Provides oversight of decisions on enrollments.
YHI_Baselined_RTM_2014-06-10.xlsm		• Requirements tracking matrix
Business_Reuse_Strategy_and_Components.pptx		• Provides information on the approach for reuse of the YHI Exchange.
YHI-GetInsuredCP2CP3DemoScopeNotes20140712.docx		• Demonstration of System areas for Non-Financial flow, Customer Service Representative (CSR) ticket management

YHI-CP4DemoScopeNotes20140819.docx		• Non-financial Flow
		  o Agent completes SSAP for a consumer
		  o Consumer logs a complaint
		• Financial Flow
		  o File an appeal against the Eligibility Results
		• Admin/CSR Override (Non-financial

		Application) o Update application to add a dependent o Update demographic data • Account Settings, FAQ
YHI-CP5DemoScopeNotes20140925_Approved.docx		• Role based permissions • Manage tickets • Customer Administration Portal (CAP) reports • Manage members • Manage agents • Issuer / plan management portals • Document verification • Referral applications • Financial management: payment redirect • Generation of 834s • Reporting
YHI-TC1_Test_Report_v1_1_Final.docx		• RIDP – Verify the applicant primary verification through the Federal hub (CMS). RIDP service can only be initiated for the purposes of identity proofing of the primary household applicant, for which Single streamlined Application (SSAp) is being submitted. The applicant's identity is verified with Experian using the credit report records. • SSAC – Check the applicants SSN verification, citizenship status, death confirmation and incarceration status. • VLP – Verify the applicant's immigration status based on documentation provided by the applicant: I-551, I-94 etc.
YHI-TC6_Test_Report_v1_0_Final2.docx		• Non-US Citizen CMS Test Case results • US Citizen CMS Test Case results
Systems_Security_Plan_V_2_1-Individual_Exchange_vFinal.docx		• System Identification, Security Controls, SSP Documents
YHI-Disaster_Recovery_Plan_v1_1_Ap		• Disaster Recovery Strategy

proved.docx		

FINAL

5.0 Assumptions/Constraints/Risks

Although CMS indicated there were no "show stoppers" noted during the ORR presentation, First Data noted recurring items which have been of key concern to CMS. These items are listed below with a recommended approach for presentation to CMS.

1. Accounts Transfer demonstration. The ability to actually observe an account transfer occur between the systems has been in question for the past two months. Setting up an overnight demo with CMS data over two days to demonstrate the handoff between real-time and batch processing may resolve any remaining questions that CMS has with this function.
2. Single Sign-On. A successful demonstration of the Single Sign-On process between the two systems may assist with mitigating CMS concerns with this functionality. The demonstration should include what occurs when an individual is locked-out of one system and attempts to log into the other system.
3. Authority to Connect to the exchange is critical to the success of final testing. *RESOLVED as of 10/22/2014.*
4. Database design documentation. Clarify all outstanding questions with Database design to ensure no delays on approval of database design documentation from CMS. Although the system is clearly operable without associated documentation such as a Database Design, this level of documentation appears to be critical to CMS approval and therefore a key requirement for project success.

6.0 Appendix A: ORR Agenda

Idaho STATE-BASED MARKETPLACE OPERATIONAL READINESS, establishment, and Year 2 Consult REVIEWs

Final Detailed Agenda

Your Health Idaho

Date of Review: October 15-16, 2014, 8:30 am- 5:30 pm (MT)
Meeting location: Idaho Department of Health and Welfare 450 W. State St., 10th floor, Boise, Idaho 83702
Conference Call Information: 1-877-885-1087, Access: 301-838-3883, Leader Pin: 1844
Webinar Information: Day 1- https://webinar.cms.hhs.gov/orrday1review , Day 2- https://webinar.cms.hhs.gov/orrday2review

Instructions of the Demonstrations: CMS will provide four test cases prior to the review. The No Financial Assistance and Mixed Household test cases should be keyed in during the demonstration. The remaining scenarios can be prepopulated with eligibility determination results calculated during the ORR review.

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
Day 1: Wednesday October 15, 2014: (Call Information: 1-877-885-1087, Access: 301-838-3883, Webinar Information: https://webinar.cms.hhs.gov/orrday1review)				
8:30 am – 8:45 am (15 Minutes)	**Welcome & Introductions**	• Attendee introductions and roles • Goals of the CMS Reviews		Idaho: YHI, DHW CMS: Czarina Biton (CCIIO) Yolande Calhoun (Information Technology, OIS) Susie Cummins (Medicaid, CMCS) David Koppel (Medicaid,

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
				CMCS)
8:45 am-9:15 am (30 Minutes)	Program Management	• Project Schedule Update • Risk Register • Financial Status Report • Performance Measures • Implementation Plan		Idaho: YHI, DHW CMS: Yolande Calhoun (Information Technology, OIS)
9:45 am-10:00 am (15 Minutes)		**Break**		
10:00 am-11:30 am (1.5 hours)	Consumer Portal	**Demo 1: Web Portal** • Anonymous Browsing • Account Creation • Non-Financial Application Demo Objectives: • Anonymous Browsing • Account Creation • RIDP • Non-financial application • Financial application Discussion(s): 1. Does the system allow for "browsing" without creating an account/submitting an application? 2. Can the system account for		Idaho: YHI, DHW CMS: Yolande Calhoun (IT Program Manager, OIS) Jenny Chen (Eligibility & Enrollment, CCIIO) Dawn Horner (Eligibility & Enrollment, CCIIO)

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
		processing issues; e.g., individual forgot login, password, no email or telephone contact information has been identified, no fixed/permanent address has been identified. 3. Can the system account for unlocking a locked account, how are individuals notified that their account has been locked? 4. Does the system have functionality in place to handle unexpected results? (e.g., error responses or invalid responses) 5. At what point in the application process is an individual expected to create an account?		
11:30 am- 1:00 pm **(1.5 hours)**	**Eligibility (including Single Streamlined Application)**	**Demo 2: Eligibility part 1** Demo Objective(s): Demonstrate the following financial and non-financial scenarios • No financial assistance (not requested or not eligible) • Eligibility for financial assistance- APTC/CSR Determinations for Individual and Family • Eligibility for financial assistance- Medicaid MAGI Determination for Individual and Family • Mixed household with eligibility for Marketplace and Medicaid/CHIP Coverage • Applicant change of address	**Single Streamlined Application (BP 3.1)** • Review of dynamic online application. • Are verifications embedded in the online application? • Does the state ask individuals who attest to being in a satisfactory immigration status when they were granted such status? **Application, Updates, Acceptance and Processing (BP 3.3)** • Business processes for accepting and processing applications (including paper and telephonic)	Idaho: YHI, DHW CMS: Yolande Calhoun (IT Program Manager, OIS) Jenny Chen (Eligibility & Enrollment, CCIIO) Dawn Horner (Eligibility & Enrollment, CCIIO) Dena Greenblum (Medicaid & CHIP

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
		• Enrolled applicant is now incarcerated • Eligibility failed due to incarceration • Applicant with a child under 26 • Applicant with a child under 26 that is employed • Processing paper applications • Processing exemptions	• Discussion on how the state is able to receive and process changes in circumstances reported by MAGI-based beneficiaries • Description of how the Marketplace will process Special Enrollment Periods Discussion(s): 1. Are MAGI-based beneficiaries able to report changes in circumstances via the following modalities? a. Online via an electronic account b. Phone c. Mail d. In person e. If another modality is available, please specify 2. For Medicaid beneficiaries determined ineligible based on MAGI due to a change in circumstances, is the state able to evaluate potential eligibility on a non-MAGI basis? What is the state's process for doing so? 3. For beneficiaries determined no longer eligible, is the state able to evaluate potential eligibility for other insurance affordability programs and transfer the individual's electronic account to the appropriate program? **Notices, Annual Redeterminations (BP 3.4, 3.9)** • Description of business processes in relation to the generation and sending of applicant notices • Update on	Applications, CMCS)

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
			redetermination/renewal process for 2014 enrollees Discussion(s): 1. Can the state produce each of the following types of notices for Medicaid and separate CHIP and QHP/APTC? a. Approval b. Denial at initial application c. Termination d. Requests for additional information e. Other types 2. Are notices dynamic? 3. Are notices available electronically? 4. Please provide a sample of each type of notice in both written and electronic formats. 5. Is the state able to send negative notices, specifically? **Eligibility Verifications (BP 3.5)** • Final comprehensive list of data sources that the State is accessing, and/or interfacing with, in order to conduct required eligibility verification (submission of CMCS verification plan) • Description of the status of connection with each data source, information associated with each source (including data sources that are used as primary verification methods or are used when information is not reasonably compatible), and contingency if connection or data source is not available • Description of plan/process for verifying eligibility criteria when an inconsistency is triggered Discussion(s):	

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
			Use of Hub Services 1. Review of hub services being utilized 2. Is the state currently using or planning to use FTI data through the Hub? 3. Does the state ask to receive consent to use tax data at renewal for up to 5 years? 4. Is the state currently using or planning to use Equifax data through the Hub? *Verification Policies & Procedures* 1. Can the states system apply a reasonably compatibility standard for income in accordance with the regulations at 42 CFR 435.952(c)(1)? 2. How are your verification policies and procedures related to: a. Reasonable Compatibility b. Accepting Self-attestation c. Conducting post-enrollment verification d. Other electronic data sources used **APTC and CSR Calculations (BP 3.8)** **Exemptions (BP 3.10)** **Eligibility Appeals (BP 3.11)** Business processes and standard operating procedures for appeals process	

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
1:00 pm – 2:00 pm (1 hour)		Lunch on your own		
2:00 pm -3:30 pm	Eligibility (including Single Streamlined Application)	Demo 2: Eligibility Part II (continued from Part 1)	Continued from Eligibility Part I discussions	Idaho: YHI, DHW CMS: Yolande Calhoun (IT Program Manager, OIS) Jenny Chen (Eligibility & Enrollment, CCIIO) Dawn Horner (Eligibility & Enrollment, CCIIO)
3:30 pm-3:45 pm (15 Minutes)		Break		

3:45 pm-5:15 pm
 	
(1.5 hours)
	Enrollment	Demo 3: Enrollment
		
		Demo Objective(s):
		• QHP Selection and Enrollment
		• 834 generation
		  ○ To issuers
		  ○ 999 receipt and transmission reconciliation
			Enrollment transaction and APTC/CSR payment information processing (BP 3.12)
			
			• Description of how the Marketplace and SHOP processes enrollments using standard electronic enrollment transactions in coordination
				Idaho: YHI, DHW
				
				CMS: Yolande Calhoun (Information Technology, OIS)

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
		processes ○ Initial and/or Effectuated Enrollments ○ Changes in enrollment ○ Disenrollment ○ Monthly reconciliation process with issuers Discussion(s): 1. Describe the 834 Generation process 2. View 834 that is to be transmitted 3. Logs and reports 4. Can the system account for QHP changes made by an application before a payment is made to the Issuer if the change is made during the open enrollment period? 5. Change is made after payment is made to the Issuer?	with issuers • Description of how Marketplace reports and reconciles enrollment transactions and APTC/CSR payment information in coordination with issuers • Description of how the Marketplace and SHOP will report mid-year changes in enrollment to issuers • Discussion on how the state is able to receive and process changes in circumstances reported by MAGI-based beneficiaries • Description of how the Marketplace will process Special Enrollment Periods • Timeline with milestones for the Marketplace to test IRS Reporting with CMS for enrollment transactions Discussion(s): 4. Are MAGI-based beneficiaries able to report changes in circumstances via the following modalities? a. Online via an electronic account b. Phone c. Mail d. In person e. If another modality is available, please specify 5. For Medicaid beneficiaries determined ineligible based on MAGI due to a change in circumstances, is the state able to evaluate potential eligibility on a non-MAGI basis? What is the state's process for doing so? 6. For beneficiaries determined no longer eligible, is the state	Jenny Chen (Eligibility & Enrollment, CCIIO) Dawn Horner (Eligibility & Enrollment, CCIIO) David Koppel (Medicaid, CMCS) Susie Cummins (Medicaid, CMCS)

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
			able to evaluate potential eligibility for other insurance affordability programs and transfer the individual's electronic account to the appropriate program?	
5:15 pm – 5:30 pm (15 Minutes)		**Close out day 1** • Day 1 takeaways		
Day 2: Thursday October 16, 2014 (Call Information: 1-877-885-1087, Access: 301-838-3883, Webinar Information: https://webinar.cms.hhs.gov/orrday2review)				
9:00 am - 9:15 am (15 minutes)		**Welcome back** • Day 2 expectations		
9:15 am-10:45	**Medicaid Review** (Policy/Operations Discussion	**Financials and APD Status (Medicaid specific)** 1. Is the state reporting enhanced match expenditures in a timely manner (within a year)? 2. If the state has not yet requested 75/25 for eligibility workers, are there plans to do so in FFY2015?		Idaho: DHW CMS: David Koppel (Medicaid,

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
am (1.5 hours)	only)	**Renewals and Redeterminations: Medicaid & CHIP** 1. Transition of 2013 legacy Medicaid beneficiaries a. Have all 2013 Medicaid beneficiaries in previously AFDC-related eligibility categories and separate CHIP been converted to MAGI? 2. MAGI-based renewal functionality a. Can the state renew Medicaid and CHIP beneficiaries on an *ex parte* basis? b. Can the state send pre-populated renewal form to Medicaid and CHIP beneficiaries who cannot be renewed on an *ex parte* basis? c. Can beneficiaries complete pre-populated form via each of the following modalities? i. Online ii. Phone iii. Mail In person iv. If another modality is available, please specify: d. How many days do individuals have to return the renewal form? e. If online renewal is available, what is the process? f. Can the state process a MAGI-based determination for beneficiaries who return the prepopulated form? 3. Is the state able to accept and process returned renewal forms within the 90 day reconsideration period after an individual's termination? 4. Evaluation for coverage on other bases a. For Medicaid beneficiaries determined ineligible based on MAGI, is the state able to evaluate potential eligibility on a non-MAGI basis? What is the state's process for doing so? b. For Medicaid beneficiaries in a MAGI-exempt category who are determined ineligible for continued coverage on the MAGI-exempt basis, is the state able to evaluate potential eligibility based on MAGI? What is the state's process for doing so? 5. For beneficiaries determined no longer eligible, is the state able to evaluate potential eligibility for other insurance affordability programs and transfer the individual's electronic account to the appropriate program? 6. How is the state monitoring the success of the renewal process, if it involves re-application? **Interface with MMIS** 1. For both Medicaid and the state's separate CHIP, does the state have an interface between the system that determines eligibility and its MMIS system to support electronic transfer of information for timely enrollment of eligible individuals? 2. Tracking of premiums and cost sharing (Medicaid) a. Does the state's system support tracking of incurred premiums and cost sharing for all members of the Medicaid		CMCS) Susie Cummins (Medicaid, CMCS) *Additional CMCS SMEs who may join:* Jessica Kahn (Medicaid, CMCS) Chris Gerhardt (Medicaid, CMCS) Anne Marie Costello (Medicaid, CMCS) Judith Cash (Medicaid, CMCS) Patricia Nowakowski (Medicaid, CMCS) Sarah Delone (Medicaid, CMCS) Rebecca Bruno (Medicaid, CMCS) Elizabeth Walker (Medicaid, CMCS) Jodie Anthony (Medicaid,

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
		household to ensure that individuals do not exceed the aggregate limit of 5% of family income (and is it currently being used to do so)? b. If Yes, is the state using: i. The MMIS ii. The Eligibility System iii. Both systems iv. Outside Entity (ex. health plan) v. If No, how does the state ensure that aggregate premiums and cost sharing do not exceed the maximum amount permissible? 3. Tracking of premiums and cost sharing (separate CHIP) a. Does the state's system support tracking of incurred premiums and cost sharing for individuals enrolled in the state's separate CHIP to ensure that individuals do not exceed the aggregate limit of 5% of family income (and is it currently being used to do so)? [yes/no, if no, free text] b. If Yes, is the state using: i. The MMIS ii. The Eligibility System iii. Both systems iv. Outside Entity (ex. health plan) c. If No, how does the state ensure that aggregate premiums and cost sharing do not exceed the maximum amount permissible? 4. Does the eligibility system or the MMIS have the capability to track beneficiary cost sharing for Medicaid? 5. Does the eligibility system or the MMIS have the capability to track beneficiary cost sharing for CHIP? Are newly determined individuals' cases transferred to the MMIS for enrollment within 24 hours? **Hospital Presumptive Eligibility** 1. Have any hospitals in the state begun making PE determinations? 2. Is the state able to receive notice of a presumptive eligibility determination from hospitals? If yes, how can hospitals notify the state of their determinations: ___electronically, ___by phone, ___by mail, ___ by fax, ___other 3. If the state has set performance standards for hospitals to follow, how are the hospitals doing in meeting these standards? **a.** Does the state's eligibility system support ending eligibility at a mid-month date? (Per 435.1100, PE enrollment periods end on the date that a full eligibility determination is made by the state). (note: this is relevant to regular PE as well).		CMCS) Jason Berry (Medicaid, CMCS) Mary Jones (Medicaid, CMCS) Courtenay Savage (Medicaid, CMCS)

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
		Eligibility for All MAGI-Based Eligibility Groups- Medicaid & CHIP Hospital 1. Can the state systems support determinations of eligibility under: a. All mandatory MAGI-based Medicaid eligibility groups (parents/caretaker relatives per 42 CFR 435.110; pregnant women per 435.116; children per 435.118; and, if applicable, adult group per 435.119) b. All MAGI-based optional Medicaid eligibility groups elected by the state (e.g., all or a reasonable classification of individuals under age 21 per 42 CFR 435.222; state adoption assistance children per 435.227; optional targeted low-income children under 435.229, etc.) c. Former foster care children per section 1902(a)(10)(A)(i)(IX) of the Act. d. Separate CHIP **Inmate Eligibility** 1. How does the state implement the restriction on FFP for services provided to inmates of a public institution who are enrolled in Medicaid at the time of their incarceration or commitment to another public institution? a. The state maintains enrollment for the inmate and limits claims to the services described in section _____ of the Act. b. The state suspends inmates' eligibility. c. The state terminates inmates' eligibility. 2. How does the state implement the restriction on FFP for services provided to inmates of a public institution who are assessed/determined eligible for Medicaid by the Marketplace? a. The state approves eligibility and enrolls inmates for coverage (and limits claims to the services described in section _____ of the Act). b. The state approves, but suspends inmates' eligibility. c. The state denies/terminates eligibility to inmates. 3. Does the state accept applications for inmates of a public institution? If so, how does the state handle inmates who meet the eligibility requirements for coverage? a. The state approves eligibility and enrolls inmates for coverage (and limits claims to the services described in section _____ of the Act). b. The state suspends inmates' eligibility. c. The state denies eligibility to inmates. Does the state ensure that inmates who are eligible for Medicaid are enrolled for coverage upon release? If so, briefly describe the process employed.		

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
		Determine Retroactive Eligibility 1. Is the state system able to support determinations of retroactive Medicaid eligibility for MAGI-based individuals who submit an application to the state agency? 2. If so, what is the state's process for obtaining information needed to determine retroactive Medicaid eligibility? 3. Is the state system able to support make determinations of retroactive eligibility for MAGI-based individuals who submit an application to the Marketplace? If so, what is the state's process for obtaining information needed to determine retroactive eligibility? **Emergency Medicaid** 1. Does the state's system support eligibility for Medicaid coverage of emergency medical services (including labor and delivery)? 2. Medicaid eligibility for coverage of emergency services for individuals who are ineligible for full Medicaid benefits due only to lack of satisfactory citizenship or immigration status: a. For such individuals who submit an application directly to the state agency, is the state able to approve eligibility and enroll the individual for coverage of emergency services at the point of application regardless of whether or not the individual currently is in need of emergency medical services for? What is the state's process for doing so? b. For such individuals determined/assessed eligible for Medicaid by the Marketplace and whose account is transferred to the state agency, is the state able to approve eligibility and enroll the individual for coverage of emergency services at the point of application regardless of whether or not the individual currently is in need of emergency medical services? What is the state's process for doing so? Are individuals who receive Medicaid coverage for emergency medical services terminated as soon as the emergency services are no longer needed or are the state able to retain enrollment of such individuals, with a benefit package limited to emergency services, until a regularly-scheduled renewal? **Performance Indicators** 1. Has the state met with any challenges collecting the required performance indicator data? 2. What improvements/changes will be made in FFY2015 to support performance indicator data collection?		

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
		Integrated Systems and Negative Actions: Interplay Around Negative Actions In Integrated Systems related to the Basic/Core Functionality 1. Has the state begun work on human services integration? 2. What are the specific services the state will develop for integration in FFY2015? • If the system is already integrated, are their challenges around initiating negative actions for just Medicaid/CHIP?		
10:45 am-11:00 am (15 Minutes)		**Break**		
11:00 am-12:00 pm (1 hour)	**Medicaid Review**	**Continue discussion with CMCS**		
12:00 pm-1:00 pm (60 minutes)		**Lunch on your own**		
1:00 pm-2:00 pm (1 hour)	**Plan Management**	**Demo 4: Plan Management** Demo Objective(s): • State Plan Review Screens • Issuer Plan Review Screens • Loaded into Plan Select Screens – Individual and SHOP Discussion(s): • Understand plan error correction process		Idaho: YHI, DHW CMS: Yolande Calhoun (Information Technology, OIS)

FINAL

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
				Rochelle Rupp (Plan Management, CCIIO)
2:00 pm-3:00 pm (1 hour)	Consumer Assistance	**Demo 5: Consumer Assistance** Demo Objective(s): • Navigator Screens • Navigator Account Creation Process • In-Person Assistors • In-Persons Account Creation Process • Customer Service Representatives Discussion(s): 1. How an application is submitted on behalf of an individual? 2. How are Navigators identified and certified? 3. How an application is submitted on behalf of an individual? How are In-Person Assisters identified and certified?		Idaho: YHI, DHW CMS: Yolande Calhoun (Information Technology, OIS) Ellen Witman (Consumer Assistance, CCIIO)
3:00 pm-3:15 pm (15 minutes)		**Break**		
3:15 pm-4:15 pm (1 hour)	Technical	**Demo 6: Technical** Demo Objective(s): • System logs and database updates • Production server updates • Disaster Recovery (DR) and Failover • IT Security and Privacy • Federal Tax Information • 508c Compliance • Test Results o IV&V reports (vendor/submission)		Idaho: YHI, DHW CMS: Yolande Calhoun (Information Technology, OIS)

Time (MT)	Topic Area	Objectives & Discussions		Participants
		IT	Policy/Operations (2014 Blueprint: 3.0 Eligibility & Enrollment)	
		○ Stress Test ○ Performance Measures • Loading code into CALT for reuse purposes		
4:15 pm-4:45 pm (30 minutes)	**Program Management**	• Work-Around Functionality • Contingency Plans • Mitigation Planning, including any mitigations for critical success factors		Idaho: YHI, DHW CMS: Yolande Calhoun (Information Technology, OIS)
4:45 pm-5:15 pm (30 minutes)		**Close out day 2** • Day 1 & 2 takeaways • Next Steps		CMS: Czarina Biton (CCIIO) Yolande Calhoun (Information Technology, OIS) Susie Cummins (Medicaid, CMCS) David Koppel (Medicaid, CMCS)

Riverside County
Department of Public Social Services

Customer Care Center
Readiness Assessment Report

Version 2.0
June 8, 2012

Revision History

Version No.	Date	Summary of Changes	Modified By
1.0	07/08/12	Original submission	Yen L. Pham
2.0	07/13/12	Incorporated client's comments from 7/11/12 meeting.	Yen L. Pham

Table of Contents

1.0 Roles and Responsibilities **4**

2.0 Executive Summary **4**

3.0 Approach and Methodology **4**

4.0 Assessment and Recommendations **7**

4.1.1 Summary of Areas Analyzed *7*
4.1.2 Detailed Analysis and Recommendations *8*

5.0 Appendix A **27**

5.1.1 Acronyms *27*
5.1.2 As-Is CCC Business Model *28*
5.1.3 As-Is CCC Workflow T-Tech *29*
5.1.4 As-Is CCC Workflow I-Tech: C4Yourself *30*
5.1.5 As-Is CCC Workflow I-Tech: Healthy Families (HF) *31*
5.1.6 As-Is CCC Workflow I-Tech: Inter County Transfers (ICTs) *32*
5.1.7 As-Is CCC Workflow I-Tech: Inter District Transfers (IDTs) *33*
5.1.8 As-Is CCC Workflow I-Tech: Mail and Fax *34*
5.1.9 As-Is CCC Workflow I-Tech: Phone In *35*
5.1.10 As-Is CCC Workflow I-Tech: Referrals Breast Cancer *36*
5.1.11 As-Is CCC Workflow I-Tech: Referrals Low Income Subsidy *37*
5.1.12 As-Is CCC Workflow I-Tech: Referrals Juvenile *38*
5.1.13 As-Is CCC Workflow I-Tech: Referrals SSI/SSP Denials and Terminations *39*
5.1.14 As-Is CCC Workflow C-Tech *40*
5.1.15 As-Is CCC Workflow C-Tech: Specialty and Combo *41*

1.0 Roles and Responsibilities

This section identifies First Data and Riverside County Department of Public Social Services roles and responsibilities associated with the Customer Care Center Readiness Assessment deliverable. The following table documents the roles and responsibilities associated with the development, review and approval of the Readiness Assessment deliverable.

Deliverable Roles and Responsibilities

ROLE	PERSON	RESPONSIBILITY
First Data Deliverable Owner	Yen L. Pham	Responsible for the Readiness Assessment deliverable.
Riverside County Department of Public Social Services- Customer Care Center	Anna Martinez	Responsible for feedback, and approval to the deliverable.

2.0 Executive Summary

The Department of Public Social Service (DPSS) provides a variety of financial, medical benefits and public assistance services to the residents of Riverside County. DPSS has a total of 18 district offices, handling approximately 180,000 active cases throughout the County. Of the 18 Districts, the Customer Care Center (CCC) serves Jurupa, La Sierra, and Moreno Valley Districts which has a total of 65,000 active cases.

First Data is engaged to provide an assessment of the Riverside County Department of Public Social Services (DPSS) Customer Care Center (CCC) in preparation for implementation of the C-IV Service Center Solution. The goal is to evaluate the current operational processes and procedures to identify gaps, risks and/or issues that would potentially impact the successful implementation of the C-IV Service Center Solution, as well as provide recommendations where improvements might need to be made.

Within the Readiness Assessment, First Data has identified 33 areas of various types and levels of issues, risks and concerns to the CCC. Each of these areas has been categorized by level of impact, and is also supported by one or more recommendations for making positive change.

3.0 Approach and Methodology

In order to conduct the Readiness Assessment of the County's CCC, First Data has reviewed the CCC planning activities with respect to Business Model, Operations, Business Process Management and Change Management, and impact to the C-IV Service Center Deployment Schedule. In addition, First Data has identified risks and issues where applicable. First Data will facilitate planning efforts to address issues and risks, as well as provide support in preparation

of the Deployment of the C-IV Service Center Solution. The status of these project activities is as follows:

1. Project Initiation and Approach *(Completed)*
2. Conduct Preliminary Assessment *(Completed)*
3. Prepare the Readiness Assessment Report *(Completed)*
4. Facilitate Strategic Planning *(In Progress)*
5. Support County to Prepare for Deployment of the C-IV Service Center Solution *(In Progress)*

The following paragraphs describe the methodology for accomplishing this effort.

Project Initiation and Approach

As part of the startup of the Readiness Assessment, First Data conducted a kickoff meeting with Riverside County DPSS Management, and any other key stakeholders to:

- Establish communication channels with DPSS Management, and other stakeholders; and
- Initiate the assessment of the CCC and provide an overview of the Readiness Assessment approach.

Conduct Preliminary Assessment

As part of this assessment, First Data evaluated current business processes associated with the proposed County work plan (CCC Annex Work Plan). The current business processes are documented in Appendix A. First Data met with various Managers, Supervisors, Clerical, T-Tech, C-Tech and I-Tech of the CCC in gathering this information. The activities that were analyzed included:

- Business Model
- Operations
- Business Process Management
- Change Management

Prepare the Readiness Assessment Report

First Data has created a formal report (this deliverable) to document the results of the analysis performed and the recommendations for each activity as appropriate, utilizing past Contact/Service Center project performance analysis and lessons learned as an input into identifying and proposing recommendations. The results of this assessment will help Riverside County understand if the current operational processes and procedures are well documented, appropriately communicated and executed and where improvements might need to be made.

Facilitate Strategic Planning

First Data will evaluate the areas described above and work with the County to define the strategy for integrating their existing CCC to the C-IV Service Center Solution. In addition, First Data will utilize information from the preliminary assessment to define the objectives of the

CCC and create a timeline to map those objectives. The timeline will reflect the logical sequence of the activities associated with the objectives and the recommended milestones.

Support County to Prepare for Deployment of the C-IV Service Center Solution

First Data will support the County with planning and coordination efforts to ensure key operational and business processes are in place and County Staff is prepared for the C-IV Service Center Solution. This support will include:

- Creating and/or refining work plans;
- Aligning activities with the C-IV Service Center Project Schedule; and
- Supporting Management and Staff with their activities.

4.0 Assessment and Recommendations

This section includes the analysis and recommendations identified as part of the Readiness Assessment effort. Each area of concern has been categorized has having a high, medium or low impact to the success of the implementation of the C-IV Service Center Solution. First Data has qualified each area/recommendation using the following taxonomy:

- **High** - The area has a major impact to the organization, and needs immediate attention. It is critical to the success of the C-IV Service Center Solution deployment.
- **Medium** - The area has a moderate impact to the organization, and should be addressed to avoid further downstream effect. It does not have a direct impact to the success of the C-IV Service Center Solution deployment but an Action Plan should be developed.
- **Low** - The area has a low impact to the organization, and should be addressed. It does not have a direct impact to the success of the C-IV Service Center Solution deployment but an Action Plan should be developed.

4.1.1 Summary of Areas Analyzed

The following table represents a summary of the areas that were analyzed:

Area	Sub-Area
Business Model	Governance
	Organizational Structure
Operations	Staffing
	Tools
	Reports
	Workload Management
	Key Performance Indicators
Business Process Management	Agent Processes
Change Management	Training/Staff Development
	Communication

4.1.2 Detailed Analysis and Recommendations

#	Area	Sub Area	Impact	Analysis	Recommendations
1.	Business Model	Governance	High	The CCC lacks defined and documented roles and responsibilities, cohesive policies and procedures, guidance and accountability. Over time, multiple changes have been implemented in order to mediate various issues, but the changes have created additional layers in the business process which are not necessary. This has led to an unstable environment with a decline in employee morale, decrease in customer satisfaction and decrease in efficiency.	Establish governance. Having governance is critical factor to the success of the CCC. The governance structure establishes the strategic, and operational decision-making process required to ensure the CCC can excel in its goals. Governance provides strategic leadership, establishes priorities, and policies, and is accountable and transparent to the CCC.

#	Area	Sub Area	Impact	Analysis	Recommendations
2.	Business Model	Organizational Structure	High	The CCC serves the Jurupa, La Sierra and Moreno Valley Districts. There are three types of Eligibility Technicians within the CCC: T-Tech, C-Tech and I-Tech: • The T-Techs takes incoming calls and processes core-Tasks related to the Continuing cases. • The C-Techs processes core-Tasks related to the Continuing cases. • The I-Techs processes non face-to-face applications related to the Intake cases. (Reference Appendix A CCC Business Model.) Though the CCC is a Service Center, it also takes on the responsibilities similar of a District Office, which adds another layer within the CCC. The CCC currently has an enormous amount of delinquent Core and Non-Core Tasks, in addition to an extremely high Average Queue Time and Abandon Rate.	The CCC should consider changing their business model to operate as a pure Service Center. An option would be to separate the C-Tech, I-Tech and associated Office Assistance Staff from the CCC umbrella and have them operate similar to a District Office. This would allow the CCC to focus the efforts on increasing customer satisfaction, improving morale and increasing productivity. In consideration of changing to a different business model, the CCC should take into account long term goals and how they would fit into the new business model.

#	Area	Sub Area	Impact	Analysis	Recommendations
3.	Business Model	Organizational Structure	Low	The CCC handles CalFresh and Medi-Cal programs for both Intake (non-face-to-face applications) and Continuing cases.	The CCC should consider handling the CalWORKs program since a large number of customers are receiving CalWORKs benefits. In addition, the C-IV IVR which is part of the C-IV Service Center Solution can accommodate CalWORKS as one of the self-service options. The CCC should also consider the staff resources needed if CalWORKs were to be part of the CCC.
4.	Business Model	Organizational Structure	Low	There is a perception that there are approximately 200 Techs that handle incoming calls at the CCC. However, only 14% of the Techs are actually dedicated to taking incoming calls, as the remaining resources are allocated to processing applications and tasks.	In combination with business model/organizational changes, the CCC should consider rebranding themselves, this could aid in developing a new image and perception of the CCC. This could include a name change along with marketing of the CCC.

#	Area	Sub Area	Impact	Analysis	Recommendations
5.	Business Model	Organizational Structure	Medium	The C-Tech, I-Tech and Office Assistance (OA) are not co-located. There are inconsistencies in work flow amongst the C-Tech, I-Tech and OA. The work is interrelated and as it is passed down to the next person, the C-Techs often re-do the work which is very time consuming. Since expectations have not been set, it is unclear where specific responsibilities reside. (As of 9/1/12, they will all be located at the CCC.)	Define and document workflows. Establish roles and responsibilities. Set expectations and enforce accountability. This would increase efficiency and avoid re-work. Ideally, centralizing the C-Tech, I-Tech and OA would help Management hone on the workflow inconsistencies and better control how work should be processed.
6.	Business Model	Organizational Structure	High	The CCC has two Regional Manager, one Regional Manager for CCC Continuing Operations and the other for CCC Intake/Clerical /Telephone Operations. Owning all three areas of Intake/Office Assistance/Telephone Operations is difficult to sustain due to competing priorities and breadth of responsibilities.	Establish a Regional Manager for Telephone Operations. This will allow the person to focus on the Service Center related items such as customer satisfaction, center and agent metrics, and Staff Development, etc. Establish a CCC Regional Manager to oversee all four areas. Their role will be to have an overall view to ensure all areas are working cohesively; and to review and refine processes to ensure that goals are consistently being met in an effective and efficient manner.

#	Area	Sub Area	Impact	Analysis	Recommendations
7.	Operations	Staffing	High	There are approximately 27 T-Techs. The T-Techs spend 50% of their time taking incoming calls, and spend the remaining time processing assigned tasks. This contributes to the 30 minutes Average Wait Time, and 47% Abandon Calls. This has caused an increase in customer dissatisfaction and an increase in stress level for the T-Techs.	The T-Techs should solely focus on taking incoming calls. (This change is already scheduled to occur as of 8/1/12.) Having the T-Techs fully dedicated to taking incoming calls and increasing the number of T-Tech staff would improve customer satisfaction, decrease stress level for the T-Techs and improve Average Wait Time and Abandon Rate. Re-evaluate the T-Tech workflow and identify where handoffs can occur. This could also improve the Average Wait Time and Abandon Rate. An estimate of 56 Agents has been recommended by the Development Vendor. After 6 months, a re-evaluation of the KPI's should be done against the number of Agents to identify staffing baselines.

#	Area	Sub Area	Impact	Analysis	Recommendations
8.	Operations	Staffing	Medium	There are 25 Office Assistants (OA). The OA play a large part in the upfront processing of applications and referrals. In some instances, such as processing of ICTs and Phone In, there are several handoffs from one OA to another OA. The process is very cumbersome (Reference Appendix A CCC Workflow I-Tech). It is unclear why there are numerous handoffs. Since the expectations have not been set, it is unclear where the responsibilities reside. The ratio of OA to ET is unclear and not defined.	Define and document workflows. Establish roles and responsibilities. Set expectations and enforce accountability. Re-evaluate the clerical processes to see where they can be streamlined. Evaluate the ratio of OA to ET and their tasks against the Non-Metro Districts to provide a gauge of the number of OAs needed and establish a staffing baseline. Establish a workgroup to define and document workflows for the OAs processes.
9.	Operations	Staffing	Medium	There are 25 I-Techs. The I-Techs handle various non-face-to-face applications. Currently, there is no back log identified. Expectations have not been set. The ratio of I-Tech is unclear and not defined.	Define and document workflows. Establish roles and responsibilities. Set expectations and enforce accountability. Evaluate the number of applications received for the CCC in comparison with the Non-Metro Districts to provide a gauge of the number of I-Techs needed and establish a staffing baseline. Establish a workgroup to define and document workflows for the I-Techs processes.

#	Area	Sub Area	Impact	Analysis	Recommendations
10.	Operations	Staffing	Medium	There are 81 C-Techs. There is an enormous backlog of Core and Non-Core Tasks. It is unclear whether this is due to understaffing or due to the existing backlog. The ratio of OA to ET is unclear and not defined. Since expectations have not been set, it is unclear where responsibilities reside.	Define and document workflows. Establish roles and responsibilities. Set expectations and enforce accountability. In order to establish a staffing baseline, the backlog must first be cleaned up. Establish a workgroup to define and document workflows for the C-Techs processes.
11.	Operations	Staffing	High	The T-Techs have indicated more assistance is needed from the Supervisors. There is a lack of Supervisors on the floor to assist, which has caused anxiety and stress with Staff.	The Supervisors should become more accessible and establish a presence for their Staff. The industry standard for Supervisor to Staff is 10:1. The roles and responsibilities need to be defined and documented to set expectations, as well as enforce accountability.

#	Area	Sub Area	Impact	Analysis	Recommendations
12.	Operations	Staffing	High	There are three Workforce Management (WFM) resources. The WFM Team executes daily and scheduled reports, some reports are not utilized. Since expectations have not been set, their roles and responsibilities are unclear.	Define and document workflows. Establish roles and responsibilities. Set expectations and enforce accountability. It is extremely important to define the WFM role, as they will play a key role in managing and monitoring operations to ensure the KPIs are met.
13.	Operations	Staffing	High	The CCC core hours are Monday through Thursday from 7:00 am - 6:00 pm. The CCC phone hours of operation are Monday through Thursday from 8:00 am – 5:30 pm. This makes it difficult to hold meetings and provide training for the T-Techs.	Establish two shifts for the T-Techs, with an early and a later shift with overlap to allow time for meetings and training. Rolling breaks and lunchtime should also be established.

#	Area	Sub Area	Impact	Analysis	Recommendations
14.	Operations	Tools (Workload Assignment)	High	The CCC lacks a consistent method of managing and tracking Tasks. The CCC currently uses a combination of C-IV Tasks and a Matrix Tool (excel spreadsheet). It is difficult for Management to get a true accurate count of all Tasks outstanding. Tasks have become unmanageable as there is no real way of tracking all Tasks. Management is not able to complete an analysis, as the reports are coming from several different data sources.	Establish one tool to manage and track Tasks. An option could be to use the Task functionality in the C-IV System to track and manage Tasks. This will ensure all Tasks are tracked in one place and reports are accurate.
15.	Operations	Tools (Workload Assignment)	Medium	The Workload assignment for the I-Tech is currently a manual process. There is a manual rotation log for each of the non-face-to-face applications. (Reference Appendix A CCC Workflow I-Tech.) The manual rotation logs are not consistent amongst the Metro Districts.	Evaluate each type of non-face-to-face applications process, and streamline the process and establish a tool to be used amongst the Metro Districts. This will establish consistency and efficiency.

#	Area	Sub Area	Impact	Analysis	Recommendations
16.	Operations	Tools (Workload Assignment)	High	The Workload Assignment for the C-Tech currently is a manual process. An excel spreadsheet is used to track and assign Tasks to the C-Techs on a monthly basis. It is extremely cumbersome and there are numerous handoffs. (Reference Appendix A CCC Workflow C-Tech.)	Evaluate the manual process and streamline the process. If the CCC were to move to the Daily Task approach, this would eliminate the need for a manual process.
17.	Operations	Tools (CCC)	High	The current tools used to manage and monitor the CCC will be replaced by the C-IV Service Center Solution as follows: • Solidus Info Manager equivalent to Exony • Solidus Report Manager equivalent to Exony Reporting • Solidus Desktop Agent Manager equivalent to Cisco Agent Desktop • Monet WFM equivalent to NICE WFM Except for the C-IV System and MEDS, there are no other applications used by the T-Tech. The current Solidus IVR menu will be replaced by the C-IV IVR menu.	Since the current tools will be replaced, a detailed analysis was not performed. Once the Development Vendor is onsite, a thorough discussion of the new tools should occur to better understand the capabilities. In addition, a thorough discussion of the C-IV IVR menu should occur to better understand the routing capabilities. The NICE Quality Monitoring Solution will be deployed as part of the C-IV Service Center Solution. This will provide the CCC the ability for call monitoring and recording. In addition utilize the tool as an opportunity for coaching and mentoring.

#	Area	Sub Area	Impact	Analysis	Recommendations
18.	Operations	Tools (Red Alert)	High	During 'Red Alert', the T-Techs advise the customer they are unable to assist at this time due to high call volumes and they will receive a call back within 24 to 48 hours. This is an issue as the Customers do not always receive a call within the promised 24 to 48 hour timeframe.	Eliminate the 'Red Alert' as this is only causing customers frustration and stress on the T-Techs. Establish an Escalation Plan which outlines operations procedures when call volumes are at peak.
19.	Operations	Reports	High	The CCC lacks a consistent reporting tool. The report data is extracted from various sources, though it is not clear which is the most accurate source. Management extracts the data provided to create their own reports. While there are numerous and various reports generated, they are not being utilized for fear of inaccurate data. Reports are emailed, where others are placed on a shared drive.	Establish a reporting tool. Define the needs, goals, and the audience of the report. Designate a person or group to execute the reports. Establish a single repository for reports. This will ensure the reports are accurate and consistent across the board.

#	Area	Sub Area	Impact	Analysis	Recommendations
20.	Operations	Workload Management	High	The Core-Tasks are currently assigned to the C-Tech on a monthly basis using the Matrix Tool (excel spreadsheet). This is not manageable and creates stress upon the C-Techs. It is difficult to quantify a 'manageable' workload as some of these Tasks could be due tomorrow or in two months. Management does not have a workload baseline and is unable to determine what a manageable workload looks like. It is difficult to hold Staff accountable.	Change the assignment of Tasks from monthly to a daily basis. This ensures Tasks that are urgent in nature are handled immediately. Assigning Tasks on a daily basis will allow Staff to better manage their day. With the 'Daily Task' approach, the CCC could utilize C-IV Task Reports to track the tasks assigned and determine a manageable workload in order to establish a workload baseline. If more details are needed then what is provided by the C-IV Task Reports, work with the internal Ad Hoc group to create reports that will meet the needs.
21.	Operations	Workload Management	High	The Cases are not owned by a Worker, there are 48 virtual caseloads that are maintained. These virtual caseloads are based on old methods and are no longer needed. The 48 virtual caseloads have created unnecessary additional work.	If the CCC were to go with the 'Daily Task' approach, the 48 virtual caseloads could be reduced to fewer caseloads for ease of manageability. An option could be to group by Language or Programs or both.

#	Area	Sub Area	Impact	Analysis	Recommendations
22.	Operations	Workload Management	High	There is a significant backlog in Core Tasks (RE's, MSR's, RC's, and QR7's), approximately 5,908 are delinquent. It is unclear how the Core Tasks have expanded. There is no current plan in place to handle these Core-Tasks.	The Core Tasks should be cleaned-up prior to the Go-Live Date of the C-IV Service Center. Otherwise the CCC will be at risk for failure and will be unable to determine a workload baseline. Establish a plan to clean up the Core Tasks. Some options are: • Allocate the Tasks across the other Districts; • Use Friday to process backlog; • Utilize a temporary agency to assist with the back log; or • A combination of the above.
23.	Operations	Workload Management	High	There is a significant backlog in Non-Core Tasks, approximately 64,000 have accumulated. This number will continue to grow as these Tasks are not being processed by the C-Techs. There is no current plan in place to handle these Non-Core Tasks.	The None-Core Tasks should be cleaned-up prior to the Go-Live Date of the C-IV Service Center. Otherwise the CCC will be at risk for failure and will be unable to determine a workload baseline. Establish a plan to clean up the Core Tasks. Some options are: • Allocate the Tasks amongst the other Districts; • Use Friday to process backlog; • Utilize a temporary Agency to assist with the back log; or • A combination of the above.

#	Area	Sub Area	Impact	Analysis	Recommendations
24.	Operations	Key Performance Indicators	High	The CCC lacks Key Performance Metrics (KPIs). The CCC has been operating under 'what feels like a good number' and has been in 'survival' mode. The current CCC Monthly Stats are: • % of Calls Abandon = 47% • Average Queue Time = 30 minutes The CCC has been unable to: • Establish baselines and performance goals for both individuals, and the CCC overall. • Identify strengths and weaknesses in the CCC. • Diagnose and understand the underlying drivers of performance gaps. • Prescribe actions to improve performance.	Key Performance Indicators (KPI) plays a key role, within a call center environment. KPIs bring accountability to both the CCC and its Staff. Effective performance measurement is critical to success and effective decision making. Establish the following KPIs : • Accessibility Metrics are used to evaluate how accessible the call center is to a caller. It includes evaluations of how long it took to answer a call, along with information about abandoned calls and calls placed on hold. • Efficiency Metrics are used to evaluate the efficiency of call center workers. It includes Average Handle Time, Agent Utilization, Calls/FTE (average direct cost per call), and Actual call time versus actual wrap up time. • Effectiveness Metrics are designed to measure the effectiveness of the CCC to handle customer contacts and the effectiveness of the WFM team. The cornerstone of contact resolution is measuring when calls (contacts) were

#	Area	Sub Area	Impact	Analysis	Recommendations
					resolved. It includes First Contact Resolution (FCR) Rate, Forecast Accuracy Index and Scheduling Accuracy Index.
25.	Operations	Workload Management	High	The CCC imaging process at Intake and Continuing are inconsistent, which inadvertently impacts the call volumes. There are District policies on Imaging processing timeframes but they are not in adherence, this has affected customer's benefits. In turn, the customers call the CCC to inquire about their benefits but the T-Techs do not have information to provide if the documents have not been imaged. This causes frustration to the customers and to the T-Techs.	Either enforce the District imaging policy or establish an imaging policy for the CCC. This would increase customer satisfaction and potentially reduce call volumes.
26.	Operations	Workload Management	Medium	Earlier in the year a BPS was completed at Riverside County. These new processes could potentially impact the CCC operations.	An evaluation of the BPS should be done to assess what needs to be integrated into the CCC. For example, is the BPS CalFresh Intake process different from the CCC CalFresh Intake process that is handled by the C-Techs. If they are different, this process should align to ensure consistency across Districts.

#	Area	Sub Area	Impact	Analysis	Recommendations
27.	Business Process Management	Agent Processes	High	The CCC has existing CCC Workflows but they are not relevant, not being used and is not centrally located. This has caused inconsistencies in delivering service to the customers. Some calls take longer to resolve and it is unclear to the T-Techs how long they should stay on the phone to assist the customers and when they should handoff to another unit. This has caused the T-Techs to create their own process within their unit. Some of the T-Techs take down customers' phone numbers to call the customers back. While other T-Techs create a Task for themselves to be processed later. This has created a ripple effect because while they are calling the customers back, new calls have come into the queue.	Re-define and document workflows. Establish roles and responsibilities. Set expectations and enforce accountability. Identify and document where the handoffs should occur, this would provide clear direction to the T-Techs and eliminate the need to create other 'customized' processes. Establish 'Average Talk Time', this would provide a gauge for the T-Techs to monitor their time on the call with the customer. These mechanisms provide the T-Techs with set expectations to deliver consistent services which leads to an increase customer satisfaction and confidence level of the CCC. Establish a Workgroup to re-define and document workflows for Agent processes.

#	Area	Sub Area	Impact	Analysis	Recommendations
28.	Business Process Management	Agent Processes	High	The CCC lacks consistent direction from Management. While some Management have advised the T-Techs to 'do what it takes' to resolve a call, others have used the 'Average Talk Time' of the unit as a guideline. This has caused confusion amongst the T-Tech and the customers.	Management should be consistent in the messages they deliver to the Staff.

#	Area	Sub Area	Impact	Analysis	Recommendations
29.	Business Process Management	Agent Processes	High	The T-Techs handles both CF and MC. Staff has indicated it is difficult to handle both due to lack of program knowledge. There is a lack of tools readily available for the T-Techs such as Change Discussion Guides, Manuals, etc.	Split the T-Techs. Those that are more knowledgeable in both CF and MC should remain as 'dual'. Those that are not a knowledgeable in both should set one program as their primary skill set and the other as their secondary skill set until they can become more proficient. This automatic call routing can be done via the Automatic Call Distributor (ACD) which is part of the C-IV Service Center Solution. The CCC should create the 'How To' guides for the T-Techs to reference while on a call with the customer. This should alleviate anxiety and stress and better serve the customers.
30.	Change Management	Training	High	The CCC lacks training for the T-Techs. There is only induction of Eligibility Training. The T-Techs have indicated they are not familiar with C4Yourself functionality and are unable to assist the customers.	Develop a Training Curriculum for the T-Techs. This could include C4Yourself Overview, Business Processes, Customer Service, KPIs and refresher courses on various programs. Establish a Workgroup to develop the Training Curriculum.

#	Area	Sub Area	Impact	Analysis	Recommendations
31.	Change Management	Staff Development	High	The CCC lacks Staff Development for the T-Techs. The T-Techs have indicated there is no clarity on their role and expectations and unsure about the progression of future opportunities.	Define and document the T-Tech roles and responsibilities. Establish Call Quality Expectations and integrate this as part of performance expectations. Provide mentoring and coaching.
32.	Change Management	Communication	High	The CCC has recurring meetings with Staff and the Districts. The non-CCC Districts are unclear of the CCC operations and are not vested in the CCC.	Establish a Communication Plan that includes frequency, audience, method, owner, etc. Educate the Districts on the type of services the CCC offers. This will provide transparency within the CCC and to the outlying Districts.
33.	Change Management	Communication	High	Currently, the IVR and C4Yourself are not widely marketed. The usage of IVR and C4Yourself will be increased as these will integrated as part of the new C-IV Service Center Solution.	Start marketing IVR and C4Yourself to the customers. This will help customers become more aware of the self-service capabilities that are available and ensuring customers understand the function the CCC plays in management of their cases. Both of which could potentially decrease the call volumes. Establish Workgroup to develop marketing materials.

5.0 Appendix A

The following As-Is Work flows describes the current process, it does not necessarily reflect what is contained in the CCC Operations Manual.

5.1.1 Acronyms

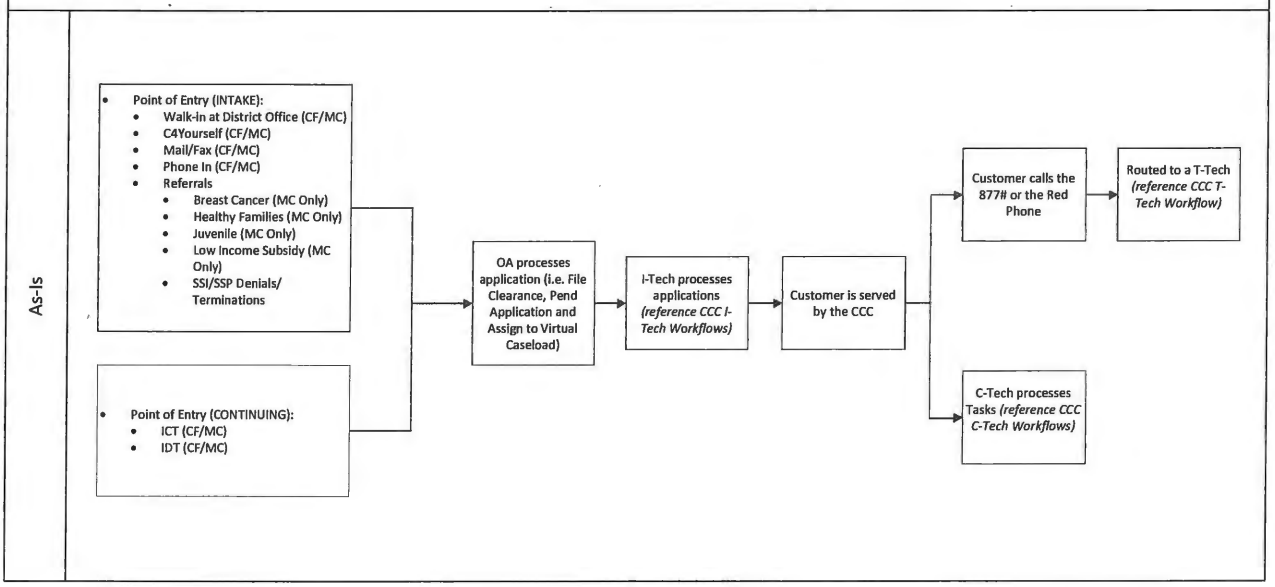
Acronym	Description
CCC	Customer Care Center
C-Tech	Continuing Eligibility Technician (CCC)
ESC	Eligibility Service Clerk
ES	Eligibility Supervisor
I-Tech	Intake Eligibility Technician (CCC)
Metro	Districts serviced by the CCC
Non-Metro	Districts not serviced by the CCC
OA	Office Assistant (also known as Clerical)
OA.1	There are different OAs that perform different functions notated as OA.1, OA.2, OA.CCC
	etc. This does not reflect their level.
OSS	Office Support Supervisor
T-Tech	Telephone Eligibility Technician (CCC)

5.1.2 As-Is CCC Business Model

CCC Business Model

VER	DESCRIPTION	DATE	BY
2.0	Initial Draft	07/11/12	FD

Notes:
- The CCC serves the following Metro District Offices: Jurupa, La Sierra and Moreno Valley.
- The CCC handles CF and MC Programs, both for Intake (non face to face applications) and Continuing Cases.
- The CCC has Virtual Caseloads.
- The CCC has T-Tech, C-Tech and I-Tech of which the T-Techs handles incoming calls. While the I-Techs are responsible to process non face to face applications and the C-Techs are responsible to process all Tasks.
- Due to limited resources, only Core Tasks are processed at the CCC.
- Core Tasks are considered QR7, MSR, RE and RECERTS, where Non-Core Tasks are considered all others.



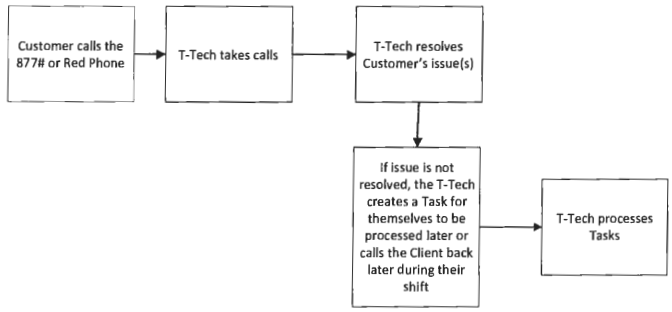
5.1.3 As-Is CCC Workflow T-Tech

CCC Workflow T-Tech

VER	DESCRIPTION	DATE	BY
1.0	Initial Draft	07/08/12	FD

Notes:
- The T-Tech spend 50% of their time on the phone, and spend the remaining time processing Core Tasks.

As-Is



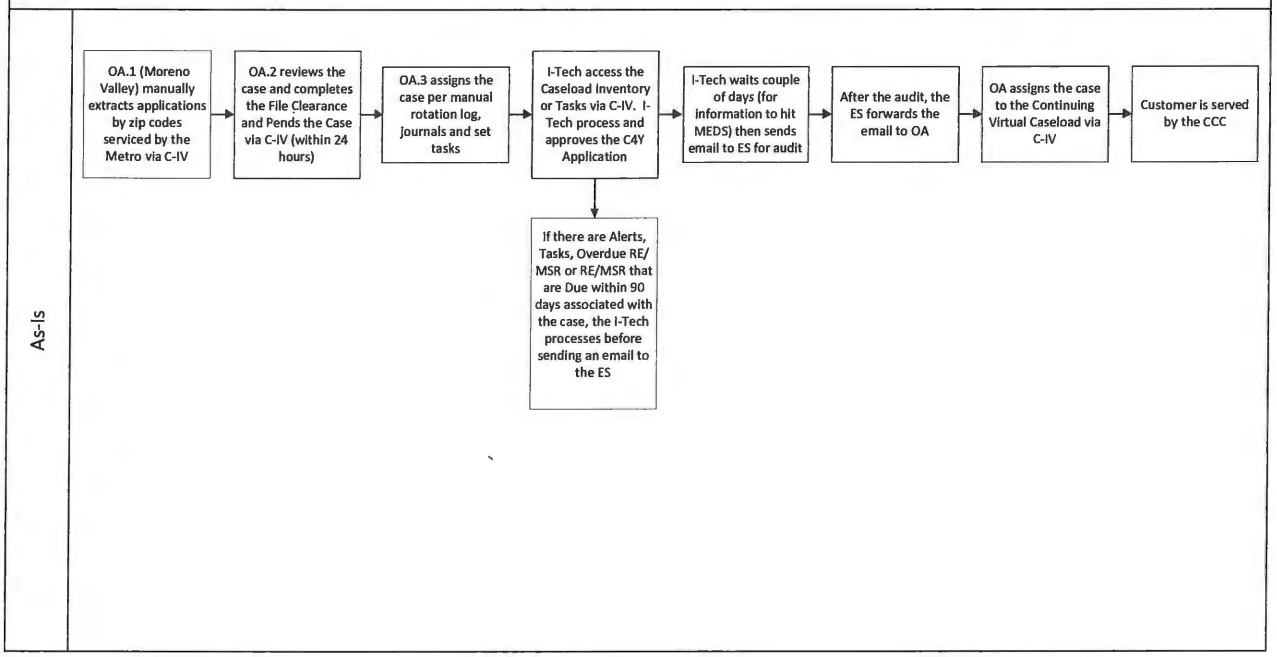
5.1.4 As-Is CCC Workflow I-Tech: C4Yourself

CCC Workflow I-Tech: C4Yourself

VER	DESCRIPTION	DATE	BY
1.0	Initial Draft	07/08/12	FD

Notes:

- The I-Tech processes all non face to face applications (i.e. C4Yourself, Healthy Families, Inter-County Transfer, Inter-District Transfer, Mail & Fax, Phone In, BCCTP Referrals, Low Income Subsidy Referrals, Juvenile Referrals, SSI/SSP Denials and Terminations Referrals)
- *If more information is needed, the I-Tech will call the customer.*



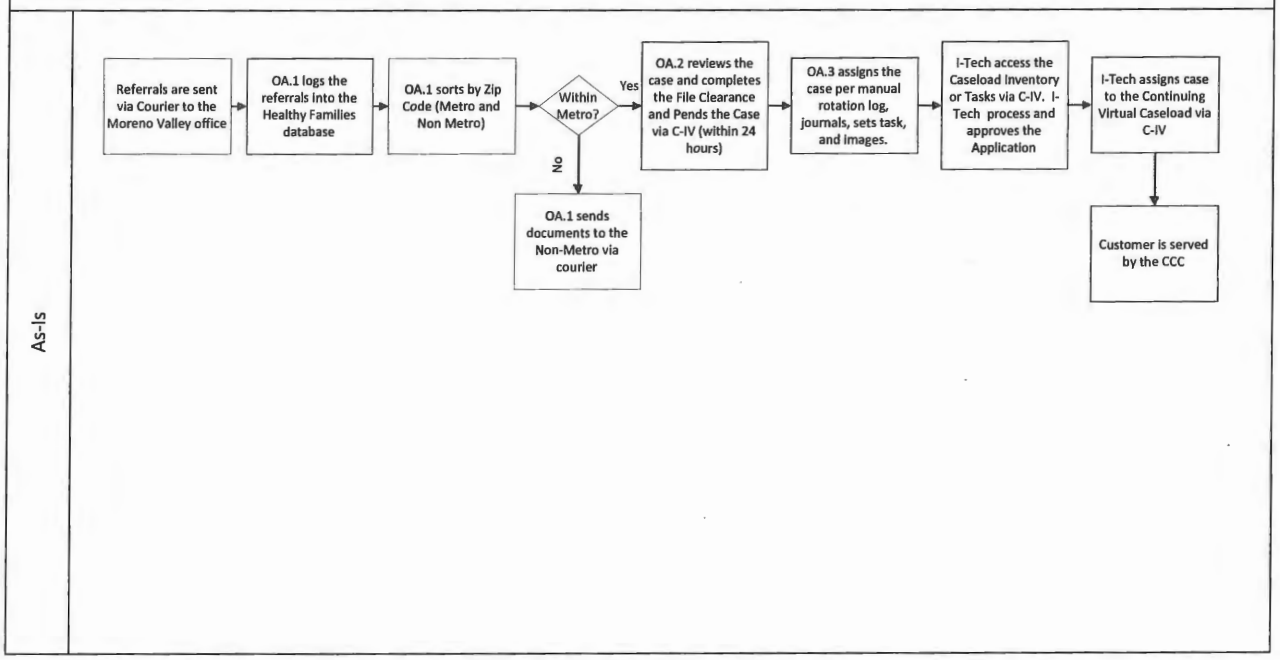
5.1.5 As-Is CCC Workflow I-Tech: Healthy Families (HF)

CCC Workflow I-Tech: Healthy Families (HF)

VER	DESCRIPTION	DATE	BY
1.0	Initial Draft	07/08/12	FD

Notes:

- The I-Tech process all non face to face applications (i.e. C4Yourself, Healthy Families, Inter-County Transfer, Inter-District Transfer, Mail & Fax, Phone In, BCCTP Referrals, Low Income Subsidy Referrals, Juvenile Referrals, SSI/SSP Denials and Terminations Referrals)
- *If more informatian is needed, the I-Tech will call the customer.*



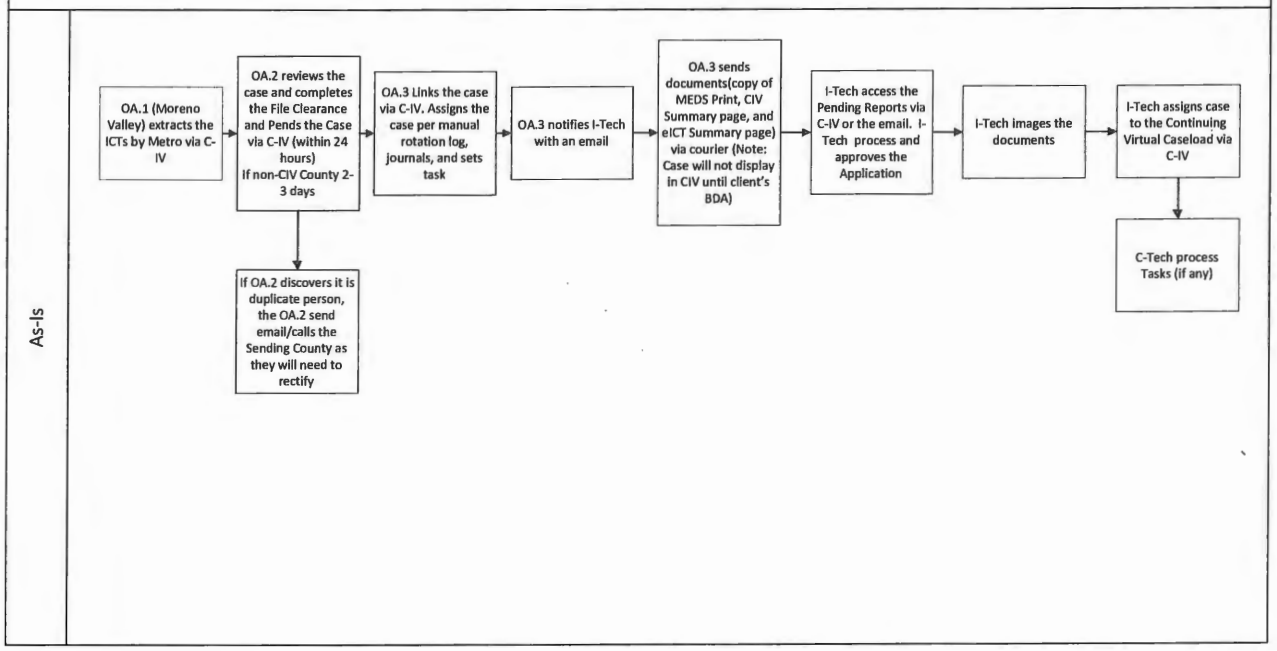
5.1.6 As-Is CCC Workflow I-Tech: Inter County Transfers (ICTs)

CCC Workflow I-Tech: Inter County Transfers (ICTs)

VER	DESCRIPTION	DATE	BY
1.0	Initial Draft	07/08/12	FD

Notes:

- The I-Tech process all non face to face applications (i.e. C4Yourself, Healthy Families, Inter-County Transfer, Inter-District Transfer, Mail & Fax, Phone In, BCCTP Referrals, Low Income Subsidy Referrals, Juvenile Referrals, SSI/SSP Denials and Terminations Referrals)
- *If more information is needed, the I-Tech will call the customer.*



5.1.7 As-Is CCC Workflow I-Tech: Inter District Transfers (IDTs)

CCC Workflow I-Tech: Inter-District Transfers (IDTs)

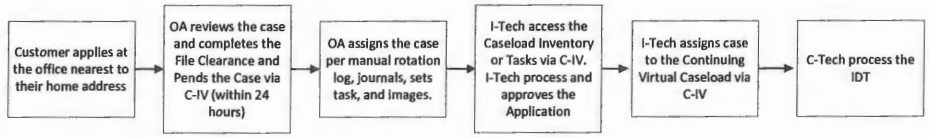
VER	DESCRIPTION	DATE	BY
1.0	Initial Draft	07/08/12	FD

Notes:

- The I-Tech process all non face to face applications (i.e. C4Yourself, Healthy Families, Inter-County Transfer, Inter-District Transfer, Mail & Fax, Phone In, BCCTP Referrals, Low Income Subsidy Referrals, Juvenile Referrals, SSI/SSP Denials and Terminations Referrals)

If more information is needed, the I-Tech will call the customer.

As-Is



5.1.8 As-Is CCC Workflow I-Tech: Mail and Fax

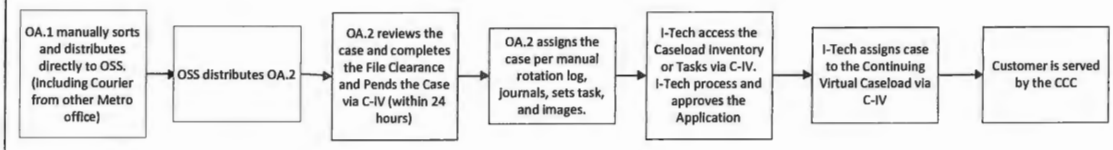
CCC Workflow I-Tech: Mail and Fax

VER	DESCRIPTION	DATE	BY
1.0	Initial Draft	07/08/12	FD

Notes:

- The I-Tech process all non face to face applications (i.e. C4Yourself, Healthy Families, Inter-County Transfer, Inter-District Transfer, Mail & Fax, Phone In, BCCTP Referrals, Low Income Subsidy Referrals, Juvenile Referrals, SSI/SSP Denials and Terminations Referrals)
- *If more information is needed, the I-Tech will call the customer.*

As-Is



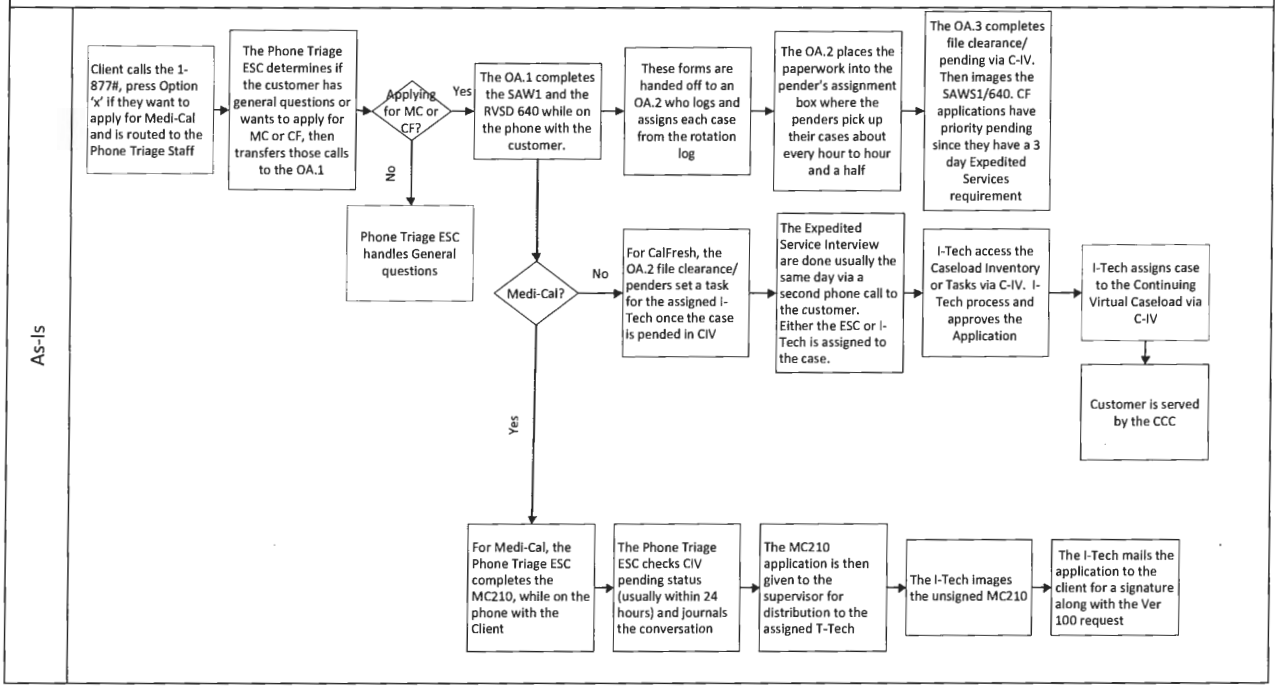
5.1.9 As-Is CCC Workflow I-Tech: Phone In

CCC Workflow I-Tech: Phone In

VER	DESCRIPTION	DATE	BY
1.0	Initial Draft	07/08/12	FD

Notes:

- The I-Tech process all non face to face applications (i.e. C4Yourself, Healthy Families, Inter-County Transfer, Inter-District Transfer, Mail & Fax, Phone In, BCCTP Referrals, Low Income Subsidy Referrals, Juvenile Referrals, SSI/SSP Denials and Terminations Referrals)
- *If more information is needed, the I-Tech will call the customer.*



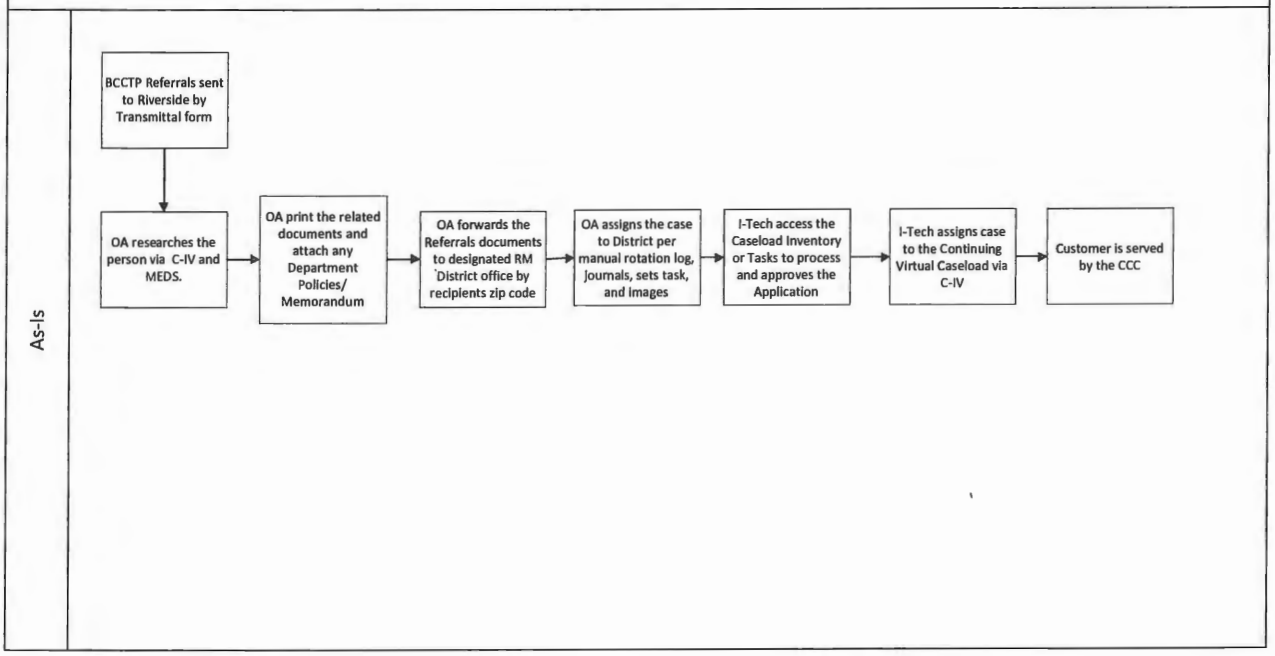
5.1.10 As-Is CCC Workflow I-Tech: Referrals Breast Cancer

CCC Workflow I-Tech: Referrals Breast Cancer

VER	DESCRIPTION	DATE	BY
1.0	Initial Draft	07/08/12	FD

Notes:

- The I-Tech process all non face to face applications (i.e. C4Yourself, Healthy Families, Inter-County Transfer, Inter-District Transfer, Mail & Fax, Phone In, BCCTP Referrals, Low Income Subsidy Referrals, Juvenile Referrals, SSI/SSP Denials and Terminations Referrals)
- *If more Information is needed, the I-Tech will call the customer.*



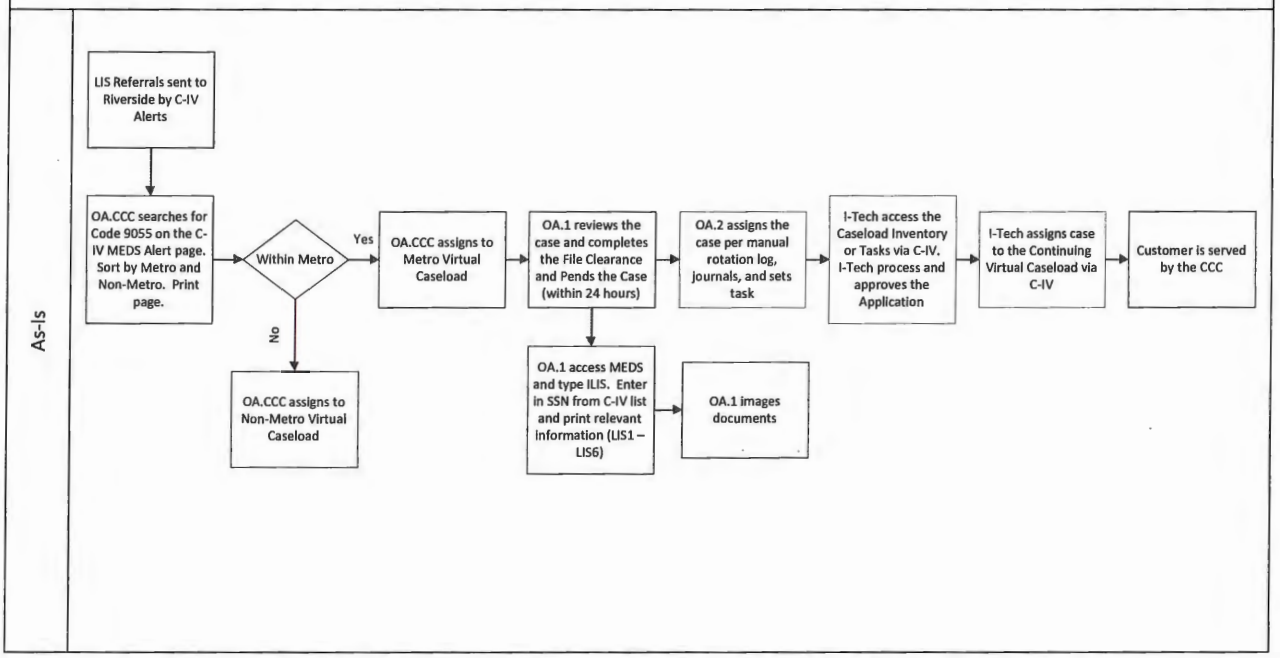
5.1.11 As-Is CCC Workflow I-Tech: Referrals Low Income Subsidy

CCC Workflow I-Tech: Referrals Low Income Subsidy

REV	DESCRIPTION	DATE	BY
1.0	Initial Draft	07/08/12	FD

Notes:

- The I-Tech process all non face to face applications (i.e. C4Yourself, Healthy Families, Inter-County Transfer, Inter-District Transfer, Mail & Fax, Phone In, BCCTP Referrals, Low Income Subsidy Referrals, Juvenile Referrals, SSI/SSP Denials and Terminations Referrals)
- *If more information is needed, the I-Tech will call the customer.*



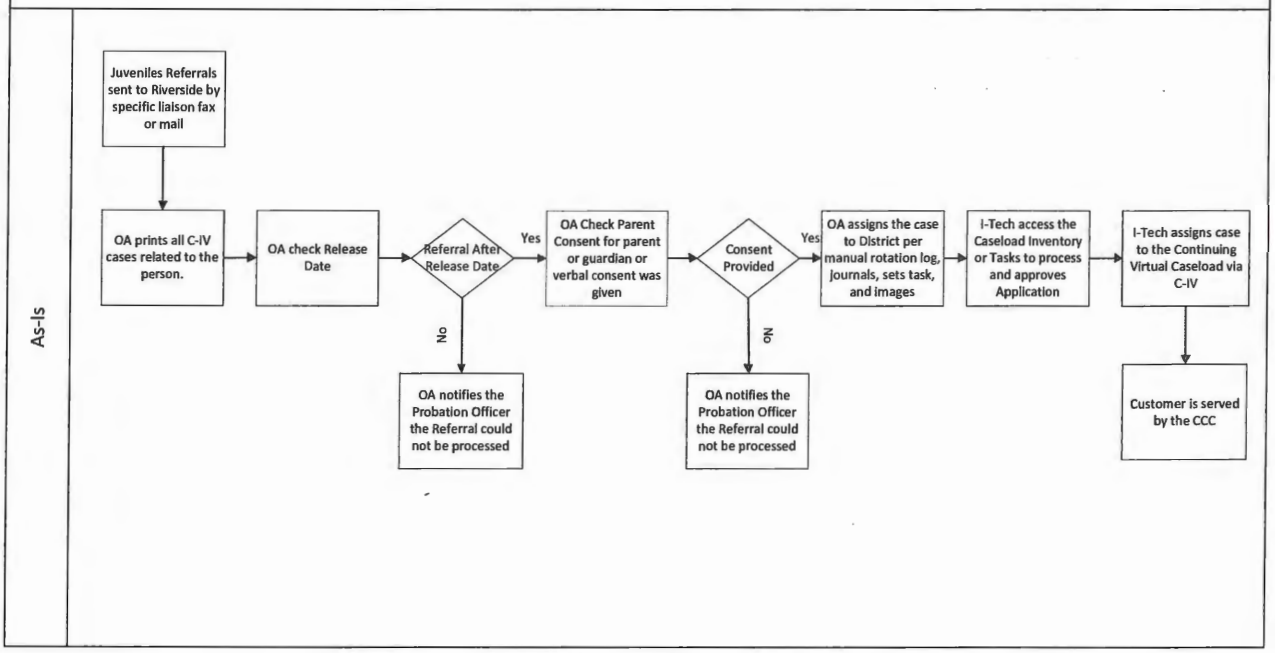
5.1.12 As-Is CCC Workflow I-Tech: Referrals Juvenile

CCC Workflow I-Tech: Referrals Juveniles

VER	DESCRIPTION	DATE	BY
1.0	Initial Draft	07/08/12	FD

Notes:

- The I-Tech process all non face to face applications (i.e. C4Yourself, Healthy Families, Inter-County Transfer, Inter-District Transfer, Mail & Fax, Phone In, BCCTP Referrals, Low Income Subsidy Referrals, Juvenile Referrals, SSI/SSP Denials and Terminations Referrals)
- *If more information is needed, the I-Tech will call the customer.*



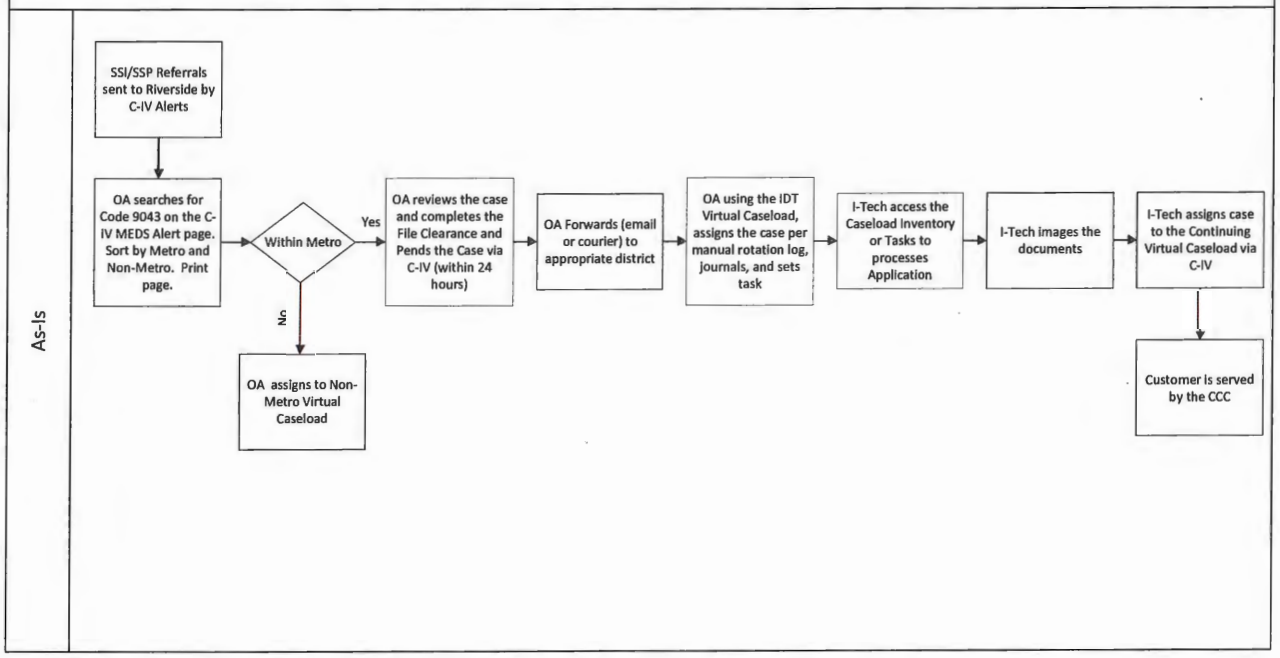
5.1.13 As-Is CCC Workflow I-Tech: Referrals SSI/SSP Denials and Terminations

CCC Workflow I-Tech: Referrals SSI/SSP Denials and Terminations Due to Excess Income

VER	DESCRIPTION	DATE	BY
1.0	Initial Draft	07/08/12	FD

Notes:

- The I-Tech process all non face to face applications (i.e. C4Yourself, Healthy Families, Inter-County Transfer, Inter-District Transfer, Mail & Fax, Phone In, BCCTP Referrals, Low Income Subsidy Referrals, Juvenile Referrals, SSI/SSP Denials and Terminations Referrals)
- *If more information is needed, the I-Tech will call the customer.*



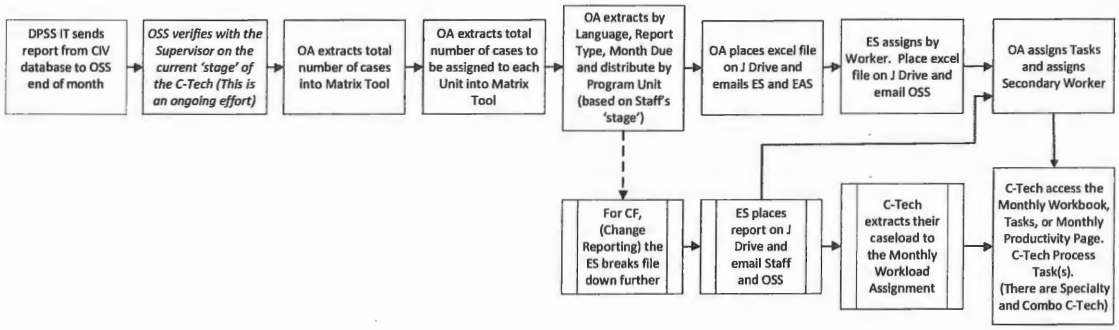
5.1.14 As-Is CCC Workflow C-Tech

CCC Workflow C-Tech

VER	DESCRIPTION	DATE	BY
2.0	Initial Draft	07/11/12	FD

Notes:
- The C-Techs are responsible to process all Tasks.
- Due to limited resources, only Core Tasks are processed at the CCC.
- Core Tasks are considered QR7, MSR, RE and RECERTS, where Non-Core Tasks are considered all others.
- The Core Tasks are assigned on a monthly basis via the Monthly Workbook spreadsheet. At the end of the month the C-Tech prints a listing of tasks that were not completed and shares with Supervisors. The Supervisors submits a Monthly report to the Regional Manager. (Some Supervisors spot check to verify the Core Task has been completed.
- The C-Tech have Specialty Staff and Combo Staff.

As-Is

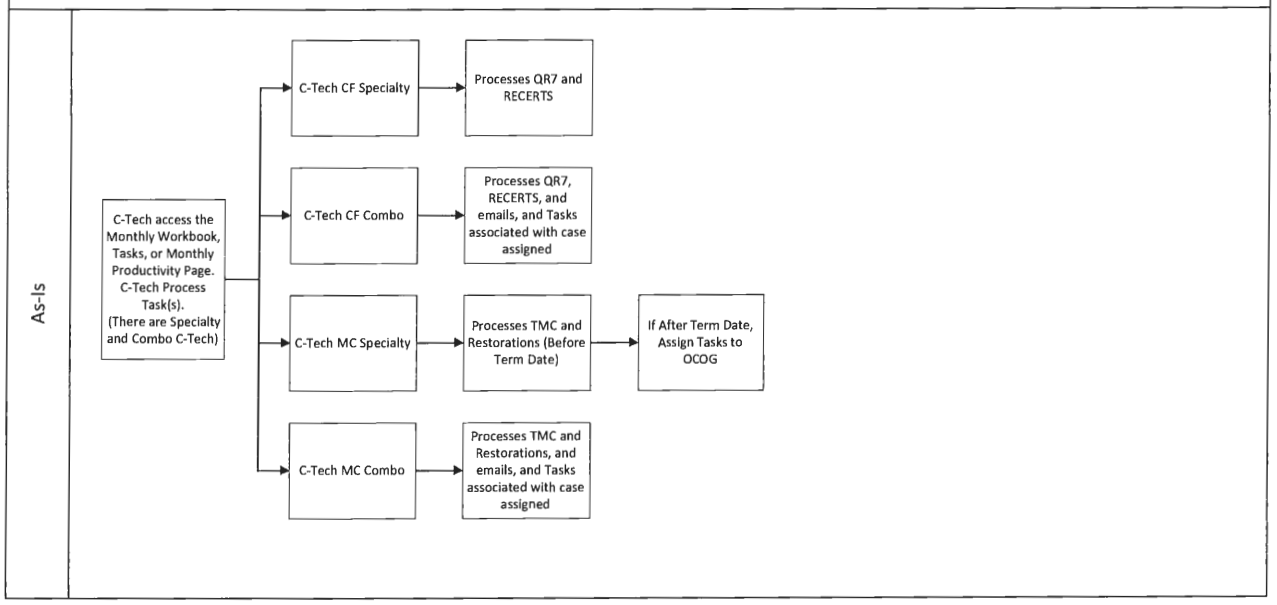


5.1.15 As-Is CCC Workflow C-Tech: Specialty and Combo

CCC Workflow C-Tech: Specialty and Combo

VER	DESCRIPTION	DATE	BY
2.0	Initial Draft	07/11/12	FD

Notes:
- The C-Techs are responsible to process all Tasks.
- Due to limited resources, only Core Tasks are processed at the CCC.
- Core Tasks are considered QR7, MSR, RE and RECERTS, where Non-Core Tasks are considered all others.
- The Core Tasks are assigned on a monthly basis via the Monthly Workbook spreadsheet. At the end of the month the C-Tech prints a listing of tasks that were not completed and shares with Supervisors. The Supervisors submits a Monthly report to the Regional Manager. (Some Supervisors spot check to verify the Core Task has been completed.
- The C-Tech have Specialty Staff and Combo Staff.



Appendix 10

California Child Support Automation System (CCSAS)
State Disbursement Unit (SDU)

SDU SECURITY PLAN
CDL OM 006

Version 2.1
P-00015-2.1-080505
August 5, 2005

Prepared By:
California Child Support Service Provider (CCSSP)

LIST OF REVISIONS

Version	Date	Description
1.0	June 7, 2005	Initial Draft Submission to State
1.1	June 28, 2005	Incorporated State Comments
1.2	July 5, 2005	Incorporated approximately 50% of actions from State review on 6/29/05. The rest of the actions will be incorporated after Draft 2 of the OM 006 is received back from the State.
2.0	July 25, 2005	Incorporated all updates, modifications and actions as a result of most recent State comments.
2.1	August 5, 2005	Modifications to Section 10 and addition of appendices M and N

SIGNOFF

The SDU Security Plan document has been reviewed and found in accordance with the requirements listed under Exhibit 6A of the Request for Proposal.

Signature	Name	Date

TABLE OF CONTENTS

LIST OF REVISIONS 2
SIGNOFF 3
TABLE OF CONTENTS 4
LIST OF FIGURES 10
LIST OF TABLES 11
1.0 INTRODUCTION 12
1.1 OVERVIEW 12
1.2 SCOPE 12
1.3 INTENDED AUDIENCE 12
1.4 REVISION CONTROL 12
1.5 INFORMATION SECURITY 12
1.5.1 What is Information Security? 12
1.6 SECURITY PROGRAM 13
1.6.1 Information Security Plan 13
1.6.2 Information Security Procedures 13
1.6.3 Disaster Recovery and Business Continuity 15
1.6.5 Human Resource Policies 15
1.7 PROTECTION OF CONFIDENTIAL INFORMATION 15
1.8 REFERENCED DOCUMENTS 15
2.0 ROLES & RESPONSIBILITIES 16
2.1 OVERVIEW 16
2.2 SECURITY MANAGEMENT 17
Senior Management 17
Information Security Officer (ISO) 18
Information Security Administrators and Analysts 19
Systems Administrators 19
Managers of System Users 20
Application Security Management 20
Physical Security management 20
System Users 20
3.0 SECURITY PROCESSES AND PROCEDURES 22
3.1 OVERVIEW 22
3.2 PROCESS AND PROCEDURES 22
3.3 COLLECTIONS 22
Standard Microsoft and CE Application Security 23
Handling of Cash 23
Security in Intelligent Data Capture (IDC) 24
Security in Exceptions Processing 25
Security in Archive Research 28
3.3.1 Suspicious Mail Handling 29
Process for Identifying suspicious mail 29
Process for Handling suspicious mail 29

3.4 DISBURSEMENTS 29
3.5 PRINTING 30
System Monitoring Procedures: *30*
Account Change Authority: *30*
Account Change Request: *31*
Review of User Access Rights Procedures: *31*

4.0 ASSET CLASSIFICATION AND CONTROL 32

4.1 OVERVIEW 32
4.2 CRITERIA FOR DETERMINING SENSITIVITY 32
4.3 INFORMATION CLASSIFICATION GUIDELINES 32
4.4 CLASSIFICATION AND CONTROL OF INTERNAL REVENUE SERVICE (IRS) INFORMATION 32
4.5 DATA OWNERSHIP 33
4.6 INFORMATION CLASSIFICATION AND ROLE BASED ACCESS 33
4.7 INFORMATION SENSITIVITY LEVELS 33
4.8 CONFIDENTIALITY CLASSIFICATIONS 34
4.9 INFORMATION LABELING AND HANDLING 35
4.9.1 Information Distribution *36*
4.9.2 Data Retention Requirements *37*
4.9.3 Additional Data Retention Requirements *38*
4.10 ADDITIONAL REQUIREMENTS FOR INFORMATION LABELING AND HANDLING 39
4.10.1 Media Identification Labels *39*
4.10.2 Overwriting and Degaussing *39*
4.10.3 Clearing and Purging Methods *39*
4.10.4 Destruction Methods *40*

5.0 PERSONNEL SECURITY 41

5.1 OVERVIEW 41
5.2 PERSONNEL SCREENING 41
5.2.1 Confidentiality Agreements *41*
5.2.2 Terms and Conditions of Employment *42*
5.3 ENFORCEMENT OF UNAUTHORIZED USE OF INFORMATION SYSTEMS 43
5.4 INFORMATION SECURITY EDUCATION AND TRAINING 43
5.4.1 Security Awareness Program *44*
5.5 SEGREGATION OF DUTIES 44
5.6 EMPLOYEE TERMINATION 45

6.0 PHYSICAL AND ENVIRONMENTAL SECURITY 46

6.1 OVERVIEW 46
6.2 CONTROLLED ACCESS 46
6.3 PHYSICAL ACCESS CONTROLS 46
6.3.1 Intrusion Alarm Systems *46*
6.3.2 Closed Circuit Television Monitoring *46*
6.3.4 Access on a Need-to-Know Basis *47*
6.3.5 Badge Program *47*
6.3.6 Locks and Storage *47*
6.3.7 Isolated Delivery and Loading Areas *48*
6.3.8 Facilities Access *48*
6.3.9 Visitor Access *49*
6.3.10 Data Center Access *49*
6.3.11 Access Log *50*

6.3.12 Restrictions on Signage and Perimeter Controls *50*
6.3.13 Auditing Physical Security *51*
6.4 FLOOR PLANS 51
6.5 PROTECTION OF EQUIPMENT 51
6.6 CONTRACT CLEANING SERVICES 52
6.7 ELECTRONIC SECURITY / PHYSICAL SECURITY FOR SACRAMENTO FACILITY 52
6.7.1 Secure Areas: *52*
6.7.2 ADA (by revolving door) & Emergency Exit Doors *52*
6.7.3 Main Entry (location to receive visitors) *53*
6.7.4 Safe Room (room used for the storage of cash, checks or other notes of financial value) *53*
6.7.5 Areas Controlled By Card Reader Access *53*
6.7.6 Additional Security Controls *53*
6.7.7 Electrical / LAN / Phone / Fire Alarm Interface Requirements *53*
6.7.8 Access Control Panel / Lock-Aux Power Supply (each panel controls up to 16 doors) *54*
6.7.9 Radionics Control / Communicator *54*
6.7.10 70" Vertical Rack (19" Equipment Rack) (if provided by security contractor will be Winsted V8801 allows 40RU) *54*
6.7.11 Digital Video Recorders / Extended Storage Module (each supports up to 16 cameras) *54*
6.7.12 19" Computer Monitor/Mouse & Keyboard (supports all Digital Video Recorders through use of KVM) *54*
6.7.13 KVM Switch (used to switch between computers on one monitor keyboard and mouse) *55*
6.7.14 Central Camera Power Supply (for interior cameras each supports up to 16 cameras) *55*
6.7.15 Camera Power Supply (for exterior camera supports 1 camera each) *55*
6.7.16 CCTV 14" Monitor (for viewing dock camera) *55*
6.7.17 Intercom System Door Station & Master (option to use PBX phone) *55*
6.7.18 Approved Lock Hardware *55*

7.0 COMMUNICATIONS SECURITY 57

7.1 OVERVIEW 57
7.2 EXCHANGE OF INFORMATION 57
7.2.1 Security of Physical Media in Transit *57*
7.2.2 Security of Data Transmissions *57*
7.2.3 Communications Encryption Requirements *59*
7.2.4 Electronic Commerce Security *59*
7.3 SECURITY OF ELECTRONIC MAIL AND MESSAGING 61
7.3.1 Electronic Mail Hosting Requirements *61*
7.3.2 Electronic Mail User Requirements *62*
7.3.3 Security Requirements for Messaging and Web Conferencing Systems *62*
7.4 CRYPTOGRAPHIC CONTROLS 63
7.4.1 Use of Cryptographic Controls *63*
7.4.2 Digital Signatures *63*
7.5 PROTECTION AGAINST MALICIOUS SOFTWARE 67
7.5.1 Controls Against Malicious Software *68*
7.6 HHSDC COMMUNICATIONS 69
7.7 ACCESSNET SECURE FILE TRANSFER 69
7.8 TELECOMMUNICATIONS CONTROLS 69
7.8.1 Remote Diagnostic Port Protection *70*
7.8.2 Use of Analog and Digital Subscriber Lines *70*
7.8.3 Private Branch Exchange (PBX) Policy *70*

8.0 ACCESS CONTROL 72

8.1 OVERVIEW 72

8.2 LOGON BANNER/SCREEN WARNING BANNER 72
8.3 ROLE BASED ACCESS CONTROLS (RBAC) 72
8.3.1 Configuration Management Overview *73*
8.4 USER IDENTIFICATION AND AUTHENTICATION 74
8.5 NETWORK ACCESS CONTROL 74
8.5.1 Segregation of Networks *74*
8.5.2 Network Routing Control (Gateways) *75*
8.5.3 Sensitive Information System Separation *75*
8.5.4 AccessNet Environment *76*
8.6 USE OF SYSTEM UTILITIES 76
8.7 LIMITATION OF CONNECTION TIME 76
8.8 USER ENROLLMENT AND REGISTRATION 77
8.8.1 User De-Registration *77*
8.9 PRIVILEGE MANAGEMENT 77
8.10 GROUP ACCOUNTS 78
8.11 PASSWORDS 78
8.11.1 Password Policy *78*
8.11.2 Group Account/Password Prohibition *79*
8.11.3 Account Locking *79*
8.11.4 Password Management System *79*
8.12 UNATTENDED USER EQUIPMENT 80
8.12.1 Screen Savers and Workstation Lockout *80*
8.13 MOBILE COMPUTING AND REMOTE ACCESS 80
8.13.1 Use of Privately Owned Mobile Computing Devices *81*
8.13.2 Centralized Monitoring for Mobile Computing Devices *81*
8.13.3 Remote Access *81*
8.14 GATEWAYS AND FIREWALLS 83
8.15 OPERATING SYSTEM HARDENING 84
8.16 MASTER FILE PROTECTION 84
8.16.1 AccessNet Environment *84*
8.17 INFORMATION STORAGE DEVICES 85
9.0 MONITORING SYSTEM ACCESS AND USE 86
9.1 OVERVIEW 86
9.2 INTRUSION DETECTION REQUIREMENTS 86
9.3 AUDIT TRAIL REQUIREMENTS 87
9.3.1 Collections Audit Log *88*
9.3.2 Disbursements Audit Log *88*
9.3.3 Systems Logging Review *88*
9.3.4 Monitoring Procedures and Areas of Risk *89*
9.3.5 Review of User Access Rights *89*
9.4 IMPLEMENTED CONTROLS FOR AUDIT TRAILS 90
9.4.1 AccessNet Environment *90*
9.4.2 Collections Environment *91*
9.4.3 Disbursements Environment *92*
9.4.4 Onyx Ticketing Environment *92*
10.0 INCIDENT MANAGEMENT 93
10.1 OVERVIEW 93
10.2 INCIDENT DEFINITION 93

10.2.1 Personal Information *93*
10.3 INCIDENT NOTIFICATION 94
10.3.1 Reporting of Incidents *94*
10.3.2 Isolation of Incidents *95*
10.4 INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURES 95
10.4.1 Identification/Prioritization *96*
10.4.2 Initial Impact Analysis *96*
10.4.3 Containment *97*
10.4.4 Eradication *97*
10.4.5 Recovery *97*
10.4.6 Damage Analysis *97*
10.4.7 Post Event Impact Analysis *97*
10.4.8 Lessons-Learned Analysis *97*
10.5 REPORTING SECURITY WEAKNESSES 98
10.5.1 Reporting Software Malfunctions *99*
10.5.2 Learning from Incidents *99*
10.6 NON-INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURES 99
10.6.1 Determining if a Violation has Occurred, and the Severity of the Violation *100*
10.6.2 Disciplinary Process *101*
11.0 DISASTER RECOVERY & BUSINESS CONTINUITY 102
11.1 OVERVIEW 102
11.2 DATA STORAGE AND BACKUP METHODOLOGIES 102
11.3 SECURITY INFRASTRUCTURE 103
11.4 MEDIA PROTECTION 103
12.0 EXTERNAL DEPENDENCIES 104
13.0 THIRD PARTY SECURITY 105
13.1 OVERVIEW 105
13.2 IDENTIFICATION OF RISKS FROM THIRD PARTY ACCESS 105
13.3 SECURITY REQUIREMENTS FOR THIRD PARTY ACCESS 105
13.3.1 Types of Access *106*
13.3.2 On-site Contractors and Temporary Employees *106*
13.4 SECURITY REQUIREMENTS FOR THIRD PARTY AND OUTSOURCING CONTRACTS 106
14.0 OPERATIONS MANAGEMENT 108
14.1 OVERVIEW 108
14.2 DEPLOYMENT AND CONFIGURATION MANAGEMENT 108
14.2.1 Change Control *108*
15.0 COMPLIANCE 110
15.1 OVERVIEW 110
15.2 SECURITY POLICY ENFORCEMENT 110
15.2.1 Technical Audit Requirements *110*
15.3 SANCTIONS FOR NON-COMPLIANCE 111
APPENDIX A – CONTACT LISTS 112
SDU CONTACT LIST 112
CCSAS CONTACT LIST 113

SP VENDOR CONTACTS 115
APPENDIX B - DIAGRAMS 117
APPENDIX C – GLOSSARY OF TERMS 120
A 120
B 120
C 121
D 123
E 125
F 125
G 126
H 126
I 127
K 129
L 129
M 129
N 130
O 130
P 131
R 132
S 133
T 135
U 136
V 136
W 137
APPENDIX D – TRAINING MATRIX 138
APPENDIX E – CERTIFICATE OF INSURANCE 139
APPENDIX F – ACCOUNTABILITY 140
APPENDIX G – CONFIDENTIALITY 142
APPENDIX H – ENCRYPTION REQUIREMENTS 146
APPENDIX I – VISITOR ACCESS LOG 147
APPENDIX J – CA SDU USER MANAGEMENT PROCEDURES 148
APPENDIX K – NOTICE OF SECURITY BREACHES 161
APPENDIX L – SECURITY EVENT FORM 163
APPENDIX M – INCIDENT REPORT 166
APPENDIX N – COMPUTER SECURITY THREAT LEVELS 169

LIST OF FIGURES

FIGURE 2.1: SECURITY HIERARCHY 17
FIGURE 3.1: CASH CONTROL LOG 24
FIGURE 3.2: USER ADMINISTRATION SCREEN 26
FIGURE 3.3: USER FUNCTIONAL SECURITY ADMINISTRATION SCREEN 27
FIGURE 8.1: LOGON BANNER/SCREEN WARNING BANNER 72
FIGURE 9.1: ACCESSNET LOG VIEWER SCREEN 91
FIGURE B.1: CASDU WAN 117
FIGURE B.2: CASDU HIGH-LEVEL NETWORK 118
FIGURE B.3: CASDU – LAN/WAN CONNECTIVITY 119
FIGURE D.1: TRAINING MATRIX 138
FIGURE E.1: PROOF OF BONDING 139
FIGURE F.1: EMPLOYEE ACCOUNTABILITY FORM 141
FIGURE G.1: CONFIDENTIALITY STATEMENT 145
FIGURE I1: VISITOR ACCESS LOG 147
FIGURE L.1: SECURITY EVENT FORM 165

LIST OF TABLES

TABLE 4.1: INFORMATION SECURITY LEVELS 34
TABLE 4.2: CONFIDENTIALITY CLASSIFICATIONS 35
TABLE 4.3: INFORMATION LABELING AND HANDLING 36
TABLE 4.4: INFORMATION DISTRIBUTION 37
TABLE 4.5: DATA RETENTION REQUIREMENTS 38
TABLE 7.1: COMMUNICATIONS ENCRYPTION MATRIX 59
TABLE 9.1: INTRUSION CLASSIFICATIONS 87
TABLE 9.2: LOG REVIEW SCHEDULE 89
TABLE 10.2: GENERAL INCIDENT REPORTING PROCEDURES 96
TABLE 10.3: THREAT LEVEL RESPONSE TIMES FOR IT INCIDENTS 96
TABLE 10.4: CLASSIFICATION OF SEVERITY LEVELS FOR NON IT INCIDENTS 100
TABLE 10.5: THREAT LEVEL RESPONSE TIMES FOR NON IT INCIDENTS 101
TABLE 12.1: SECURITY RELATED TOUCH POINTS 104
TABLE 15.1: TECHNICAL AUDIT FREQUENCY 111
TABLE A.1: SDU CONTACT LIST 113
TABLE A.2: CCSAS CONTACT LIST 114
TABLE A.3: SP VENDOR CONTACTS 116
TABLE J-1 – SYSTEM USER TYPES 149

1.0 INTRODUCTION

1.1 OVERVIEW

The California Department of Child Support Services State Disbursement Unit (SDU) requires that its assets be protected from unauthorized disclosure, theft, and environmental hazards. In addition, the integrity, confidentiality, and availability of all information must be ensured to a level commensurate with the level of protection required for sensitive State and Federal protected information. This Security Plan details all security controls that are in place or planned that protect all assets in accordance with State requirements and security best practices.

This Security Plan encompasses a multitude of other documents relating to physical security, logical security, general SDU operations, technical architecture, disaster recovery and business continuity. References to separate documents exist throughout the Security Plan and such documents will be made available as requested (or as soon as they are completed). All documents are to be considered living documents that must be continually updated, correlated back to the Security Plan and controlled under configuration management.

This Security Plan encompasses both Version 1 and Version 2 activities. A glossary of terms has been included in Appendix C.

1.2 SCOPE

The scope of this Security plan is limited to the State of California SDU and the security controls applied by the Service Provider (SP) and authorized third parties. All documentation contained herein is applicable only to information, services, facilities, and third party providers of the State of California Department of Child Support Services State Disbursement Unit.

1.3 INTENDED AUDIENCE

The intended audience for this document is the California Department of Child Support Services (DCSS), the SP staff, and all applicable third parties.

1.4 REVISION CONTROL

This Plan will become effective upon approval by the State of California and will be reviewed annually by the SP Information Security Organization to determine its effectiveness. Upon State approval, versioning of this document will be strictly managed under Configuration Management controls. This document will be resubmitted to the State every 6 months following first submission on the 10th of the month if any changes have been made. All revisions to this document require prior authorization and must occur as significant modifications occur that affect the security of the environment.

In addition, the Service Provider utilizes independent review as a means to preserve and sustain system and program integrity. As a part of this annual independent audit of the SDU as a whole, all security related policies and procedures will be examined.

1.5 INFORMATION SECURITY

1.5.1 WHAT IS INFORMATION SECURITY?

Information is a significant form of assets, which like other important business assets, has value to an organization and consequently needs to be suitably protected. Information Security protects

information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it will always be appropriately protected.

Information Security is characterized as the preservation of:

- **Confidentiality**: Ensuring that information is accessible only to those authorized to have access;
- **Integrity**: Safeguarding the accuracy and completeness of information and processing methods;
- **Availability**: Ensuring that authorized users have access to information and associated assets when required.

Information Security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

Information and information systems are obvious valuable assets to any business or government agency. There is a reliance on information and information systems to maintain and advance that particular organization's competitive edge. Security is an essential component for enhancing consumer confidence by ensuring that electronic commerce and supporting operations are held to high standards for integrity, confidentiality, and availability.

As a representative of the DCSS, the SP will strive to protect its people, information assets, information systems, customers, and clients from unauthorized access. A secure environment provides customers with assurance that all assets are protected against unauthorized access and natural threats that could result in the loss of information, confidentiality or integrity of all information assets.

1.6 Security Program

The State of California State Disbursement Unit security program is comprised of several separate components of documentation. The collection of documents encompasses the rules of behavior, implementation, and management of information and physical security that makes up the overall security program for a specified entity. The security program consists of the following documents:

1.6.1 Information Security Plan

Security Planning is a process by which the information system, subject to policies and standards, is verified compliant in its implementation and operation. This is normally conducted by means of using a template questionnaire that follows policy and standards and includes the following components:

- Data/Asset Classification
- Risk Assessment and Mitigation
- Vulnerability and Threat Assessment
- Logical Network and Data Flow Diagrams
- Laws and Regulations Compliance
- Authorization to Process
- Certification

1.6.2 Information Security Procedures

Detailed documentation describing policy implementation details by means of a step-by-step process required in routine and specialized activities.

1.6.3 Disaster Recovery and Business Continuity

Standards and procedures related to the resumption of business operations during disaster or failure. The Disaster Recovery Plan, CDL OM005 and the Business Continuity Plan, CDL OM009 will go into details specific to the information system and its readiness for disaster or failure.

1.6.5 Human Resource Policies

Human Resource Policies relate to employees only. Policies usually include those concerning hiring, firing, investigations, and code of conduct.

1.7 Protection of Confidential Information

Confidential information is kept confidential by means of adherence to the security program that encompasses all policies, regulations, processes and procedures that in combination ensure proper protection of sensitive and confidential information. This is done by ensuring that information is identified, classified, controlled and associated with a protected information system that ensures accountability for storage, transmission and processing of all protected information.

1.8 Referenced Documents

This deliverable relies on or references the following documents:

- CCSAS CSE Retention Control Document (CDL TM089)
- SDU Disaster Recovery Plan for SDU Services(CDL OM 005)
- SDU Business Continuity Plan for SDU Services(CDL OM 009)
- SDU Operations Management Plan (CDL OM 001)
- SDU Configuration Management Plan
- SDU Collections Procedures - Version 1&2 (CDL CO 001-1&2)
- SDU Disbursement Procedures – Version 1&2 (CDL DB 001-1&2)
- SDU Incident Response Procedures (internal)
- Internal Revenue Manual (IRM) Sect. 25.10.1

2.0 ROLES & RESPONSIBILITIES

2.1 OVERVIEW

Organizational entities are identified and defined as representative groups or roles within the SP operation. Each role is unique in function and maintains high level responsibilities for subordinate roles to ensure that tasks are carried out effectively and enforces segregation of duties. Each role is assigned specific responsibilities relating to the protection of physical and logical assets.

The Information Security Group (InfoSec) implements the Information Security Program for the SP. Each SP business unit has an assigned Information Security Officer (ISO) responsible for the security of the SDU operation as a whole. These management personnel are primarily responsible for setting the Information Security posture, leadership, and providing advisory services for the SDU operation.

The responsibilities and accountability of owners, providers, and users of SP information systems and other parties concerned with the security of computer systems should be explicit. The assignment of responsibilities may extend across organizational boundaries.

As it pertains to ongoing reviews and lessons learned, the SP's security policies and this Security Plan are always being evaluated and updated to match the needs of the SDU operation. As part of the OM 007 - SDU Security Assessment Report effort, the SP ISO is responsible for not only authoring the report, but also to ensure that assessment results and lessons learned are reflected in both SP security polices and the OM 006 - SDU Security Plan. In addition, and as defined in the OM 008 - Problem Resolution Plan, the SP utilizes a structured approach to identifying, managing and resolving problems, which include problems pertaining to security.

Figure 2.1 describes the SP's high-level hierarchy as it pertains to the management of security documentation, security processes, and the resolution of breeched security issues:

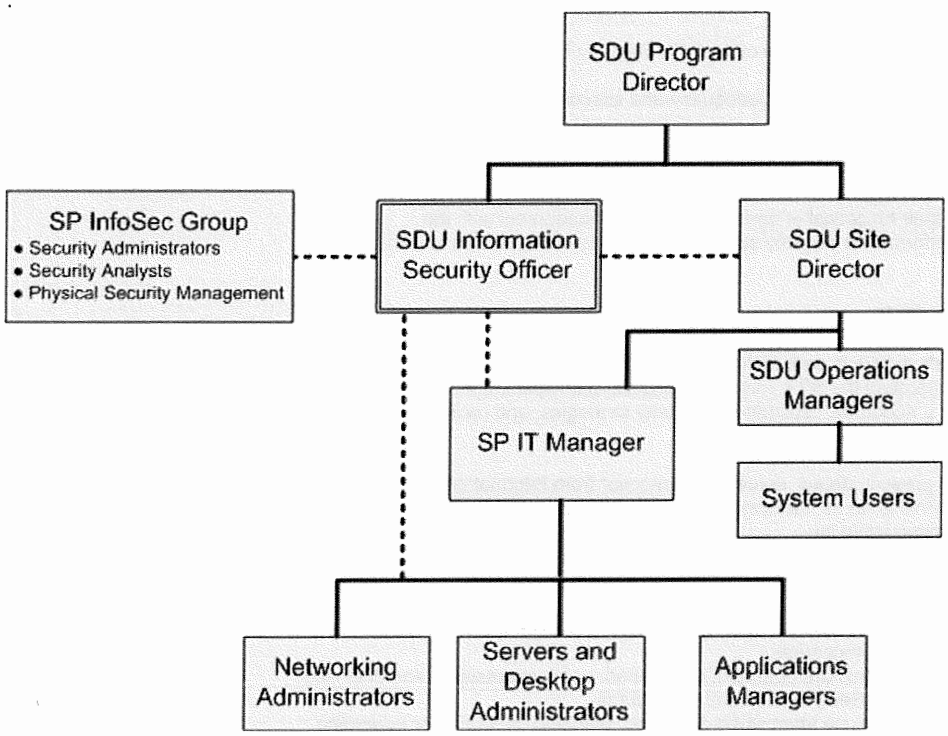


Figure 2.1: Security Hierarchy

2.2 Security Management

Security must be applied at the management level of the SDU operation. Thus, the SP will integrate the following responsibilities into our management structure:

- Security assessment, review, and enforcement
- Designation or appointment of an Information Security Officer (ISO)
- Assignment of Information Security roles and responsibilities
- Coordinate security implementation and consult in project design
- Develop and maintain Security Plan and standards of operation
- Interact with human capital and legal departments
- Develop/administer violations process
- Provide security event detection, incident response, and forensic capabilities

Senior Management

Senior Management, comprised of the SP Program Director and SP Site Director, is ultimately responsible for the security strategy and must make the necessary resources available to combat business threats. Senior Management is also responsible for disseminating strategy, establishing a security-aware culture, protecting the physical and logical assets of the operation, and assigning responsibilities to security personnel.

Senior Management will be responsible for administering the following functions:

- Ensuring implementation and maintenance of the SDU Security Plan and associated procedures as directed by InfoSec
- Making decisions on whether to accept the adequacy and associated risks of security controls for information systems
- Reviewing and accepting Information Security Plans and procedures
- Ensuring that the company effectively implements and maintains Information Security procedures and control techniques
- Assigning members of their functional or operational unit's management with the responsibility to direct Information Security activities, which ensures compliance with SP Security Plan

INFORMATION SECURITY OFFICER (ISO)

The Information Security Officer's duty is to ensure that the Security Plan and procedures are established and implemented to protect the SP's information assets, participate in the creation and review of the Security Plan and procedures, recommend security strategies, and maintain Information Security systems.

The SP will have procedures to prevent, detect, contain, and recover from Information Security breaches from internal and external sources, including both natural and man made disasters. The Information Security Officer is responsible for:

- Assigning information system security responsibilities to systems personnel
- Ensuring risk management activities are accomplished
- Ensuring that the SP IT resources are adequately protected, consistent with the SDU Security Plan, standards, and procedures
- Ensuring that information systems are operated, inventoried, used, maintained, and disposed of in accordance with the SDU Security Plan and procedures
- Participating in the decision-making team when *designing, planning, procuring* or *upgrading* technologies
- Informing Senior Management of breaches, Information Security activity, and risks
- Ensuring that the responsibilities of the Information Security Administrators are performed
- Ensuring that Security Assessment documentation that details the information system hardware and software configuration control and security countermeasures that protect it is maintained and authorized
- Implementing security awareness and training programs to promote the education of SP staff about Information Security subject matter, associated risks, and common practices
- Establishing and reviewing mitigating controls in relation to SDU Security Plan compliance

The Information Security Officer collaborates with Intrusion Detection and Forensic Analysis personnel to manage investigations into any alleged computer or network security compromises, incidents, or problems. All security compromises or potential security compromises must be reported to the SDU Information Security Officer.

The Information Security Officer directs the day-to-day management of the computer security program. This individual is also responsible for coordinating all security-related interactions among organizational elements involved in the security program, as well as those external to the organization.

Since a security incident on a SP secured system may have an impact on others, the Information Security Officer must have full access to the system and must be reachable 24 hours per day, 7 days per week in the event of a major security incident.

INFORMATION SECURITY ADMINISTRATORS AND ANALYSTS

Working in conjunction with the ISO and under the guidance of InfoSec, Security Administrators and Analysts are responsible for acting as information systems security coordinators. These individuals are responsible for establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the systems they administer. They are also responsible for reporting all suspicious computer and network-security-related activities to Intrusion Detection and Forensic Analysis personnel. Security Administrators and Analysts also serve as local Information Security liaisons, implementing the requirements of this and other information systems security policies, standards, guidelines, and procedures.

The Security Administrators and Analysts will be familiar with documented security practices and have prior approval before accessing the system. These individuals will be responsible for:

- Developing standards, procedures, and methodologies for the protection of all information and computing assets that are consistent with all SP policies
- Performing Security log and device configuration reviews conducted on a schedule reflective of the classification of data and devices being protected
- Administering and periodically reviewing access to information systems
- Assigning initial identifications and passwords, security profiles, and other security characteristics to new users and applications
- Changing security profiles for existing users
- Setting security characteristics of devices and communication channels
- Ensuring that user's access or type of access is restricted to the minimum necessary to perform his/her job
- Monitoring system integrity, protection levels, and security-related events
- Inspecting and monitoring user files, *with appropriate management direction*
- Periodically testing and evaluating security controls and techniques
- Generating audit trails and security reports and distributing them to the appropriate manager.

SYSTEMS ADMINISTRATORS

Under the direction of the SP IT Manager and Information Security Officer, designated System Administrators may be required to perform *limited* security administration functions on systems for which the individual(s) is assigned system administrator duties.

System Administrators will be familiar with documented security practices and have prior approval before accessing the system. System Administrators will be responsible for:

- Adding and removing system users with prior documented authorization
- Ensuring that all personnel who install, operate, maintain, or use an information system have authorized access to do so and are familiar with documented security practices before granting them access
- Maintaining a copy of the authorization/approval request for each user accessing a system systems under his/her control
- Monitoring access of system users
- Maintaining an up-to-date list of authorized system users for systems under his/her control;
- Generating, at least annually, a listing of current system users and their access profiles and distributing to the appropriate manager for review, update, and certification
- Configuring system parameters to harden the operating system as defined by the data classification level assigned to the information system in question
- Maintaining current documentation that properly defines the technical hardware and software configuration of system and network connections
- Ensuring that approved anti-virus software is installed and configured for real-time scanning, weekly full system scans, at a minimum, and configured to automatically update virus definition files

- Ensuring the proper acquisition, installation, testing, protection, and use of system software
- Starting up and shutting down systems

MANAGERS OF SYSTEM USERS

Managers at all levels are responsible for the actions of their subordinates on the system(s) for which they are authorized access.

Managers of system users are responsible for the following:

- Ensuring that users acknowledge that they understand the system security requirements, system security rules, and their responsibilities prior to being granted system access
- Using approved medium/process to authorize access to SP systems
- Ensuring that users' access to a system is restricted to the minimum (least privilege) necessary to perform their job
- Ensuring that duties and responsibilities in critical functions are divided/separated among different individuals to ensure that no individual has all the necessary authority or system access which could result in a fraudulent activity
- Ensuring that the status of system users' background investigations (including drug screening) are checked to determine if the background investigations have been successfully completed before granting them system access
- Providing prompt notification to system/security administrators of changes in employee status
- Ensuring prompt action to change or remove employee access profiles
- Reviewing employee access profiles at least annually as required by the system standards and procedures, for required changes and certifying to the system administrator that system access for each employee has been reviewed and is appropriate
- Reviewing audit trails and reports as deemed necessary by the Information Security Department
- Maintaining a copy of the authorization/approval form for each user accessing a system

APPLICATION SECURITY MANAGEMENT

It is important that an individual be assigned responsibility in writing to assure that each SDU computer system application has adequate security. These individuals are knowledgeable in the information and processes supported by the application and in the management, personnel, operational, and technical controls used to protect the application and associated information. This individual will assure that effective security products and techniques are appropriately used in the application and will be contacted when a security incident occurs concerning the application.

Within the SDU, and as specified in Appendix A of this document, each application will be represented from a security perspective by a system lead.

PHYSICAL SECURITY MANAGEMENT

Physical Security, in consultation with information security management, program and functional managers, and others as appropriate is responsible for developing physical security controls. Physical security is responsible for, but not limited to, physical access, central computer installation, backup facilities, and office environments. Physical Security is responsible for ensuring the physical security of all facilities containing operational SP information systems, that is, all SP equipment that processes, transmits, or stores information.

SYSTEM USERS

All SP information systems users are responsible for handling resources according to its classification, owner's requirements, and all applicable policies, standards, procedures, and safeguards.

Information systems users are responsible for the following:

- Knowing, understanding, and agreeing to the rules of system use and confidentiality, prior to access
- Accessing only authorized data and applications needed to perform management approved tasks, users must recognize that access capability does not equate authority
- Protecting access identification and authentication codes (e.g. passwords, personal identification numbers (PIN), encryption codes, etc.) from any misuse and improper disclosure
- Ensuring that input/output media (e.g., data sets, electronic media, magnetic media, paper copy, etc.) is properly safeguarded and destroyed as necessary
- Changing their password when required
- Properly logging off system(s)
- Properly protecting access to their workstation when it is unattended
- Notifying their supervisor and system/security administrator when access or authority is no longer required for their authorized tasks
- Acquiring software through authorized channels
- Adhering to copyright restrictions stated in each software license agreement
- Applying the security controls required by security policies, standards, and procedures
- Recognizing and protecting sensitive systems, applications, and data
- Providing cooperative assistance with security audits and reviews as required by laws, regulations, and other agreements
- Promptly reporting all suspicious activity to management or other designated contacts. (*Appendix A – Contact Lists* provides SP contact information for all security related resources. This list will be expanded to include other CCSAS resources and external services 60 days prior to the SDU go-live date.)

3.0 Security Processes and Procedures

3.1 Overview

Security processes and procedures are the direct effect of the implementation of security policy and describe the actions taken to ensure that policy requirements are applied to information systems, facilities, and all protected assets. Security procedures are detailed to a level that untrained personnel can perform as required and within specified guidelines to reduce the possibility of interruption to services and maintain compliance with all policies through repeatable practices.

3.2 Process and Procedures

Due to the large number of procedural documents related to the secure processing of child support payments for the State of California, all procedures are separately documented within other SDU technical and operational procedures manuals and plans. These procedures manuals and plans must be used in conjunction with the Security Plan to be fully effective.

Standard operating procedure, as they pertain or relate to security matters, can be found within the following documentation references:

- SDU Disaster Recovery Plan for SDU Services(CDL OM 005)
- SDU Business Continuity Plan for SDU Services(CDL OM 009)
- Interface Implementation Descriptions (IID – CDL IM 005-1&2)
- SDU Operations Management Plan (CDL OM 001)
- SDU Quality Assurance Plan (CDL OM 004)
- SDU Collections Procedures - Version 1&2 (CDL CO 001-1&2)
- SDU Disbursement Procedures – Version 1&2 (CDL DB 001-1&2)
- SDU IT Procedures (internal)
- SDU Security Procedures Manual (internal)

3.3 Collections

Security within the Collections Engine (CE) portion of the SDU is found at several levels. These levels are further defined in the following sub-section of Section 3.3. These levels include:

- Standard Microsoft and CE Security Features (logons, passwords, permissions, etc.)
- **Handling of Cash** (transaction controls)
- Security in Intelligent Data Capture (imaging, proof operations)
- Security in Exceptions Processing (research, check in-clearing)
- **Security in Archive Research** (data research and transmissions)
- **Separation of Duties** (review and reconciliation, transaction controls, terminal entry, data management)

An operator will need a valid password to begin processing on any workstation. Each operator is assigned a random unique operator identifier and a password. Each function is also assigned an access level dependent upon the role and position the user is in. Operators can only access those functions that are less than or equal to their operator access level. Operators can also be limited to only a specific work source or group of work sources. Specific security procedures related to such things as suspicious mail handling, as well as the items mentioned in this section of the document can be found in the SDU Security Procedures Document.

Standard Microsoft and CE Application Security

System security mechanisms will be established such that system, terminal, and password identifications are controlled, randomly selected, and uniquely identify the system user. All standard Microsoft user logons, passwords and permissions contribute to system security within the CE R&L application (Remittance and Lockbox). Each workstation on the network is supported by Microsoft Active Directory, and each user is provided a unique ID and password (that abide by all contractual security obligations). This initial access point will provide the SP with the ability to suspend all system access at the operating system level.

The CE R&L application includes an optional **unified logon** feature that utilizes an operator's Microsoft Windows Active Directory logon to control access within the application and therefore a separate R&L logon is not required. Using this unified logon feature does not affect the functional access levels assigned to each operator.

The following values are maintained for each operator on the CE R&L system:

- Operator ID
- Operator Password
- Access Level
- Default Key Ahead value
- Operator Name
- Work-sources
- Active vs. inactive – ex: on vacation, on jury duty, etc

Handling of Cash

Cash will be processed using a cash substitution document called the Cash Control Log shown below in *figure 3.1: Cash Control Log.* If an OPEX operator encounters cash they will immediately contact a supervisor. Together the operator and supervisor will count the cash and write the amount in the Cash Control Log. This log will be scanned and processed like any other financial instrument. Due to the identifying RTA (Routing and Transit / Account Number) the system will be able to report on the amount of cash received and processed on any given day.

SDU CALIFORNIA

CASH CONTROL LOG

Date	Opex Clerk Initials	Customer Name	Customer Participant ID	Cash Amount	Supervisor Initials	CA SDU Check Number

Deposit Total	Deposit Made By	Deposit Verified By	Deposit Delivered to Bank By

Attach Teller Receipt for Deposit to this form

Figure 3.1: Cash Control Log

SECURITY IN INTELLIGENT DATA CAPTURE (IDC)

The following section describes the site-specific information related to the configuration and installation of the IDC system on the Microsoft Windows 2003 Servers.

R&L APPLICATION FUNCTION ACCESS

Each operator within R&L is assigned an operator access level from 1-9. Each function is also assigned an access level of 1-9. Operators can only access those functions that are less than or equal to their operator access level. Operators can also be limited to working on only specific work sources.

The following fields are defined for each operator using the R&L Operator Administration function.

- Operator ID
- Operator Password
- Access Level
- Default Key Ahead value
- Operator Name
- Work-sources that this operator is allowed to work on
- If a work-source restriction has been placed on this operator
- Active vs. inactive – ex: on vacation, on jury duty, etc.
- Preferred Language (used if multi-language site)

Security in Exceptions Processing

The Exceptions processing system is governed by several different categories of security, which are all administered differently. Generally, there are two types of security: Physical Security and Access Security.

Physical Security governs physical access to disk drives, keyboards, and monitors on system servers. Access Security refers to network access to the system servers through network access logins and server logins. This access security encompasses the entire Exceptions processing system and is split into three areas, each of which is controlled by an administrator:

- Windows server security
- MS-SQL Server database security
- Exceptions processing security

Windows Server Security

MS-SQL Server Database Security

MS-SQL Database Security protects the database server and the data stored on that server. SQL Server security determines who can log onto the server, the administrative tasks each user is permitted to perform, and which databases, objects, and data each user can access.

SQL Server will be configured for security integration with Windows, thereby taking advantage of the security capabilities of Windows and authorizing Windows users to log directly into the SQL Server by mapping Windows user accounts to SQL login IDs. Database security and user login administration will controlled by the Database Administrator.

Exceptions Processing

The Exceptions processing system security features are what govern access rights to perform functions and work on individual objects. The functional abilities and the objects each have their own individual type of protection.

Functional Security

This type of security involves restrictions and allowances, which are imposed directly upon each user account.

The system administrator or other assigned individual will create users and passwords in the Exceptions processing system. Once a user exists in the system, the administrator may provide them with access to specific work items or classes of documents. These access rights to system services and tools are referred to as a "user profile". Each user is required to have a user profile. A user security profile represents the total set of access privileges assigned to a user, directly or indirectly, for all work items and import classes on the domain.

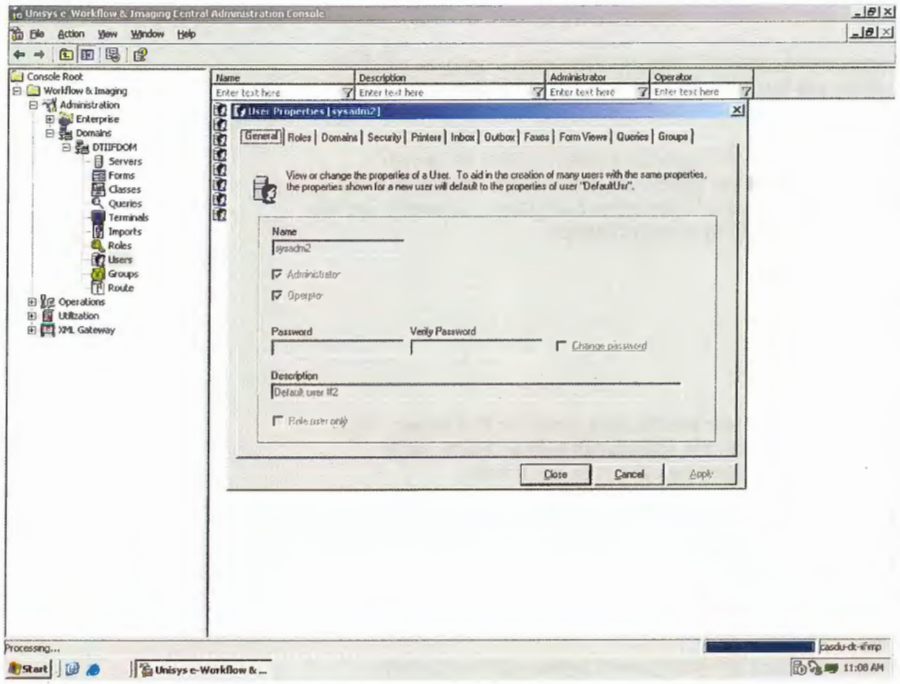


Figure 3.2: User Administration Screen

The user profile enables specific form views, queries, work-sets, queues, and other operations for each specific user. It therefore adds a level of security to the Exceptions processing system.

The Administration module is used almost exclusively to establish these functional security permissions for those users who will be performing ad hoc retrievals. Users may be given access rights to all document types or merely to a limited subset of documents. These functional rights are grouped into Batch, Desktop Menu, Desktop Tools, Viewer and Control Administration Console security functions. All new users are given access to only the functional rights and desktop tools within the system necessary to perform each task related to their specific role. User rights can be modified by the system administrator as required through a request at the supervisor or management level.

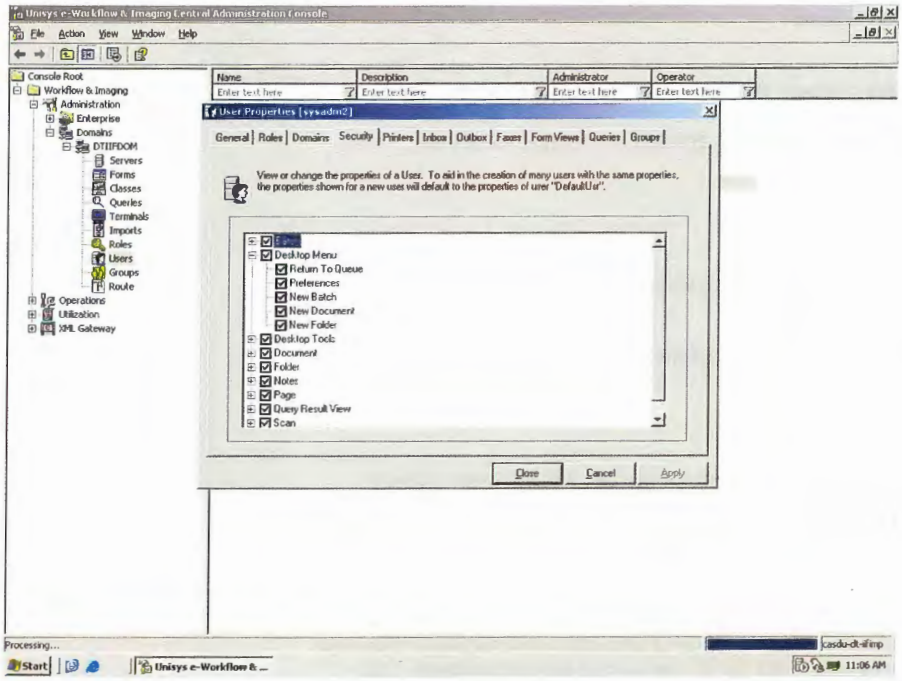


Figure 3.3: User Functional Security Administration Screen

Access management for scanning, indexing, adding documents, and printing are some examples of actions enabled or restricted by Functional Security for Exceptions processing. An overall list of functions that each user can have rights for includes:

BATCH

- Cut, copy, paste, delete, check quality, and rescan pages.
- Print, fax, reclassify, and index documents.
- Import and export images into documents.
- Reserve a batch for changes.

DESKTOP MENU

- Return work items to the queue from which they were retrieved.
- Create new batches, folders, and documents.
- Access the preferences dialog box on the desktop and in the document, file cabinet, and inbox viewers.

DESKTOP TOOLS

- Enable and disable File Cabinet, inbox, outbox, scanner, form builder, batch print, and system console.
- Document index, name, file, unfile, scan, print, fax, and reclassify documents.
- Import and export images and third-party application files.
- Cut, copy, paste, and delete pages.
- Reserve document for changes.
- Folder import and export third-party application files.
- Index, file, unfile, rename, print, fax, and reclassify folders.

- Cut, copy, paste, and delete documents.
- Create subfolders.
- Reserve folder for changes.
- Note create, modify any, modify if creator, delete any, and delete if creator of notes.
- Page print or fax page.
- Create, modify any, modify if creator, delete any, and delete if creator of markups.
- Query results.

VIEWER

- Print and fax.
- Retrieve reserved.
- Scan, select scan options, load profile from image server.

CONTROL ADMINISTRATION CONSOLE

- Set domain, work-step, image server, and user options.

SECURITY IN ARCHIVE RESEARCH

LOCAL SECURITY

When operators run windows based IMPS modules, IMPS utilizes their Windows User name to determine what modules they may load and what functions they are able to perform. IMPS Administrators can configure for each Windows User name what modules they are allowed to run and, for certain modules, such as IMPSOi, what functions within that module they are allowed to run.

WEB SECURITY

Since web requests may come from non-Windows machines, Windows security cannot be used. In this case, each Web User will be required to enter a user name and password to access the website. This user name and password will be passed to the IMPS Web Service with each request. SSL (Secure Sockets Layer) will be required to ensure that this information is encrypted before being transmitted over the network. An IMPS Administrator will be able to configure what functions each Web User will be able to perform.

SEPARATION OF DUTY

The SP will ensure via policies and procedures that duties are segregated in accordance with 45 CFR 302.20, "Separation of cash handling and accounting functions," which says that the State is required to maintain methods of administration to assure that persons responsible for handling cash receipts of support do not participate in accounting or operating functions which would permit them to conceal in the accounting records the misuse of support receipts. An individual will not have responsibility for more than one of the three transaction components: authorization, custody, and recordkeeping. Specific segregation of duties within the SDU will occur where an individual will not perform more than one of the following:

- Mail Processing - Open mail-process mail
- Data Entry and Aged Exceptions - Participant identification and processing exceptions
- Pass 2 - Encoding and endorsing
- End of Day Procedures - Reconciliation and transmitting to SWS/CSC
- Daily Reconciliation - Preparing deposit and monthly reconciliations
- Manage Adjustments and Aged Exceptions - Processing unidentified payments

In addition, an individual, either at the worker level or at the supervisory level, will not participate in more than one area of payment processing. A SDU worker or supervisor will not perform more than one function with respect to payment(s) in a particular batch. However, a supervisor will have the option to assist a SDU worker with respect to more than one function for payment(s) in a batch when necessary.

Finally, the SP will ensure that individuals receiving collections or making deposits are not involved in reconciliations.

3.3.1 Suspicious Mail Handling

Process for Identifying suspicious mail

Suspicious packages are identified as follows:

- Look for inappropriate or unusual labeling
- Excessive postage
- Strange return address
- Marked with restrictions, such as "Do not x-ray"
- Marked with threatening language
- Postmarked from a city or state that does not match the return address

Suspicious appearance is identified by:

- Powdery substance felt through or appearing on the package or envelope
- Oil stains, discolorations or odor
- Lopsided or uneven envelope

Other suspicious signs for identification include:

- Excessive weight
- Ticking sound
- Protruding wires or aluminum foil

Mail Room staff are instructed to NOT OPEN any package or envelope that appears suspicious.

Process for Handling suspicious mail

If a Suspicious Package or Envelope is encountered, staff are instructed to act in the following manner:

1. Do not shake or empty the contents of any suspicious packages or envelope.
2. Do no carry the package or envelope, show it to others or allow others to examine it.
3. Put the package or envelope down on a stable surface, do not sniff, touch or taste or look closely at it or at any contents which may have spilled.

In addition to the steps above, staff must adhere to the following:

1. Notify a supervisor, Manager
2. Alert others in the area about the suspicious package or envelope. Leave the area, close any
   doors, and take actions to prevent others from entering the area.
3. Wash hands with soap and water to prevent spreading potentially infectious material to face or skin.
4. Management contacts local law enforcement

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

3.4 Disbursements

The SDU Help Desk and System Administration group will have responsibility for user administration and password reset assistance for the SDU Disbursement Engine (DE). Initial set-up and

configuration of users will be managed by the SP with written instructions from the State on specific users and the agreed-upon Security Persona(s) to be used.

Access to the DE web interface requires a two-level authentication (user ID and password) that is cross-referenced to a Security Persona table. At the time of granting an individual user access to the DE web interface, the user is assigned to a security group, referred to as a Security Persona, which defines and limits what data the user can access (SWS, ARS, and/or CASES) and then further defines and limits what application functions can be utilized, including *Inquiry*, *Update*, *Alert Resolution*, and *Reporting*.

The following denotes the criteria applied by the DE specific to password administration:

- When the user ID is created, the initial password is randomly generated and will automatically expire when the user first logs on to the system, which prompts the user to create a new password
- Password expires after 30 calendar days, with the user prompted to create a new one
- Minimum password length is eight bytes
- Construction requirements include using three of the following four criteria:
  - Upper case characters
  - Lower case characters
  - Numeric values
  - Special characters (e.g., #, %, $, @)
- May not contain more than four consecutive letters from the User ID
- Passwords are not displayed on the screen in "clear text," but are displayed as "*******" regardless of whether the actual password contains an "*" or not.
- Access is disabled after three consecutive failed login attempts
- Access is disabled after 45 calendar days of inactivity or non-use

All operating system and database security descriptions defined for the Collections Engine in section 3.3 also apply to the Disbursements Engine.

3.5 PRINTING

Security at the SDU Printing facility with regards to system access and monitoring occurs as outlined below. Physical security within the facility follows the same guidelines, policies and procedures as all other areas of the SDU and meets all requirements as outlined in the SOW.

SYSTEM MONITORING PROCEDURES:

- All servers that house data for the SDU will have auditing turned on to capture both successful and failed login attempts.
- Specific folders located on these servers will have auditing turned to capture both successful and failed access.
- The Network Administrator will review these audit logs once every two weeks.
  - Process:
    - Event logs can be accessed by running the Event Viewer, listed under Admin tools on Windows 2000.
    - The Information Security Officer should be notified immediately of any incidents of suspicious failed access attempts.
    - Event logs will be saved to files during the audit review process.

ACCOUNT CHANGE AUTHORITY:

- All requests for adding new user accounts will be initiated by the Operations Manager for approval and completion.

- Requests for modifying existing user accounts will be initiated by the Operations Manager for approval and completion.
- Requests for disabling of user account will be initiated by Human Resources. Cancellation of user rights / deletion of accounts has to be authorized by the Operations Manager.
- New users will be setup so that the first time they log in, they are required to change their password.
  - Process:
    - Account changes can be made using the Active Directory Users and Computers listed under Admin Tools on Windows 2000.
    - See support documents N120, N170 and N130.

Account Change Request:

- Human Resources will maintain signed copies of account access rights.
  - Process:
    - Account changes can be made using the Active Directory Users and Computers listed under Admin Tools on Windows 2000.

Review of User Access Rights Procedures:

- The Information Security Officer will review account access rights every 3 months.
  - Process:
    - Event logs can be accessed by running the Event Viewer, listed under Admin tools on Windows 2000.
    - The Information Security Officer should be notified immediately of any incidents of suspicious failed access attempts.
    - Event logs will be saved to files during the audit review process.

4.0 Asset Classification and Control

4.1 Overview

Asset classification and control is one of the most important aspects of a complete security program. By evaluating the type of information in question and its associated value, a level of classification can be assigned to the information that then will be used to simplify policy implementation and enforcement through class-based controls.

4.2 Criteria for Determining Sensitivity

Determining sensitivity in an IT environment involves consideration of the system, data, applications, and type of user (i.e., users in a network across the country, users are contractor employees, etc.), which must be examined individually and in total.

All systems and applications require some level of protection for confidentiality, integrity, and availability. This is determined by an evaluation of the sensitivity, and criticality of the information processed, the relationship of the system to the organization's mission, and the economic value of the system components.

Information and information systems are sensitive if one or more of the following criteria applies:

- ***Confidentiality.*** The information and/or information system requires protection from unauthorized disclosure and access. A requirement that private or confidential information not be disclosed to unauthorized individuals.
- ***Integrity.*** The information and/or information system must be protected from unauthorized modification or destruction of information. The two facets of integrity are data integrity and system integrity. Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity is a requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- ***Availability***. The information and/or information system must be available on a timely basis to meet mission requirements or to avoid substantial losses. A requirement intended to assure that systems work promptly and service is not denied to authorized users.

Systems critical to the performance of the SDU's mission are sensitive. The data on each must be secured against unauthorized disclosure, modification or loss, and against unacceptable system downtime. Nothing in this section shall be construed to prohibit the disclosure of information when such disclosure is required by law or is requested or authorized by the legal owner of the information.

4.3 Information Classification Guidelines

The following guidelines will assist in determining the classification of the information that each SDU information system stores, processes, or transmits. A combination of several requirements determines information's classification. Determination of confidentiality, integrity, availability, risks, and the information system's role are required for proper classification and is the foundation of Security Assessment within the organization.

4.4 Classification and Control of Internal Revenue Service (IRS) Information

Information Systems that store, process or transmit information on behalf of the Internal Revenue Service must adhere to all policies of the U.S. Federal Government and the Department of the Treasury concerning the protection of Sensitive but Unclassified (SBU) information that pertains to tax

payers of the United States of America. Specifically, policies regarding information labeling and handling of Sensitive but Unclassified (SBU) data must be strictly adhered to and have been documented within the Internal Revenue Manual (IRM) section 30.9.1.

4.5 Data Ownership

A data (asset) owner is assigned responsibility for data classification and adherence to policy requirements for the protection of such information commensurate with the level of classification assigned. The owner of a specific data asset is the manager or administrator within the functional area where the data is either created or utilized to the furthest extent. For example, an operations audit report would be under the ownership of, and therefore be classified by the Operations Manager.

4.6 Information Classification and Role Based Access

Information and information systems are classified based on assessment of risk, valuation and the levels of integrity, availability, and confidentiality. Role Based Access Controls (RBAC), as described in detail in Chapter 8, Section 8.3, are employed on all information systems and properly segment authorities and rights by means of user assignment into predefined groups with access rights limited by their designed function. Due to this, user rights are not associated to the classification level of the data or the information system as doing so would not provide for the amount of granular control necessary to restrict user rights appropriately. Essentially, a greater level of security and control is applied through role based access controls than through assigning users functions based on classification since the majority of systems will be classified at levels 3 and 4. All access is based on need-to-know and appropriate group assignment based on user function and assigned responsibilities.

4.7 Information Sensitivity Levels

Classification	Description	Examples
UNRESTRICTED (Class 1)	Non-sensitive information that, if disclosed outside of the SDU, would not impact DCSS and the SP, its business partners, and/or its customers. Public information is releasable to any person.	Annual reports, news releases, marketing materials. SDU public web site containing static information.
INTERNAL (Class 2)	Information that, if disclosed outside of the SDU, might impact DCSS and the SP, its business partners, and/or its customers. Internal information is releasable to any employee or contractor.	Routine correspondence, employee newsletters, internal phone directories, inter-office memoranda, internal policies & procedures.
CONFIDENTIAL (Class 3)	Information that, if disclosed outside of the SDU, would adversely impact DCSS and the SP, its business partners, and/or its clients and their customers. Only those persons that have a demonstrated need-to-know and approval by the asset or resource owner may be granted access rights to CONFIDENTIAL information. This definition includes any specific information relating to cardholders, consumers, customers, employees, or clients.	Customer information, financial data, purchasing information, confidential audit reports, vendor contracts.

Classification	Description	Examples
RESTRICTED (Class 4)	Highly sensitive information that, if disclosed, would cause grave damage to DCSS and the SP, its business partners, and/or its customers. Only employees that have formal access approval (i.e., written approval by the asset or resource owner) may be granted access rights to RESTRICTED information. RESTRICTED information owners must be able to identify both the specific information in all its formats (electronic or printed) and all employees that access it. Records must be kept of all persons and systems that access resources containing RESTRICTED information.	Regulatory protected and sensitive information such as pending mergers or acquisitions documents, highly sensitive audit reports, strategic service provider plans/financial information.

Table 4.1: Information Security Levels

4.8 Confidentiality Classifications

	Unrestricted (Class1)	Internal (Class 2)	Confidential (Class 3)	Restricted (Class 4)
Description	Non-sensitive information available for external release	Information that is only sensitive outside the SDU. Generally available to employees and approved non-employees.	Information that is sensitive within the SDU, and is intended for business use only by specific groups of employees.	Information that is extremely sensitive, of highest value to the SDU and intended for use by named individual(s) only.
Examples	Advertising literature once issued.	Telephone Directory Organization charts	• Customer and Client information • Personnel information • Collections Data • Disbursements Data	• Strategic plans • Financial results prior to release • IRS Data
Impact of Unauthorized Disclosure	No adverse impact	Limited adverse impact	Significant adverse impact: • May incur financial or legal liabilities • May adversely affect DCSS and the SDU, its employees, its clients or customers • May assist a competitor • May undermine confidence in the service provider	Severe averse impact: • May cause severe financial or legal damage to the service provider • May prejudice the actual financial existence of the SDU, its employees, its clients and its customers • May destroy confidence in the SDU • May damage the SDU's reputation

Access Restrictions	Accessible to all employees and Public	Access normally restricted to employees and approved non-employees for business purposes only	• Access must only be granted on a business need to know • Access by external parties must be subject to a non-disclosure agreement as well as a business need to know	• Access must be limited to named authorized individuals • Access lists must be maintained • Information must not be shown to or discussed with anyone not authorized • Access by external parties must be subject to a non-disclosure agreement as well as a business need to know

Table 4.2: Confidentiality Classifications

4.9 Information Labeling and Handling

- A secure environment is a physically secure area e.g. computer room, where written authorization is required in order to remove any information storage media (e.g. tape).
- If any member of staff finds a confidential item and it is not properly secured, it is their responsibility to secure it in accordance with the classification label attached to it.
- Examples when labeling would be required are; printed report containing confidential information being circulated around a department or a PC diskette containing confidential information that is used during the day and locked in a drawer outside working hours.

	Unrestricted (Class 1)	Internal (Class 2)	Confidential (Class 3)	Restricted (Class 4)
Storage of Information (electronic)	No security control requirements	Site/Department storage will be adequate to prevent casual disclosure	Information may require encryption, where it does, approved methods must be used.	Sensitive fields must be encrypted using service provider-approved methods of encryption. See *Appendix I – Encryption Requirements.*
Storage of Information Media	No security control requirements	Site/Department storage will be adequate to prevent casual disclosure	Backup media must be kept in locked storage or a secure environment Off-site storage of backup media required.	Backup media must be kept in a locked drawer or equivalent, to which the owner has sole access. Off-site storage of backup media required.
Labeling of Information (documents only)	Labeling not required	Must be labeled with the classification	The documents must be marked 'CONFIDENTIAL' and/or physically separated and protected during	The documents must be marked 'RESTRICTED' and/or physically separated and protected during storage. Copies must

	Unrestricted (Class 1)	Internal (Class 2)	Confidential (Class 3)	Restricted (Class 4)
			storage	contain a unique ID
Labeling of Information Media (e.g. diskettes)	Labeling not required	Must be labeled with the classification	Media must be marked 'CONFIDENTIAL' Individual copies must contain a unique ID	The information media must be marked 'RESTRICTED' Individual copies must contain a unique ID
Disposal of Information (electronic)	Removal of Directory entry for file	Removal of Directory entry for file	In addition to removing the directory entry for the file, the space used by the file must be over-written by approved means.	In addition to removing the directory entry for the file, the space used by the file must be over-written by approved means.
Disposal of Physical Media (e.g. paper / magnetic media)	No Restrictions	ALL media must be regarded as CONFIDENTIAL information and be disposed of securely using approved methods and based on retention strategies.	ALL media must be regarded as CONFIDENTIAL information and be disposed of securely using approved methods and based on retention strategies.	Information must be disposed of securely using approved methods and based on retention strategies A record must be kept of how, when and by whom the information was destroyed.

Table 4.3: Information Labeling and Handling

4.9.1 Information Distribution

	Confidential (Class 3)	Restricted (Class 4)
Distribution	• Distribution lists of those groups authorized to receive information must be checked regularly to ensure currency • Distribution must be kept to a minimum • The item may only be copied or distributed by the originator of this item or the addressee • Items must be labeled with the classification before any copies may be made and subsequent copies must equally be labeled	• Distribution is to named individual(s) only • The originator of the information item must keep a record of the unique identifier associated with the copy, and the named individual designated to receive that copy • The item may only be copied or distributed by the originator of the item • Items must be labeled with the classification before any copies are made and subsequent copies must equally be labeled and enumerated

Voice	• Voice mail messages will be deleted as soon as possible. • Messages must not be forwarded (in case of misdialing or unauthorized access to other mailboxes).	• Information must not be discussed on speakerphones or during teleconferences unless all participating parties first acknowledge that no unauthorized persons are in close proximity. • Information must never be discussed on cordless or cellular telephones
Note: All legal and regulatory requirements will be reviewed regularly concerning the use of encryption technology.		

Table 4.4: Information Distribution

4.9.2 Data Retention Requirements

Data Retention Requirements for Information Security (in years unless otherwise specified)

Terms and Definitions:

- *Official* records are the archived versions of the native information.
- *Copy* records are the original records in their native form, e.g. system/security logs within the system itself and physical forms with original signature rather than a copy.
- *Domain* refers to the description of an attribute's allowed values. The *physical* description is a set of values the attribute can have, and the *logical* description is the meaning of the attribute.

Data Type	Official	Copy	Domain	Description / Notes
Payment data	4.3 Years	90 Days	Logical	Will be kept for life of contract
Supporting data	4.3 Years	90 Days		Will be kept for life of contract
Previously Produced Reports	4.3 Years	90 Days		Will be kept for life of contract
Statistical and all other pertinent data	4.3 Years	90 Days		Will be kept for life of contract
Images	4.3 Years	90 Days		Will be kept for life of contract
Logical Security Device and Application Logs	1 Year	90 Days	Logical	Examples: Firewalls, Intrusion Detection, Anti-Virus, Authentication Systems and Remote Access Systems
Operating System and Application Logs	1 Year	90 Days	Logical	Operating system and application specific logs concerning information relevant to information security and system/application status.
Service Provider E-mail Messages	60 Days	60 Days	Logical	Alternative means exist for longer retention upon employee request.
Router and Network Device Logs	1 Year	90 Days	Logical	Does not include network traffic; only configuration changes and information relevant to security such as authentication & access control.
PBX Outbound Call Records	1 Year	90 Days	Logical	
Network Plans/Drawings/Diagrams	LI*	SU	Logical	

Data Type	Official	Copy	Domain	Description / Notes
Access Request Forms	TE	N/A	Logical	
Employee Physical Security Access Cards	TE+AR	TE	Physical	
Employee Physical Security Access Database	1 Year	1 Year	Physical	
Surveillance Video Tapes and Logs	30 days	30 days	Physical	
Visitor Sign-In Logs and Access Reports	1 Year	1 Year	Physical	
Incident Reports	1 Year	1 Year	Physical	Physical Security specific incident reporting only.
Investigation Reports – External	5 Years	1 Year	Physical	Physical Security specific investigations only.
Investigation Reports – Internal	1 Year	1 Year	Physical	Physical Security specific investigations only.
Information Security Investigations: Forensic and Incident Data and Reports	LI	1 Year	Investigations	All information related to the investigation of an information security incident and forensic analysis.
Retention Policy Event Codes	Additional Requirements: Data stored for life (LI) must remain readable over the lifetime of the information. The media utilized to archive the information must be checked at least every four (4) years for readability and applicability to modernized hardware and software requirements.			
LI – Life (of corp., property, system, etc.)				
SU – Superseded				
TE – Termination				
QR – Quarterly Review				
AR – Annual Review				

Table 4.5: Data Retention Requirements

All additional data storage and back-up methodologies, standards and procedures, and off-site storage strategies, standards and procedures are detailed in the SDU Disaster Recovery Plan (CDL OM 005).

4.9.3 Additional Data Retention Requirements

In addition to the time-relative requirements listed in the previous table, the following requirements also pertain to the CA SDU:

The SP shall create, store, and maintain back-ups of the SDU system files, programs, documentation, data files, etc. off-site in secure, waterproof, earthquake-proof, and fireproof facilities in accordance with ACF H-5(f) and consistent with the CCSAS CSE Disaster Recovery Plan (CSE CDL TM 090) and the SDU Disaster Recovery Plan for SDU Services (CDL OM 005).

The SP shall retain back-ups files for time periods specified in the Statement of Work.

4.10 Additional Requirements for Information Labeling and Handling

4.10.1 Media Identification Labels

Removable magnetic media is uniquely labeled so it can be distinguished from other media and receive the security protection required for the data contained. Each piece of magnetic media used in conjunction with a system shall have an external label containing the following information:

- Media name;
- Media identification - identify the system on which the media was created;
- Owner's name – group, department or business unit responsible for the data;
- Location – the data center of facility in which the media was originally created;
- Date created - indicate the date that the data or information was created and stored on media;
- Retention date (how long data will be retained), and
- Any special sensitivity indicators.

4.10.2 Overwriting and Degaussing

4.10.2.1 Overwriting

Overwriting is a process whereby unclassified data is written to storage locations that previously held service provider/project data. To purge the information system storage media, this process overwrites the media with a bit pattern, then it counters with another pattern, and finally with a 3rd pattern; e.g., overwrite first with 0011 0101, followed by 1100 1010, then 1001 0111. The number of times an overwrite must be accomplished depends on the storage media, and sometimes on the sensitivity of the media. A purge is not complete until a final overwrite is made using unclassified or null data.

4.10.2.2 Degaussing

Degaussing is a process whereby the magnetic media is erased. It may be accomplished in two ways:

Alternate current erasure, the media is degaussed by an alternative field that is reduced in amplitude over time from an initial high value (i.e., alternate current powered), or

Direct current erasure, the media is saturated by applying a unidirectional field (i.e., direct current powered by employing a permanent magnet).

4.10.3 Clearing and Purging Methods

- *Magnetic Tapes*. A Type I or Type II degausser is acceptable for clearing Type I, II, and III tapes.
- *Magnetic Hard Disks and Magnetic Drums*. Both overwriting and degaussing are approved methods to clear or purge this media.
- *Magnetic Floppy Disks and Cards*. Overwriting for clearing is an approved method for cards. Degaussing with Type I degaussers or approved hand-held magnets are the preferred method for purging floppy disks and cards.
- *Magnetic Core Memory*. Magnetic Bubble Memory and Thin Film Memory. Overwriting and degaussing, using Type I degaussers and hand-held magnets, are approved methods to clear and purge magnetic core memory.
- *Random Access Memory (RAM)*. Both overwriting and removal of power for at least one minute are approved methods for clearing and purging.
- *Read Only Memory (ROM)*. Data is permanently stored in ROM; therefore, clearing and purging this media has no relevance.
- *Erasable Programmable Read Only Memory (UVPROM)*. The use of ultraviolet is approved as a method to clear and purge.

- *Electrically Erasable Read Only Memory (EEPROM)*. Different forms of overwriting (e.g., single-step chip erase, individual overwriting, etc.) are approved methods to clear and purge.
- *Optical Disks*. Currently, no procedures exist that are considered adequate to ensure purging of these media. However, magneto and optical disks can be cleared by a single overwrite. Examples of optical disk include: CD-ROM (Compact Disk Read-Only Memory), WORM (Write-Once-Read-Many), and magneto-optical (Read-Many-Write-Many).
- *Ferromagnetic RAM*. No standards have been published for providing procedures for this media. However, consistency with all other types of storage media would dictate that a single overwrite is sufficient for clearing.
- *Disk Exercisers*. Many drawbacks exist to using overwrite software for purging disks. Some of these drawbacks are not applicable to disk exercisers, which use a dedicated operating system. Exercisers have the capability of writing at different frequencies. This makes them a more effective alternative to overwrite software; however, the exerciser is not approved to purge disks.

4.10.4 Destruction Methods

Destruction of confidential information, envelopes, other paper media, and electronic media must occur in accordance with State policy (22 CCR 111460 Record Disposal).

- Media shall be overwritten or degaussed, before submitting for destruction by one of the following methods:
  - Destruction at a metal destruction facility (i.e., smelting, disintegration, or pulverization),
  - Incineration or Application of an abrasive substance (emery wheel or disk sander) to a magnetic disk or drum recording surface.

- Whenever media contains government data or Restricted (Class 4) data, destruction procedures and process shall include a control log, which contains:
  - Media label ID,
  - Date destroyed,
  - Method of destruction, and
  - Signature of employee providing destruction services

5.0 PERSONNEL SECURITY

5.1 OVERVIEW

Personnel security controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

These controls are put into place to improve the security of a particular system (or group of systems). Personnel security controls often require technical or specialized expertise and rely upon management activities and technical controls.

All other issues regarding employees of the SP not covered herein are to be addressed by the Human Resources Department separately.

5.2 PERSONNEL SCREENING

All applicants (after accepting an offer of employment) must complete a background check. The applicant must provide detailed past employment information dating back seven years, among other information. The background check is then processed by Security Compliance to verify the information given by the applicant is accurate and complete.

Personnel screening employs the following controls:

- Availability of satisfactory references;
- A check (for completeness and accuracy) of the applicant's application;
- Independent identity checks (passport or similar document); and
- Criminal history check.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and in particular if these are handling sensitive information, e.g. financial information or highly confidential information, the organization may also carry out a credit check. For staff holding positions of considerable authority this check will be repeated periodically or at least every 7 years. Results of this check may be cause for termination or reassignment.

A similar screening process will be carried out for contractors and temporary staff. When these staff are provided through an agency the contract with the agency will clearly specify the agency's responsibilities for screening and the notification procedures it needs to follow if screening has not been completed or if the results give cause for doubt or concern.

This information will be handled in accordance with any appropriate legislation existing in the relevant jurisdiction.

5.2.1 CONFIDENTIALITY AGREEMENTS

Employees and contractors must sign the DCSS Confidentiality and Disclosure agreement before being allowed to access information systems, as well as on an annual basis. Agreements are issued by the Human Resources department, and must be completed before access is granted. Thus, any IT Administrator (or anyone that grants user access) must check with Human Resources to ensure that the DCSS Confidentiality and Disclosure agreement is on file for the user. Refer to Appendix F – Accountability and Appendix G – Confidentiality for specific agreement content.

When an employee leaves the organization, all information stored by that employee on SP owned or leased computers, electronic networks and other information-processing and storage devices remains the property of the SP.

While it is not the organization's practice to review either electronic mail messages or documents stored on computers, electronic networks and other information-processing and storage devices on a regular basis, the SP reserves the right to monitor and review the content of any such electronic message or document for any business or legal purpose without informing the sender or recipient of that electronic message or the person in whose possession those computer files reside.

In using the e-mail system, all employees must comply with the following guidelines:

- E-mail systems may not be used for any type of solicitation other than those directly related to business activities. This restriction includes, but is not limited to any religious, political, charitable, social, or personal purposes.
- E-mail users will not send or disclose SP confidential or sensitive information to anyone without the need to know. Under no circumstances will the use of unencrypted Internet e-mail be used to send any SP sensitive information to any persons.
- Sensitive information or files being transmitted by email should be encrypted, regardless of destination.
- Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be created, sent, or forwarded by e-mail. If an employee encounters this kind of material, they are obliged to report it to their supervisor.
- Chain e-mail is a non-business related message sent to a number of people asking each recipient to send copies with the same message to a specified number of others. Employees should delete all chain e-mail and all non-business-related mass e-mail immediately upon receipt and refrain from forwarding to any other employees.
- Never alter the "From:" line or other attribute-of-origin information in e-mail. Anonymous or pseudonymous messages are forbidden.

Violations may expose an employee to disciplinary action, including loss of employment.

5.2.2 Terms and Conditions of Employment

SP employees are employed at will and must adhere to all policies and procedures for proper use of information systems. All system users of SP systems are responsible for handling information system resources according to the information's classification, owner's requirements, and all applicable policies, standards, procedures, and safeguards.

Information systems users are responsible for the following:

- Know, understand, and agree to the rules of system use and confidentiality, prior to access;
- Access only authorized data and applications needed to perform management approved tasks, users must recognize that access capability does not equate to authority;
- Protect access identification and authentication codes (e.g. passwords, personal identification numbers (PIN), encryption codes, etc.) from any misuse and improper disclosure;
- Ensure that input/output media (e.g., data sets, electronic media, magnetic media, paper copy, etc.) is properly safeguarded and destroyed as necessary;
- Change their password when required;
- Properly log off system(s);
- Properly protect access to their workstation when it is unattended;
- Notify their supervisor and system/security administrator when access or authority is no longer required for their authorized tasks;
- Acquire software through authorized channels;
- Adhere to copyright restrictions stated in each software license agreement;

- Apply the security controls required by security policies, standards, and procedures;
- Recognize and protect sensitive systems, applications, and data;
- Provide cooperative assistance with security audits and reviews as required by laws, regulations, and other agreements; and
- Promptly report all suspicious activity to their management or other designated contacts.

5.2.2.1 Disciplinary Process

Violation of policy requirements is subject to disciplinary action. The appropriate action is determined by an employee's manager in coordination with the SP Human Resources Department.

5.2.2.2 Exiting Employees and Contracted Labor

Employees or contracted labor leaving the SP for any reason are required to submit a disclosure of all information located on computers that may have been used to perform work related to the SP and either:

- Return all such work to the SP while acknowledging that all such information has been returned, or;
- Submit a declaration that all such information has been removed and will not be used for personal benefit.

5.3 Enforcement of Unauthorized Use of Information Systems

Information system users are not to utilize systems for use other than that which has been authorized by the business. Enforcement of allowed usage is performed through technical measures designed to detect and reduce unauthorized use of information systems. The following controls are employed:

- Internet content filtering
- Email scanning
- Limited protocol access (firewalls)
- Monitoring usage trends

5.4 Information Security Education and Training

The requirement for end-user Security Awareness Training applies to contractor and temporary employees as well as all employees of the service provider and its subsidiaries.

During the On-Boarding process, employees review the CCSAS Project overview video, CCSAS Data Security Training document, DCSS Internet/Electronic E-mail Policy document, DCSS Confidentiality Training video: Securing the Future, DCSS Confidentiality Statement, and the UNAX & Safeguarding Federal Tax Information video. Contractors receive the same information upon beginning their assignment and will be required to review the videos as well. All re-training on these items is done on an annual basis. In addition, all employees are automatically bonded within our crime insurance coverage. Please see Appendix E – Certificate of Insurance for proof of bonding coverage.

Terms and conditions of employment include the assignment of responsibility for information security to each authorized employee or contractor.

Employees complete the DCSS Confidentiality and Disclosure form during their on-boarding training. Their information is then loaded into the training matrix, and all confidentiality statements are stored in the employee's security/training file located on-site. The SDU Human Resources Manager has access to these secured files and can provide access to the DCSS upon request.

A training matrix listing all employees and contractors involved on the project is updated and maintained by the SDU HR Manager. This Matrix lists all items regarding security, confidentiality, on-boarding, and compliance trainings with dates of completion. In addition, a checklist of completed

training, with dates, is also used and attached to the employee's training/security folder that is located on-site. Please see Appendix D – Training Matrix.

5.4.1 Security Awareness Program

The purpose of computer security awareness, training, and education is to enhance security by:

- Improving awareness of the need to protect system resources;
- Developing skills and knowledge so system users can perform their jobs more securely; and
- Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

The Security Training and Awareness Program ensures that the following goals are met:

- All SP employees and contractor employees involved with the management, operation, programming, maintenance, or use of SDU information systems will receive training in acceptable computer security practices *prior to information system access*.
- All employees and contractor employees will be briefed on their system security responsibilities, as often as necessary, but *no less than once a year.*
- All new employees will receive a system security orientation *within the first ten working days* following initial employment. The orientation will be given separately or as part of the existing new employee orientation.
- All seasonal and other SP employees who have been in a non-work status will be given a refresher system security orientation within the first ten work*ing days* upon return from a non-work status of four months or longer.
- Contractor employees must receive the same level of Information Security awareness and training as SP permanent employees. While under contract with the SP, contracting vendors are responsible for ensuring that their employees have been provided appropriate security training and awareness.
- All required documents such as acceptable use policies and non-disclosure agreements are signed by new employees prior to commencing work and by existing employees every seven (7) years.

5.4.1.1 Security Awareness Program Responsibilities

Information Security is responsible for:

- Providing assistance to ensure that security training goals are met; and
- Providing direction and priority to the security awareness training program.

Business Units: Individual Business Units (specific areas of the SDU operation such as Data Entry, Help Desk, etc.) are responsible for ensuring that their users are:

- Trained on how to fulfill their security responsibilities prior to allowing them system access;
- Appropriately trained to what they need to know to use the system securely;
- Versed in the rules of the system before allowing them usage; and
- Periodically trained to assure that they continue to understand and abide by the applicable rules.

5.5 Segregation of Duties

Separation of duties was previously discussed in Section 3.3, but is expanded further in this section as it relates specifically to Personnel Security. The purpose of separating duties is to reduce the risk (intentional or otherwise) of system misuse and interruption. It is recognized that staff limitations may necessitate the multitasking of personnel performing Information Security duties. However, when

there is a perception of partiality, personnel are instructed to make the best decision based on the position they are currently filling.

The SP shall conform to the Code of Federal Regulations, Separation of Cash Handling and Accounting Functions to assure that persons responsible for handling cash receipts of support do not participate in accounting or operating functions which would permit them to conceal in the accounting records the misuse of support receipts.

Situations that would give a single person the ability to approve their own critical work will be identified and either eliminated or the supervisor/manager is responsible for ensuring there is supervision and audit trails of any work done in that situation.

5.6 Employee Termination

When an employee terminates employment with the SP, the following guidelines will be followed:

Immediately change or remove the passwords for those user ids to which an employee leaving the SDU has had access or update capabilities. This standard practice serves to protect the employee in the event of any problems and the SDU systems against possible tampering. Monitoring such user ids is primarily the responsibility of user's manager, with assistance from the Data Owner and the system administrator. Reinstatement will require the same level of authorization as establishing a new user id.

Terminated employees, in conjunction with their Supervisor/Manager and the Human Resources Manager are required to return all SDU property and materials, or perform specific tasks including but not limited to:

Items to be Returned

- Keys (office, building, other)
- Badge/ID (office, building, other)
- Card keys (office, building, other)
- Service provider guidelines and/or manual(s)
- Departmental/service provider-issued IT equipment (See attached custody forms for specific items if needed.)
- Computer
- Laptop

Tasks to be completed

- Deactivate keyless entry account
- Clean out lockers, desk, etc.
- Remove name from SP directories
- Verify for correspondence
- Deactivate network access accounts (network, mainframe, servers, etc.)
- Deactivate specific software access (accounting software, HR software, etc.)
- Deactivate e-mail account
- Deactivate Telephone access
- Deactivate Voice mail
- Deactivate service provider-provided dial-up account access

The SDU Human Resources Director, in conjunction with the area Human Resource Manager and SDU Site Director are accountable for communicating employee turnover to each functional area responsible for any of the aforementioned tasks.

6.0 PHYSICAL AND ENVIRONMENTAL SECURITY

6.1 OVERVIEW

Physical security involves the use of locks, access/photo ID badges, alarms, procedures, and similar measures to control access to the information system.

Physical and environmental security controls are implemented to protect the facility housing the system resources, the system resources themselves, and the facilities used to support their operation from theft, espionage, waste, fraud, abuse, or damage by accident, fire, and environmental hazards.

The SP shall adequately protect its facilities used to process, transmit, or store sensitive service provider information in support of critical operations and missions. The specific security policies for each SP physical location may vary.

6.2 CONTROLLED ACCESS

Access to all SDU secured facilities is controlled through the implementation of physical security policies to ensure protection of facilities processing sensitive information 24 hours a day and 7 days a week.

6.3 PHYSICAL ACCESS CONTROLS

Physical access controls are unified by policy but may vary in their implementation depending on the facility of question. The following controls have been established for each facility that stores, processes or transmits sensitive information related to the State of California Child Support Services Disbursement Unit (including the SDU Printing Facility):

6.3.1 INTRUSION ALARM SYSTEMS

Access Control and Intrusion Alarm System requirements:

- Ensure that the electronic access level(s) provided to each employee, contract worker, vendor services provider, etc., is commensurate with business and operational requirements.
- The electronic access system must be programmed to historically document the activities of all cardholders.
- Electronic access control cards shall be issued to one individual. At no time shall personnel "pass" their access card to another individual to access company facilities.
- Termination of employment or change vendor status shall be immediately reported and the disable termination checklist must be completed. Security access cards shall be returned and immediately deactivated to prevent unauthorized usage.
- The loss of an access control card shall be immediately reported. The access control card shall be immediately deactivated to prevent unauthorized use.
- Maintain and distribute alarm activation and deactivation codes on a restricted, need-to-know basis for those facilities that have independent monitored security systems.

The intrusion alarm system that is in place within the State Disbursement Unit employs a dialer system that notifies the central monitoring station, which in turn calls authorities upon alarm. Specific contact information is programmed directly into the dialer system and can be updated or modified as necessary..

6.3.2 CLOSED CIRCUIT TELEVISION MONITORING

The following standards are applicable to the installation and administration of closed circuit television (CCTV) systems:

- Historical review of negative occurrences is required for all CCTV monitoring.
- Maintain digital recording equipment in a secure location.
- Non-functioning and/or simulated CCTV systems are to be removed so as not to give employees a false sense of protection.

6.3.4 Access on a Need-to-Know Basis

All facilities access is granted on a need-to-know basis only. All employees and visitors require authorization from an approved manager prior to gaining access.

6.3.5 Badge Program

All secured facilities require the use of a photographic identification badge for entry and accountability. The following standards are applicable to the service provider issued Photographic Identification Badge Program:

- Photographic identification badges will be issued to all service provider employees, extended term contract workers, and other regular vendor services providers, including cleaning crew personnel. The photographic identification badge will be securely laminated to the employee specific access control card and the laminate must have the SP iridescent logo and it must be prominently displayed on your front torso between the neck and just below the waist at all times while at service provider facilities.
- All persons seeking entrance to a facility, who are not in possession of a service provider issued photographic identification badge, including off-site employees, etc., will be required to comply with visitor registration procedures and will be issued a temporary identification badge to be displayed for the duration of the visit.
- All non-resident employees, short-term contract workers, and all vendors must be continuously escorted at facilities unless previously authorized for access.
- Service provider issued photographic identification badges can be obtained by the responsible management personal, upon completion of; a) an executed Security Facility Access Request Form; b) an approved background check; and c) an employee photograph. The photographic identification badge will be laminated to a pre-programmed access control card. Photographic identification badges and/or access control cards shall not be issued prior to the completion of an approved background investigation.

6.3.6 Locks and Storage

The use of locks as security controls are implemented to protect the facility and resources from theft, espionage, waste, fraud, abuse, or damage by accident, fire, and environmental hazards.

The following are guidelines for the use of mechanical locks and keys.

- The installation of mechanical locks and keys that overrides the electronic access control system should be strictly limited. Should the requirement exist to provide a manual lock that overrides the access control system, this mechanism should be located on a secondary entrance and utilized only in the event of emergency circumstances.
- The issuance of keys should be conducted in a strictly controlled and well-documented manner. All key control assignments and records shall be maintained by the Information Security Officer and audited as required.

In addition, equipment should be physically protected from security threats and environmental hazards. Protection of equipment (including that used off-site) is necessary to reduce the risk of

unauthorized access to data and to protect against loss or damage. The following controls should be adhered to, at a minimum:

- Work areas containing sensitive data will be identified and physically secured. Access to these locations will be limited to persons on a need-to-know basis only.
- All wiring cabinets/closets will be physically secured. Network cables, except workstation cabling (where some exposure is required), shall not be exposed and should be inspected routinely.
- Authorized administrators will control distribution and use of diagnostic monitoring equipment (software and hardware), such as protocol analyzers and packet sniffers will be limited to authorized personnel.
- Uninterruptible power sources (UPS) should be used for all LAN servers to protect against loss of critical services due to a power outage.
- Sensitive information systems must be isolated.
- Information systems shall be reasonably protected against all anticipated environmental and natural hazards to reduce the risk as much as possible.
- Surge suppression will be used on all workstations to protect against power fluctuations.
- There must be no eating, drinking and smoking within data centers or computer rooms/closets.
- Computer/communications hardware not in compliance with the SDU's technical architecture or not owned or leased by the SDU is not permitted to be used on company property.
- Visitors may be an exception to this policy if specifically authorized by management.
- SDU processing facilities must utilize desks that do not contain drawers or any other methods of storage regardless of the ability to lock them.
- Personal belongings must be stored within approved lockable containers for all SDU processing facilities.

6.3.7 Isolated Delivery and Loading Areas

Delivery and loading areas are controlled and isolated from information processing facilities to avoid unauthorized access. Security requirements for such areas are determined by a risk assessment of the environment in question. The following controls are required:

- Access to a holding area from outside of the building must be restricted to authorized personnel.
- The holding area will be designed so that supplies can be unloaded without delivery staff gaining access to other parts of the building.
- The external door(s) of a holding area must be secured until arriving cargo has been validated and when the internal door is opened.
- Incoming material shall be inspected for potential hazards before it is moved from the holding area to the point of use.

6.3.8 Facilities Access

All facilities that contain information processing systems, or other sensitive information or processes will meet the following minimum physical security parameters:

All personnel entering SP facilities containing operational SP systems must be identified and all access privileges must be minimized. All access must be registered to provide a minimum of a sixty (60) day audit trail. All visitor access to SP facilities must be registered and identified. The capability must exist for this log to be accessed and reports produced as required.

- Upon employment with the SP, all employees receive an access/photo identification badge (ID). This ID badge allows access to those areas required by the employee. Management is responsible for notifying Physical Security regarding the type of access each employee requires. SDU management is responsible for notification for access.
- ID badges are to be worn and clearly visible at all times while in SDU facilities. The ID badge is to be used for entry to the facility and controlled areas.
- Any authorized badge holder who does not have their ID badge must enter through the Main facility entrance and report to their management for temporary access. Temporary badges are issued for no more than one day.
- No external indication of sensitive operations (i.e., signs will not indicate sensitive operations within, no directories or floor-plans that indicate the location of sensitive areas will be available to the public).
- All Office equipment such as photocopiers, fax machines, and printers, will be located within the security perimeter.
- All doors and windows outside of the security perimeter will be appropriately secured (i.e.: bars and/or alarms for windows, and doors that are alarmed and lock automatically).
- Security systems will be installed that are monitored to detect intrusions during off hours, or areas that are unoccupied.
- Hazardous materials and all loading-docks/freight reception areas will be physically separate and as distant as possible from the sensitive areas within the security perimeter.
- A basic objective in the design of a facility or building is to provide adequate means of entry and egress only for authorized personnel. Each pedestrian entrance requires a means of security control.
- Personnel leaving the building with proprietary or confidential information and/or equipment must have the appropriate authorizations.

6.3.9 Visitor Access

In concert with State Disbursement Unit facilities access, visitor access requirements are also deemed necessary with regards to physical security. Detailed below are applicable requirements for SDU visitors:

- All visitors entering SDU facilities must sign the visitor's log. Visitors will receive a temporary visitor badge which must be worn at all times while in the building. An authorized badge holder is responsible for escorting the visitor and ensuring that all applicable procedures are followed. Before access is granted, special access rights may be required, and all access must be authorized and logged.
- Visitors are not permitted to carry briefcases, boxes or other containers into any restricted area in which personal items are not allowed, unless reviewed and approved by management. Any such items removed from the facility are subject to search.
- When leaving the facility, the badge holder will escort the visitor to the main lobby and ensure that the temporary badge is returned.

6.3.10 Data Center Access

There are additional Data Center access requirements as it pertains to the California State Disbursement Unit. They are detailed below:

- The appropriate data center site manager must approve all tours that require access to data centers.
- No cameras or recording devices are allowed inside the computer room without prior written authorization by the SDU Site Director.
- The tour escort will be responsible for ensuring that all tour members remain under their direct supervision at all times.
- Routine entry to Data Centers should be allowed only to individuals whose primary workstation is within the workplace area. Entry by persons whose primary workstation is not

within the area should be logged and authorized on an as-needed basis. Authorized support personnel should be kept under visual control.

6.3.11 Access Log

Visitor access logs are required for all entry and exit of facilities. Requirements for log detail are specified in the visitor registration program requirements below:

The following standards are provided to facilitate the implementation of a visitors registration program:

- A visitor registration program should be implemented and maintained at each facility. All visitors should be required to sign in and sign out upon each arrival and departure.
- The visitor registration sheet should contain the following information at a minimum:
  - Date
  - Visitor's name
  - Visitor's company
  - Name of employee sponsor
  - Arrival time
  - Departure time
  - Visitor badge number
- All contract services providers who do not pass the approved background program shall be required to adhere to visitor documentation processes.

These Visitor Access logs are made available to the state as requested. Current and closed visitor log books are requested through the SDU Site Director and must be viewed and remain on the SDU premises. A sample log can be viewed in *Appendix I, Visitor Access Log*.

6.3.12 Restrictions on Signage and Perimeter Controls

Strictly enforced policies concerning signage or logos as they pertain to information processing facilities are detailed as part of physical security as it pertains to the perimeter. Physical security to a particular building, or area within a building is designed with a "Security Perimeter" in mind. This Security Perimeter is a physical barrier surrounding the area to be protected. There must be no gaps in the barrier and all entrances and exits should be properly controlled with the appropriate level of access control.

Additional perimeter controls are as followed:

- Perimeter should be clearly defined.
- The number of public and employee perimeter entrances should be restricted. When possible, the visitor entrance to all company offices should be clearly marked and limited to one (1) entrance. The visitor entrance should be continuously supervised during regular business hours.
- The perimeter of a building or site containing information processing facilities shall be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur). The external walls of the site shall be of solid construction and all external doors should be suitably protected against unauthorized access, e.g. control mechanisms, bars, alarms, locks etc.
- A manned reception area or other means to control physical access to the site or building must be in place. Access to sites and buildings should be restricted to authorized personnel only.
- Physical barriers shall be extended from real floor to real ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire and flooding.
- All fire doors on a security perimeter shall be alarmed and should slam shut.

- Where appropriate, a staffed reception area should be located in all sites that contain sensitive information processing. Access to these sites should be controlled through either the staffed reception area, or other electronic means such as card-access systems.
- Management should instruct employees to assume responsibility for building access control by verifying that doors used to enter or leave the facility are not left ajar but are securely locked after each use.
- SDU Processing facilities shall not be identified by signage or logos.

6.3.13 Auditing Physical Security

The development and implementation of physical security initiatives is predicated upon the completion of the security assessment and audit processes by Service Provider Physical Security, to determine site specific vulnerabilities and to develop cost effective strategies.

The security assessment and audit processes may include a review of the following: security related incidents, interviews with service provider employees and outside entities, a review of the premises, and testing of existing physical and electronic security system(s).

The Service Provider Physical Security Department is responsible for conducting security audits at all service provider facilities.

6.4 Floor Plans

Floor plans of each processing facility are detailed for use in physical security architecture and logistics of device placement. All floor plans have been separately detailed and may be available upon request.

6.5 Protection of Equipment

Protection of equipment relies on security controls and policies utilized to protect equipment from unauthorized use and environmental hazards. Equipment protection is detailed above in section 6.3.6 Locks and Storage.

In addition, protective measures are applied to all mobile computing devices. The term "mobile systems" or means any SP information device that is in use and not in a fixed location (most commonly laptops, but it also includes PDA's, cell phones, etc., herein referred to as Portable Electronic Devices (PED's)). Mobile systems may be quantified as "devices capable of mobile processing and storage of digital information", i.e. any device that is not fixed in its location and can leave a SP physical environment.

The following controls have been established for mobile computing devices:

- Mobile computing devices require additional protection measures and must include the following:
  - Software firewalls capable of inspection must be employed on all mobile computing devices, when the capability exists. The ability to disable such software shall not be allowed.
  - Virus scanning software must be employed by all mobile computing devices and should be setup to automatically update virus definitions every 24 hours, at a minimum.
- The local Information Security Officer is responsible for establishing and maintaining a standard mobile computing security configuration, compliant with all policy requirements.
- All use of remote control software on any modem-connected or VPN-connected device, which is also attached to the SDU network must be approved before implementation.

Privately owned computers or mobile computing devices may only be used to process or store sensitive information if such devices meet all the requirements set forth herein and the use is authorized. All mobile computing devices must be monitored and controlled so that any changes in the status of their security is detected and managed. Non-compliance with the requirements for portable electronic devices should be detected and remote access disallowed until compliance has been met.

6.6 Contract Cleaning Services

The following security related standards are applicable to contract cleaning companies and personnel who perform services at service provider facilities and are the responsibility of SDU Physical Security:

- The contract services provider shall be required to pass the approved SP background program on all personnel assigned to SDU facilities.
- It's desirable that contract cleaning personnel assigned to service provider facilities will have completed six (6) months of successful employment with the contract services provider.
- Contract cleaning personnel can be issued a SDU contractor's badge and access control card for utilization while cleaning the facility. The access control card will be programmed for limited access during the specific hours of the cleaning activity, for example 5:00 p.m. to 11:00 p.m., weekly. Access during all other periods will be denied.
- A visitor badge must be issued to each contract cleaning personnel who do not hold a valid SDU access/photo ID badge and must be escorted by a service provider employee who holds a valid badge.
- Contract cleaning personnel will not be issued a master key, etc., which would allow the user to bypass the perimeter access control system.

6.7 Electronic Security / Physical Security for Sacramento Facility

The electronic and physical security will be established to limit unauthorized access to restricted areas and provide separation between general office, visitor, and break areas to secure production area. Cameras will be positioned to view activity at all doors leaving the protected area, along with specific security areas called out below.

6.7.1 Secure Areas:

6.7.1.1 Dock

Secure the area with an interlock that creates an interior and exterior barrier wall so that doors on the exterior and interior cannot be open at the same time. Overhead doors will be controlled by electric operator and interfaced to security system for override with interlock.

Provide delay egress maglock on interior dock doors and or emergency override with sounder as allowed by code for exiting facility in an emergency.

If allowed by local code installation of delay egress maglock will be used in addition to mechanical locking hardware

6.7.2 ADA (by revolving door) & Emergency Exit Doors

Will have card readers to control entry and exit along with door contact connected to local annunciator and connected back to security headend for remote annunciation of alarms. This door will be programmed to work for only those people with a need for ADA assistance

Door will be equipped with door closer, mechanical locking hardware and exterior trim that works in conjunction with fail secure electric lock to allow access from outside protected area for ADA. Interface to handicap operator if provided.

Additionally, Emergency Exit doors (defined as a door on the perimeter of the secured facility used for exit only) will be equipped with an alarm system which will sound upon unauthorized exit and must be manually reset by authorized representative.

6.7.3 Main Entry (Location to receive visitors)

Construction of walls from building floor to deck above, security screen or hard lid ceiling construction will be needed.

6.7.4 Safe Room (Room used for the storage of cash, checks or other notes of financial value)

Room will be constructed of concrete, concrete block or two layers of drywall with security mesh between. The walls will be constructed from structural floor to deck above or hard lid ceiling consisting of at a minimum two layers drywall with security mesh between.

6.7.5 Areas Controlled By Card Reader Access

- Entry from Outside into Vestibule or Lobby
- Entry through the Security Revolving Door
- Entry through the ADA door (both sides of door) next to the Security Revolving Door
- Entry from Lobby to Office and or Production Area
- Entry to LAN/Computer Room (Combination Keypad/Card Reader)
- Entry to IDF Room (Combination Keypad/Card Reader)
- Entry to Console Room (Combination Keypad/Card Reader)
- Entry to Check Printing
- Entry to Safe Room (Combination Hand Reader/Card Reader)
- Entry to HR / HR File Storage
- Entry from Dock to Secure Area
- Entry from Outside into Dock

6.7.6 Additional Security Controls

- Glass Break Detectors will be installed in all areas vulnerable to intrusion glass windows and doors.
- Motion Detectors will be installed in areas vulnerable to intrusion.
- Duress buttons installed in the following areas, Dock, Human Resources, Reception and or Security Desk.
- Floor to ceiling walls.
- Contacts will be installed on all roof hatch and other access openings.

6.7.6.1 Floor to Ceiling Walls

The SP has furnished the SDU facility with floor to ceiling walls between separated functions. Specific walls designated as floor to ceiling are located in the dock area, NDP and OPEX rooms, safe room and the IDF closet, as well as the check printing and check storage areas. These areas are self contained to meet internal controls and separation of duties.

6.7.7 Electrical / LAN / Phone / Fire Alarm Interface Requirements

All electronic security equipment and revolving door will need to be on emergency power (UPS / Generator)

- Boon Edam Revolving Doors
- Model: Tourlock 180+90

- Dimension: 6'-9" or 7'-3" O.D. x 8'-0" Nominal Height
- Fire Alarm output connection required
- Location: Each employee Entry
- Power: 208vac (200 - 240vac, 50/60Hz, 0.25kW max.)

Note: In most locations a second means to emergency egress is required.

6.7.8 Access Control Panel / Lock-Aux Power Supply (each panel controls up to 16 doors)

This unit powers all access control electronic devices to include card readers, motion detectors, and electric locks. Exception to providing power for electric locks in situations where lock requires high inrush / current to operate or require special power supply at the door.

- Location: LAN/Computer Room - Wall mounted (Allow 32" of wall space per panel from floor to ceiling per panel)
- Power: 120vac receptacle (5amp 988 BTU/hour)
- LAN: Requires network jack and static IP address to network
- Fire Alarm Output: Requires fire alarm contractor to provide normally closed dry output contact activation on general alarm

6.7.9 Radionics Control / Communicator

- Location: LAN/Computer Room - Wall mounted
- Dimension: 16.5"W x 16.5"H x 3"D
- Power: 120vac receptacle (120vac input 16vac output 40va class II transformer)
- Phone Line: Requires dedicated telephone line for communications to Central Alarm Station

Note: In most locations the keypad for servicing the system will be mounted to the door of control cabinet or on the wall

6.7.10 70" Vertical Rack (19" Equipment Rack) (if provided by security contractor will be Winsted V8801 allows 40RU)

- Location: LAN/Computer Room
- Dimension: (requires 77"H x 23"W x 28"D for rack, plus enough space in front and back to swing open doors)
- Power: Two 120vac receptacles. Rack will be equipped with two power strips for connection of equipment mounted inside
- LAN: See requirements on equipment mounted in the rack for details

6.7.11 Digital Video Recorders / Extended Storage Module (each supports up to 16 cameras)

- Location: LAN/Computer Room - Mounts in 19" equipment rack
- Power: Two-120vac receptacle (2amp 853 BTU/hour) one each for DRV and ESM
- LAN: Requires network jack and static IP address to network

Note: Extended storage module is needed to meet requirement for data storage over 90 days.

6.7.12 19" Computer Monitor/Mouse & Keyboard (supports all Digital Video Recorders through use of KVM)

- Location: LAN/Computer Room - Mounts in 19" equipment rack
- Powebr: 120vac receptacle (1.5amp 136.52 BTU/hour (maximum) and 116.04 BTU/hour (typical)

6.7.13 KVM Switch (used to switch between computers on one monitor keyboard and mouse)

- Location: LAN/Computer Room - Mounts in 19" equipment rack
- Power: 120vac receptacle (5 watts class II transformer)

6.7.14 Central Camera Power Supply (for interior cameras each supports up to 16 cameras)

- Location: LAN/Computer Room - Wall mounted
- Power: 120vac receptacle (2.2amps 264 watts and 901 BTU/hour)

6.7.15 Camera Power Supply (for exterior camera supports 1 camera each)

- Location: Provided receptacle inside building opposite camera mounting location
- Typical Camera Location: Outside to view overhead and pedestrian door at dock - Wall mounted
- Typical Camera Location: Outside on each exterior wall to provide perimeter coverage of the building - Wall mounted
- Dimension: 12"W x 16"H x 5"D (approximate wall space required)
- Power: 120vac receptacle (4.40amps 528 watts)

6.7.16 CCTV 14" Monitor (for viewing dock camera)

- Location: Inside dock area or at location responsible for receiving deliveries - Wall or Ceiling/Pendant mount
- Dimension: 14"W x 13"T x 16"D
- Power: 120vac receptacle (60watts)

6.7.17 Intercom System Door Station & Master (option to use PBX phone)

- Location: Intercom Unit - Door for Delivery Drivers at Dock wall mount unit
- Location: Intercom Master - Area responsible for receiving deliveries, on desk or wall mounted
- Power: 120vac receptacle (28watts output 12vdc 1amp max) (at intercom master location)

6.7.18 Approved Lock Hardware

All electro-mechanical locking hardware used in conjunction with access control system will be 24vdc, fail secure, exception if not allowed by code

- Von Duprin - For electric strikes (6000 Series), electric panic bar latch retraction or vertical rods and latches
- Sargent - For electric panic bar latch retraction or vertical rods and latches
- Schlage - For electrified lever sets and door hardware for mechanical lock portion (Storeroom function lever sets used in conjunction with electric strikes)
- Securitron - For standard maglocks and delay egress maglocks
- Locknetics - For delay egress maglocks

Contractor/hardware supplier will provide correct model of door hardware and locks, compatible and work in conjunction with each other as designed by the manufacture including door swing, frame size and design.

Additional hardware required:

- Storeroom function locksets or latch retraction door hardware (mechanical only) is needed for card reader doors with electric strikes.

- Latch guard is required for all doors with electric strikes that open out of the secure space and have an opening that allows tampering with door latch.
- All card reader and emergency exit doors will be equipped with automatic door closer.

Boon Edam revolving door installation, the Developer will be responsible for ADA/emergency egress door and construction around the revolving door.

The door will be purchased direct from Boon Edam, and Boon Edam will arrange for an authorized dealer/contractor to install and test the door.

Developer will be responsible for closing the gap between construction walls and revolving door once it has been set in place and final adjustments are made by Boon Edam door contractor.

7.0 COMMUNICATIONS SECURITY

7.1 OVERVIEW

Communications security involves the protection of information in transit. Transit can be constituted by logical, physical or even voice. Communication security utilizes technical methods to ensure the integrity, confidentiality, and availability of this protected information.

7.2 EXCHANGE OF INFORMATION

Exchanges of information and software between organizations will be controlled, and will be compliant with any relevant legislation.

Exchanges will be carried out on the basis of agreements. Procedures and standards to protect information and media in transit will be established. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls must be considered.

7.2.1 SECURITY OF PHYSICAL MEDIA IN TRANSIT

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. The following controls apply to safeguarding computer media being transported between sites:

- Reliable transport or couriers will be used. A list of authorized couriers will be agreed with management and a procedure to check the identification of couriers implemented.
- Packaging will be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications.
- Special controls will be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification. Examples include:
  - Use of locked containers;
  - Delivery by hand;
  - Tamper-evident packaging (which reveals any attempt to gain access);
  - In exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes;
  - Class 3, Confidential information and above must be in an encrypted form on the media in transit, i.e. tapes containing such information must be encrypted.

7.2.2 SECURITY OF DATA TRANSMISSIONS

Digital information in transit requires special attention paid to the media used for transit and the information to be transmitted. The following controls have been established and are required for data in transit:

- Encryption shall be used for transmitting sensitive information (Class 3 or above) over public networks among SP facilities and between the SP and other facilities. This includes, but is not limited to file transfers, email and messaging systems.
- Data in transit over private communication lines does not require encryption by default but all types of information associated with the SDU will fall under additional requirements for encryption based on the California SDU SOW, as well as its classification or function, i.e. Database or system administration or database information with a classification of Class 3 or above.

- Encryption is required for transmission of sensitive or transactional information for all Public Information Systems.

7.2.3 Communications Encryption Requirements

Communications encryption refers to active communications to information systems and associated applications, including database access. (i.e. Intra/Internet sites, systems administration applications, web to application server, etc.)

All applications must utilize encryption for the transmission of user credentials, passwords, financial and personally identifiable information and all other information protected by privacy and security regulations.

7.2.3.1 Communications Encryption Matrix

	Unrestricted (Class 1)	Internal (Class 2)	Confidential (Class 3)	Restricted (Class 4)
Application Access	No	No	Yes	Yes
Systems Administration	Yes	Yes	Yes	Yes
Specifics on encryption requirements can be found in *Appendix H, Encryption Requirements*. Systems Administration is defined as non-console access to information systems technology for the purpose of remotely managing the technical resource. Encryption of the data stream and its contents are always required.				

Table 7.1: Communications Encryption Matrix

7.2.4 Electronic Commerce Security

Electronic commerce can involve the use of electronic data interchange (EDI), electronic mail and online transactions across data networks between third parties. Security requirements for electronic commence will include the following controls:

- **Authentication.** All access to information classified as Internal (Class 2) or above must be authenticated by means of, at a minimum, username and password adherent to authentication requirements specified herein.
- **Authorization.** Authorization must be provided in a discretionary form and role based permissions, ensuring that only those with a need-to-know have access to the information in question.
- **Accountability.** All authorized access to information classified as Internal (Class 2) or above must include appropriate controls required to audit access to the information in question. Event logging must be inclusive enough to be able to reconstruct any event in time accurately, and in a timely fashion, in order to identify malicious activity for the purpose of forensic investigation.
- **Contract and Tendering Processes**. For non-public forms of access, i.e. access between businesses or partners requiring contractual agreements, all access must be documented, contracted, and reviewed annually.
- **Order Transactions.** Confidentiality and privacy statements, integrity of order, payment and delivery address verification, and confirmation of receipt must be provided as a part of the application design.
- **Vetting.** Vetting, or inspection of information provided for financial transactions must be verified through reasonable means to ensure that payment methods and associated purchaser are valid prior to accepting payment for any services or products.
- **Ordering.** Protection of ordering must be provided through acceptable means of encryption, integrity and confidentiality controls, means of non-repudiation, and equivalent privacy statements.
- **Liability**. Liability for fraudulent transactions must be identified and details of such terms of liability must be available to any individual conducting financial transactions.

Many of the above considerations can be addressed by the application of cryptographic techniques outlined in Section 7.4 of this Security Plan, taking into account compliance with legal requirements.

Electronic commerce arrangements between trading partners will be supported by a documented agreement which commits both parties to the agreed terms of trading, including details of authorization. Other agreements with information service and network providers may be necessary.

7.2.4.1 Security of Domain Name Services

Security of Domain Name Services (DNS) is critical to the support of all information systems since exposure of private naming and addressing could allow for simplified infrastructure mapping and potential compromise. The following policies apply to all SDU Domain Name Services:

- SDU DNS servers must be configured to disallow zone transfers to unauthorized hosts.
- External DNS server may only serve information that is publicly available, i.e. internal addresses and internal naming conventions are not allowed to pass to public networks. Authorized third party connections are excepted if such connections are privatized by use of private lines or VPN.
- Firewalls must filter traffic to and from external DNS servers for only UDP Port 53 unless authorized zone transfers are in effect. Authorized zone transfers must be restricted to TCP Port 53 between only those authorized zone transfer hosts.

7.2.4.2 Electronic Payment Processing

7.2.4.2.1 Electronic Payment Processing Security

All electronic payment (ACH and EPC) processing within the SDU Disbursements function will be coordinated with Bank of America and EPC. The Disbursements Engine will transmit ACH (PPD, CCD, and CTX) and EPC origination files via SFTP with PGP encryption ensuring the transmitted files are secure. In addition, all data stored within the Disbursements databases is encrypted with PGP encryption.

Additionally, electronic payment processing within the SDU Collections function is well protected and controls are in place to protect against fraudulent activity. Physical security controls are implemented to control whom can access physical operating areas. Systems and facilities are secured by multiple layers of security to ensure adequate protection of resources.

Defense-in-Depth ensures that access to critical resources must pass through multiple layers of security before access is granted.

- Physical Security
  - Security Presence at all Points of Entry.
  - Digital Access Cards Required.
  - CCTV Surveillance of all Entry Points and Data Centers 24x7.
  - Mantrap Entrance for Data Centers.
  - Temporary Use, Digital Access Cards Required for Data Center Access.
  - All Persons Must Pass a Background Verification Before Granted Access to SERVICE PROVIDER Facilities and Systems.

- Network Security
  - The Web Client accesses the protected web page which is continually monitored by host-based intrusion detection in real-time. Host-based IDS scans the application traffic for suspicious activity and known exploits.
  - Back-end database and application servers are further protected by a second firewall that restricts communications between specific hosts and protocols.
  - All back-end database and application servers are also protected by host-based intrusion detection.
  - Internet Routers filter out unwanted circuit-level traffic.

  - Internet Facing Firewalls filter unwanted traffic up to the application layer and check for denial-of-service attacks, spoofing, and a host of other advanced filtering techniques.

- Application Security
  - All application servers are hardened by eliminating unnecessary services, regularly applying security updates.
  - Operating systems and hosted applications must adhere to strict security policies that set requirements for accounting, authorization, and authentication.
  - System logs and alerts are continually monitored.

- Assurance
  - Prior to implementation, all systems are assessed for risks, security controls, and vulnerabilities.
  - Vulnerability assessments, penetration tests, and policy reviews may be conducted on a regular basis to meet client requirements.
  - Systems may be continually monitored for availability, performance, security, application, and system events.

- Policies and Procedures
  - Maintain strict policies for all information systems. Public exposure application requirements are most restrictive. All systems must adhere to policy requirements before production.
  - Procedures ensure that setup, configuration, and maintenance of secure systems are consistent with applicable policies throughout the system lifecycle.

7.2.4.2.2 Payment Processing Security

AccessNet Specific

Within the AccessNet environment, in addition to all other access controls, segmentation, security monitoring and filtering, there are two specific and significant controls currently in place. The first control is the requirement that all users have a Tin/Pin to access the system. Therefore, fraudulent activity would require a valid Tin/Pin to access the system. The second control is a check to verify that a user is coming from the same IP address during a session. If the IP address changes during a session, the user is disconnected immediately.

7.3 Security of Electronic Mail and Messaging

E-mail has become one of our most important methods of communicating with each other and with our clients, customers, vendors, and consultants. To maximize the benefits of this medium and minimize potential liability, the following guidelines have been developed:

7.3.1 Electronic Mail Hosting Requirements

Information systems hosting electronic mail services must comply with the following:

- Information systems hosting service provider email services, by default, fall under the classification of Confidential (Class 3), at a minimum, and must be protected in accordance to classification. Individual messages held by such system remain individually classified for the purpose of sending and receiving messages in relation to security compliance. See Section 4, *Asset Classification and Control* for additional information.
- Electronic mail transiting between SP locations must not travel over public networks unless protection of sensitive information has been established as per requirements of data in transit as specified in Section 7.2.2, *Security of Data Transmissions.*

- E-mail transiting from the Internet or external systems to service provider e-mail subscribers must be searched for malicious code and viruses at all Internet e-mail gateways. E-mail gateways must have installed and running an up-to-date version of anti-virus software. Anti-virus software on e-mail gateways must be updated within two hours of the release of a new update. In the case of the SDU, Norton Anti-Virus will be used.
- SP personnel sending or receiving e-mail via Internet or other external systems must be identified and authenticated. All e-mail sent to or from SP e-mail subscribers via the Internet or other external systems must be logged. The capability must exist for logged e-mail and attachments to be rapidly keyword searched.
- This footer must be appended to all email sent outside the SDU by the mail gateway:

> The information contained in this message may be proprietary and/or confidential, and protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the SP immediately by replying to the message and deleting it from your computer.

7.3.2 Electronic Mail User Requirements

In using the e-mail system, all employees must comply with the following guidelines:

- E-mail systems may not be used for any type of solicitation other than those directly related to business activities. This restriction includes, but is not limited to any religious, political, charitable, social, or personal purposes.
- E-mail users will not send or disclose SDU confidential or sensitive information to anyone without the need to know. Under no circumstances will the use of unencrypted Internet e-mail be used to send any SDU sensitive information to any persons.
- Sensitive information or files being transmitted by email will be encrypted, regardless of destination. Encryption is further discussed below in Section 7.4 of this Security Plan.
- Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be created, sent, or forwarded by e-mail. If an employee encounters/receives this kind of material, they are obliged to report it to their supervisor.
- Chain e-mail is a non-business related message sent to a number of people asking each recipient to send copies with the same message to a specified number of others. Employees will delete all chain e-mail and all non-business-related mass e-mail immediately upon receipt and refrain from forwarding to any other employees.
- Never alter the "From:" line or other attribute-of-origin information in e-mail. Anonymous or pseudonymous messages are forbidden.

7.3.3 Security Requirements for Messaging and Web Conferencing Systems

Chat, instant messaging, web conferencing, and all other forms of digital communication over public networks are not allowed unless authorized by Information Security and supported internally. Transmission of SDU information over public networks is not allowed unless it can be appropriately secured through acceptable forms of encryption; see *Section 7.2.2, Security of Data Transmissions*. Also, please see Section 7.5, *Protection Against Malicious Software* for acceptable use of software on service provider information systems. Messaging systems must adhere to the following requirements:

- The ISO must approve all systems/connections used to transport service provider messages prior to systems/connections becoming operational and must maintain an up-to-date

inventory of all approved systems/connections. Only approved systems/connections are permitted.

- Messages transiting from one service provider site to another may not be transported via the Internet or other external systems.
- All systems/connections to the Internet or other external systems that transport service provider messaging will be real-time monitored and controlled so that any changes in the status of systems/connections is detected and managed.
- Messages transiting from the Internet or external systems to service provider messaging subscribers must be searched for malicious code and viruses at all Internet messaging gateways. Messaging gateways must have installed and running an up-to-date version of anti-virus software. Anti-virus software on messaging gateways must be updated within two hours of the release of a new update.
- SDU personnel sending or receiving messages via Internet or other external systems must be identified and authenticated. All messages sent to or from service provider messaging subscribers via the Internet or other external systems must be logged to provide a sixty (60) day audit trail of both inbound and outbound messaging traffic. The capability must exist for logged messages and attachments to be rapidly keyword searched.
- In the event a security breach of our messaging systems/connections is detected, staff must have an incident response plan. This incident response plan must include notifications, points-of-contact, back-up procedures, and all relevant actions that are required to recover from an incident.
- Testing to validate the sufficiency of messaging security controls must be conducted at least monthly. Messaging systems/connections must employ the latest security patches, anti-virus software, and be capable of identifying any changes to existing configurations.

7.4 Cryptographic Controls

Cryptographic controls ensure that sensitive information may be transmitted and stored securely while maintaining the confidentiality and integrity of the information.

Cryptographic controls are required for information in storage or transit that meets requirements for sensitivity by means of data classification.

In addition to the encryption requirements outlined in *Appendix H, Encryption Requirements*, management schemas as defined in the sub-sections below detail the program involving cryptography.

7.4.1 Use of Cryptographic Controls

Making a decision as to whether a cryptographic solution is appropriate should be seen as part of a wider process of assessing risks and selecting controls. A risk assessment and data classification should be carried out to determine the level of protection that information should be given. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.

7.4.2 Digital Signatures

Digital signatures provide a means of validating the authenticity and integrity of electronic documents. Digital signatures can be applied to any form of document being processed electronically.

Care should be taken to protect the confidentiality of the private key. This key should be kept secret since anyone having access to this key can sign documents, e.g. payments, contracts, thereby forging the signature of the owner of that key. Integrity protection may be provided by the use of public key certificates.

The use of Digital Signature Algorithm must be used for all signatures. Cryptographic keys used for digital signatures should be different from those used for encryption.

In the United States of America, Public Law 106-229, June 30, 2000, Electronic Signatures in Global and National Commerce Act dictates that digital signatures constitute as supplement for physical signatures in the majority of cases. Please refer to this act to determine compliance with U.S. laws on digital signatures.

All SP systems employing digital signatures must adhere to industry-accepted best practices, as described in the American National Standards Institute (ANSI) X9.79, *Public Key Infrastructure Practices and Policy Framework*. ANSI X9.79 describes the process for establishing policy, for implementing a system, and for auditing the system.

7.4.2.1 Approval of Systems Employing Digital Signatures

The Information Security Officer is responsible for approving all systems employing digital signatures. The Information Security Officer reviews all systems employing digital signatures, approves the policies of each business unit, interprets adherence to policy, and resolves all disputes related to the policy. The Information Security Officer must authorize in writing all systems within the SDU employing digital signatures prior to such systems becoming operational.

7.4.2.2 Required Policy and Practices Documentation

Guidelines for establishing policy and practices documents are provided in American National Standards Institute (ANSI) X9.79, *Public Key Infrastructure Practices and Policy Framework*. The Information Security Officer must authorize in writing any changes to an operational system using digital signatures if such changes result in modifications to either the policy or practices documents. In addition, the Information Security Officer must maintain an up-to-date inventory of all systems under their responsibility that employ digital signatures.

7.4.2.3 Non-Repudiation Services

In general terms, the term "non-repudiation" crypto-technically means:

- In authentication, a service that provides proof of the integrity and origin of data, both in an unforgeable relationship, which can be verified by any third party at any time;

or,

- In authentication, an authentication that with high assurance can be asserted to be genuine, and that cannot subsequently be refuted.

Non-repudiation services should be used where it might be necessary to resolve disputes about occurrence or non-occurrence of an event or action, e.g. a dispute involving the use of a digital signature on an electronic contract or payment. They can help establish evidence to substantiate whether a particular event or action has taken place, e.g. denial of sending a digitally signed instruction using electronic mail. These services are based on the use of encryption and digital signature techniques.

7.4.2.4 Key Management

Key Management is the secure administration, implementation and use of cryptographic keys throughout their Life Cycle, which includes its generation, distribution/receipt, loading/entry, storage and archival, destruction and for some asymmetric keys, registration. Sound key management practices protect cryptographic keys from disclosure, substitution, replacement or misuse and thereby reducing the threat to cryptographic applications and decreasing business risk.

The Key Life Cycle is the same for an asymmetric private key as it is for a symmetric key, unless otherwise specified. The Key Life Cycle differs for an asymmetric public key after the key generation step.

The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services.

SP Information Security Officer is responsible for the following with regards to Key Management:

- Management of all encryption keys used to support SP operations.
- Overseeing the management of all encryption keys managed on behalf of a SP client.
- Additionally, different individuals shall be responsible for different key management related functions. These functions include, but are not limited to, key management, key custody, application development, hardware management and audit trail reviews.

The following are requirements under key management:

- Key management processes and procedures shall be sufficiently documented to enable all personnel to consistently apply the procedures, and enable the reconstruction of all related activities.
- Dual control shall be used for all key components.
- Cryptographic keys, when in multiple component or share form, shall be entrusted to and controlled by two or more key custodians.
- One key custodian shall not have access to, or knowledge of, all key component or share values.
- Physical access to cryptographic materials and equipment shall be limited to authorized individuals.
- No more than two entities shall use a symmetric key and no more than one entity shall use an asymmetric private key.
- A key used in a production system or environment shall not be used in a test or non-production system or environment.
- Keys shall only exist in one of the following forms:
  - As a clear key in a Tamper Resistant Security Module (TRSM).
  - As two or more components or shares using dual control and split knowledge.
  - Encrypted by another key of equal or greater length.

7.4.2.5 Cryptographic Strength

Keys shall be replaced prior to the time feasibly required to determine them through crypto-analysis, i.e. a dictionary attack. A key shall not be used to ensure the security or integrity of data where it is feasible to determine that key in a period of time less than the useful life of that data.

7.4.2.6 Key Generation

In order to reduce the likelihood of compromise, keys should have defined activation and deactivation dates so they can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used and the perceived risk. In addition, keys or components shall be generated using a random or pseudo-random process, a resulting asymmetric key shall be equally segmented, and the length of each component of a symmetric key shall be equivalent to the length of the resulting key.

7.4.2.7 Key Storage

Keys and their components or shares shall exist in the fewest possible locations and forms necessary to enable their effective use. Systems utilizing keys shall prevent the disclosure of any key that has been used to encipher any still-secret or confidential data with the exception of asymmetric public keys.

7.4.2.8 Key Transport

All clear-text key components or shares shall be transported either in person or via a courier. Any other means for transporting clear-text key components or shares shall be approved in writing by a SP Key Manager. Both the sending and receiving entities shall each use two or more designated key

custodians. When transporting clear-text key components or shares only bonded couriers should be used. The components or shares shall be enclosed in tamper evident packaging in addition to the courier packaging and they shall be sent either using different couriers or different days.

When transporting clear-text key components or shares in person each designated Key Custodian shall retain physical possession of the component or share during transport and the components or shares shall be enclosed in either tamper evident packaging or a security container approved by a Service Provider Key Manager.

7.4.2.9 Key Usage

Each key shall be associated with a specific protocol or set of related protocols and with only one key type. It must be unique and used for the sole purpose for which it is intended. All systems utilizing keys shall be capable of determining a key's type and identifying a key associated with more than one key type.

7.4.2.10 Key Destruction

All active instances of cryptographic keys shall be erased and destroyed at the end of the key's life cycle.

7.4.2.11 Key Compromise

Mechanisms shall exist to either prevent or ensure the detection of unauthorized attempts to disclose, access, use, modify or substitute a key or key component, or restore a key known or suspected of compromise. The following requirements pertain to the protection and mitigation of key compromise:

- All key management processes shall include a means for detecting the compromise or use of a key for unauthorized purposes.
- A compromised key shall not provide any information used to determine its replacement.
- A cryptographic key or component suspected, or known to be compromised shall be replaced. A suspected compromise includes, but is not limited to:
  - A key or component of unknown authenticity, security, or integrity.
  - A key used for more than its intended purpose.
  - A key protected by a compromised key.

7.4.2.12 Audit Trails for Key Management

All key management activities shall be logged and maintained for all actions that occur within the life cycle of cryptographic key or key components. System related activities shall also be logged. Additionally, the following apply to audit trails for key management:

- Audit trails shall be retained for a given key throughout the life and for three (3) years subsequent to the destruction and/or deletion of the key.
- Audit trails shall identify, at a minimum, when the key activity occurred, why, by whom, the key(s) involved and any hardware involved.
- Audit trails shall be secured such that only authorized persons can read them and they cannot be modified.
- Audit trails shall be reviewed at least annually.

7.4.2.13 Key Custodian Requirements

- The Information Security Officer shall designate key custodian responsibilities.
- Key Custodian credentials shall be established and validated.
- One key custodian shall not report to an individual that either is or has been a custodian of a different component or share of the same key. A custodian may report to another custodian, provided he or she, either is or has been the custodian of the same component or share, or of an unrelated key.
- Each Key Custodian shall sign a Key Management nondisclosure agreement.

7.5 Protection against Malicious Software

Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses and logic bombs.

Detection and prevention controls to protect against malicious software and appropriate user awareness procedures will be implemented. Protection against malicious software is based on security awareness, appropriate system access and change management controls.

Antivirus software for both servers and workstations is centrally managed. All virus definitions are updated on a daily basis and pushed to all clients upon arrival through a vendor proprietary secure communications channel.

7.5.1 Controls Against Malicious Software

Detection and prevention controls to protect against malicious software and appropriate user awareness procedures should be implemented. Protection against malicious software is based on security awareness, appropriate system access and change management controls.

The following controls are required for all SP information systems:

- Only company approved, certified anti-virus software that have passed professional evaluations are allowed.
- Installation and regular update of anti-virus detection and repair software to scan computers and media either as a precautionary control or on a routine basis;
- Conducting regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorized amendments should be formally investigated;
- Checking any files on electronic media of uncertain or unauthorized origin, or files received over untrusted networks, for viruses before use;
- Checking any electronic mail attachments and downloads for malicious software before use. This check may be carried out at different places, e.g. at electronic mail servers, desk top computers or when entering the network of the organization;
- Appropriate business continuity plans for recovering from virus attacks, including all necessary data and software back-up and recovery arrangements.
- Procedures to verify all information relating to malicious software, and ensure that warning bulletins are accurate and informative.

The Information Security Manager should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or anti-virus software suppliers, are used to differentiate between hoaxes and real viruses. Staff should be made aware of the problem of hoaxes and what to do on receipt of them.

7.5.1.1 Misuse of Software

All end user use of software on SP information systems must be authorized for use prior to implementation. Authorization requires Information Security coordination with supporting business units prior to use.

Users may not copy software for use on their home computers; provide copies of software to any clients or third parties; install software on any of the SP's workstations or servers; download any software from the Internet or other online service to any of the SP's workstations or servers; modify, revise, transform, recast or adapt any software; reverse-engineer, disassemble or decompile any software without prior management authorization:

Employees who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors or the Information Security Officer.

7.5.1.2 Anti-Virus Software

Anti-virus checking software must be present on all desktop personal computers (PC's). The anti-virus software will check all software, including software contained on floppies. Under no circumstances will an employee turn off or otherwise disable this software.

7.5.1.3 Eradicating Computer Viruses

If users suspect infection by a computer virus, they must stop using the involved computer and immediately contact a manager for assistance.

7.5.1.4 Use of Encryption Software

Users may not install or use encryption software on any SP computers without first obtaining written permission from the Information Security Organization. Such uses of encryption software are reviewed and approved on a user-by-user basis. Use of encryption for production systems is discussed in the cryptography standard located in *Appendix H, Encryption Requirements*.

7.5.1.5 Testing Systems Security

Unless specifically authorized, users shall not test nor attempt to compromise internal system controls.

7.5.1.6 Integrity Review

Business critical systems should be regularly checked for unauthorized or unknown file or application changes and data content modifications. Any data content that has been changed or without explanation, and any software that has had modifications or file changes without explanation should be formally investigated by Change Management under advisement with the Information Security Officer.

7.6 HHSDC Communications

All communications with the California Health and Human Services Data Center (HHSDC) must adhere to all security policies concerning the protection and transmission of sensitive information. In addition, such communications must also adhere to the following:

- TCP/IP must be utilized when communicating with the HHSDC over Wide Area Network (WAN) connections.
- The SP must utilize the WAN connection provided by the HHSDC and connect to the WAN Point of Presence established by the State at the SDU facility.

7.7 AccessNet Secure File Transfer

File manager moves files received into AccessNet between servers or externally by encrypting the file using AES 256bit encryption. FTP into/from the ftp servers requires FSecure. Moving files between servers manually, not by File Manager, requires FSecure for secure ftp. This is the case even for code moves into the environment. Sensitive data stored on AccessNet is encrypted using AES 256bit encryption or Triple DES encryption. Sensitive data displayed on a web page is masked, showing only the last 4 digits of the data. This is the case for credit card numbers, bank account numbers, and SSNs.

7.8 Telecommunications Controls

Data communication for the SDU incorporates LAN/WAN connectivity to include Intranet and Extranet access. Dual carriers have been provisioned to provide redundancy and dynamic failover. What this means is that typically there are circuits from one telephone company that serve as our primary transport, while another telephone company is then utilized for a backup circuit in the unlikely event that the primary circuit carrier has network problems.

Administration of the network devices will be limited to the Network Engineering department where 2 factor authentication will be used. The 2 factor authentication process uses two factors, typically: 'something you have' such as a digital certificate or security token, and 'something you know' such as user ID and password for authentication purposes.

A terminal server is used for console access and local authentication and the network will be monitored 24/7 by the SP monitoring group.

7.8.1 Remote Diagnostic Port Protection

Any connection from outside of the protected network that is used to access a SDU-related system for maintenance shall be protected by physical and procedural controls. This includes training authorized users, restricting use to authorized users, and maintenance of a usage access log. Additionally:

- Only a limited number of personnel shall have remote diagnostic access.
- They must be properly identified and have appropriate clearances.
- Unique User ID's must be used for each user. Users will be instructed that they must never share their ID or password.

When a vendor must have remote maintenance access for system maintenance, means shall be provided to properly identify, authenticate, and audit such access sufficiently enough to provide assurance at least equivalent to the former controlled access protection level. This may be achieved by:

- Procedural controls such as manual enabling and disabling remote access for the period of required access or
- Use of approved remote access methods, such as secure virtual private networks.

7.8.2 Use of Analog and Digital Subscriber Lines

The Service Provider Telecommunications Manager/Administrator (Telecom) must approve the use of all analog and digital subscriber lines (DSL). No analog or DSL lines shall be used for personal access to the Internet by end-users while at SP facilities unless approved by Telecom and Information Security. Additionally, the following controls apply:

- Local ISO must approve the use of all analog and DSL lines.
- Analog and DSL lines must be re-approved at least annually.
- Dial-in modems will only be used for dynamic remote access when accompanied by VPN technology, strict authentication, dial-back techniques, and third party contracts as necessary.
- Analog lines used for modems shall be controlled by class of restriction and set to outbound only unless otherwise approved by the SP Information System Manager and Information Security.
- Any access to the Service provider network and another network simultaneously by means of dynamic connectivity established through analog or DSL lines must be analyzed separately for risk determination and it may be necessary to employ split-tunneling, firewall, and/or intrusion monitoring services to prevent threats from unauthorized external access.

7.8.2.1 Analog Line Auditing Requirements

Station Management Detail Recording / Call Detail Recording must be activated on all analog lines all call records the lines generate. Call records must be maintained to provide a minimum of sixty (60) days of useful audit trail data. Telecom must maintain a record of all analog lines including ownership and business purpose. Analog lines shall be physically disconnected from the PBX when no longer needed.

7.8.3 Private Branch Exchange (PBX) Policy

Network security problems are not limited to connections to the Internet. There have been sharp increases in reported incidents of telephone system criminals skilled in programming computer systems, which access service provider telecommunications systems through remote administration or maintenance ports.

The system owner is responsible for ensuring that the validity of the security controls are tested at least annually and certified sufficient based on the controls set forth in this policy.

- Minimize the number of external connections to PBX. If external access is required, each accessing system must be authenticated. Remote access must adhere to all requirements set forth below in Section 8.13, *Mobile Computing and Remote Access.* If remote access is not required it must be disabled.
- Disable all default logins and follow policy guidelines for password management.
- All remote access to PBX must be logged to ensure there is an adequate audit trail of all access to the PBX and audit trails must contain, at a minimum, 90 days of useful audit trail data.
- Station Management Detail Recording / Call Detail Recording must be activated on all trunk groups (inbound, outbound, tie lines etc.) and activated within the system to capture all call records the PBX generates. The call records need to be sent to a call accounting software package. Call records must be maintained to provide a minimum of 90 days of useful audit trail data.
- All network-attached PBXs shall be configured to meet network security standards for authentication, access control, and logging.
- Each site that manages a PBX must determine whether the vendor is contractually responsible for fraud with respect to the PBX system.
- All network-attached PBXs shall be tested upon initial setup, each major change, and on a regular basis to ensure that the PBX has been implemented to effectively support Remote Access security standards.
- The dial-up maintenance ports on any PBX must be monitored frequently.
- The User ID of any terminated employee who has system administrator access to a PBX must be removed upon termination.
- The system files of any PBX must be backed up on a regular basis.
- Use of analog lines requires prior approval.

7.8.3.1 AMIS (Audio Messaging Interchange System) Networking and Out calling

If the AMIS networking or the Out-calling feature is activated on the voice messaging system, only Enhanced Call Transfer or Transfer to Subscriber Only can be utilized. If these features are not applicable to your specific switch and software version, then Automated Route Selection, World Class Routing (WCR), or vendor equivalent, must be implemented.

7.8.3.2 Call Forwarding Off-Net

Call "forwarding off-net" must be disabled unless otherwise approved by Telecom. Telecom must maintain an inventory of all telephones for which "call forwarding off-net" is enabled.

7.8.3.3 Voice Messaging &VRU/ARU Ports

The voice ports associated with voice messaging or voice response units will be disabled from access to external networks unless approved by management. If approved, an inventory of all such voice ports must be maintained. If calls are being routed off net from the voice response unit, then Automated Route Selection World Class Routing or vendor equivalent must be implemented.

8.0 Access Control

8.1 Overview

Access control is the method by which access to information or sensitive areas of business operations is controlled. The purpose of access control is to manage risk associated with business interruption; information misuse, loss, or interruption; or system misuse or interruption.

Business requirements dictate that each system user must be uniquely identifiable and their use monitored and audited. Access controls allow for unique identifiers, audit trails, and group based access.

8.2 Logon Banner/Screen Warning Banner

Each SDU information system must display an approved logon banner/screen warning that identifies the system as the property of the SP and is for "Authorized Use Only". In addition, it must make clear that the system is subject to monitoring, coupled with the requirement for a user's affirmative decision to accept the conditions in the banner notice by continuing to use the information system. It is recommended that the following logon banner be utilized:

> **WARNING! THIS SYSTEM IS FOR AUTHORIZED USE ONLY!** The information on this computer and network is the property of a private corporation and is protected by intellectual property rights. You must be assigned an account on this computer to access information and are only allowed to access information as defined by the system administrators. Use of service provider resources should be for business purposes only and should be in compliance with the Code of Conduct and service provider policies and procedures. As the property of a private corporation, your activities may be monitored and/or recorded and you should have no expectation of privacy on this computer and its networks. All actions are monitored and recorded. Use of this computer implies consent to monitoring.

Figure 8.1: Logon Banner/Screen Warning Banner

8.3 Role Based Access Controls (RBAC)

Role based access controls (RBAC) are defined as controls within an authentication system based on a hierarchy of privileges assigned to groupings of individual systems and/or user accounts. RBAC simplifies security administration by using roles, hierarchies, and constraints to organize privileges. Most modern authentication systems currently utilize roles to group account permissions. Several examples that have the inherent capability available include MS Active Directory, SQL and Oracle Databases, as well as many derivatives of UNIX. RBAC has been formally defined in the American National Standard 359-2004. More information can be found about RBAC from NIST at http://csrc.nist.gov/rbac/.

- SDU authentication systems will utilize role based access controls when the system provides the capability.
- If the authentication system does not allow for RBAC, alternative systems will be investigated and a risk analysis conducted to determine the necessity.

As it pertains to the SDU, the SP will strictly follow all OCSE guidelines and standard industry policies and procedures for controlling and managing access to all SDU servers. Access to all SDU servers is viewed from the perspective of two high level groups, System Administrators and System Users.

System Administrators are the only SP team members who have the ability to administer operating systems, databases, application code and system level utilities. System Administrators are responsible for the day-to-day monitoring, maintenance, support and management of all SDU subsystems. Further information on access privileges and procedures

System Users, including all general SDU users, supervisor users, business management users, LCSA/DCSS users and public users will not be granted the capabilities to directly administer any sever operating system, database, application or system level utility. System users do have the ability to use SDU business applications on both their desktop and SDU servers. The use of applications also includes administrative functions within the application. These administrative functions are used for the purpose of manipulating business level variables, utilizing business level utilities and in some cases are given the ability to administer user access privileges.

Further information on what users have access to which systems, as well as the procedures for gaining access to each system can be found in *Appendix J – California SDU User Management Procedures*. Further information on separation of function/duty can be found in Sections 6, 11 and 12 of CDL OM 001 – Operations Management Plan.

From an SDU operations perspective, all SDU subsystems will be segregated by network segments that only allow certain groups of workstations and users to access servers on those segments. For example, collections, customer service, human resource/financial management each have their own network segments. Furthermore, production workers within the Collections workflow are further segregated from specific servers by department and role (See section 3.3 for more information).

8.3.1 Configuration Management Overview

System configuration management (CM) is a formalized methodology typified by the processes, controls, documentation, testing and implementation of system changes. These system changes are comprised of planned modifications, strategic modular updates, complete upgrades and sometimes emergency fixes to SDU software and hardware. Performing these changes in a controlled manner provides system stakeholders with the insurance that changes will not interrupt normal business operations nor cause significant productivity or financial losses,

One of the most important overriding aspects of configuration management is the concept of version control. Version control provides a given operation the structure it needs to ensure that the most valid version of a specific system component is the one being developed from, tested, approved and deployed. Version control is not only important from an independent item perspective, but is also important to ensuring that interrelated components are compatible, tested and stabilized prior to production deployment. It involves the strict processes of staging code, freezing code, managing COTS updates, and providing the controls and flexibility necessary to resolve emergency situations when they arise.

All major subsystems used by the SDU (CE, DE, CIE, Onyx, SDU IVR and SDU Web) will utilize separate system instances for development, testing and production. The following formalized processes behind our CM program govern the basic steps common to all CM efforts;

- **Baseline** – The baseline is the concept of an agreed upon, properly tested, properly deployed, stable starting point
- **Change Mechanism** – Is the reason and processes associated with initiating any form of system change
- **Planning** – Is the process of defining how a change will be built, controlled and implemented in an organized and timely manner
- **Design** – Includes the broad set of processes associated with analysis, requirements generation, system architecture and product determination,
- **Development** – Is the actual process of building the application, database and/or presentation mechanism identified during design. Development environments are always

physically separated from all non-unit test, test and production environments. I addition, all source code is strictly managed via Microsoft SourceSafe or some other code library management tools.

- **Unit Test** – Is the process of testing each modular unit of code prior to unit integration testing multiple related modules together. For our purpose here, unit test and unit integration test are combined in the general "Unit Test" subset. Unit testing is typically performed by developers on the development platform.
- **System Test** – Is the testing of the entire production system and all the modules that make up that system. The objective of system testing is to verify that the system functions as a whole. In most cases, system testing is performed on a separate environment than production, but there will be cases where production equipment, such as mail openers and scanners will be utilized during system testing during SDU off hours.
- **Integration Test** – Are tests performed on multiple applications or systems simultaneously. Integrated tests confirm whether computer programs function properly as they interact with other programs, often times via interface data transmissions.
- **User Acceptance Test** –Represent the level of testing where the customer/stakeholders evaluate and eventually sign-off on system functionality, stability and performance. Also represents tests which are performed with users to validate whether the remediation(s) have been done correctly and applications still function as expected.
- **Regression Test** - Selective retesting to detect faults introduced during modification of a system or system component, to verify that modifications have not caused unintended adverse effects, or to verify that a modified system or system component still meets its specified requirements. Regression testing is critical to any form of system change regardless of complexity or severity. Even when an emergency system repair is deployed a regression test plan will be created and carried out prior to resuming normal production,
- **Deploy** – The actual release of a system change into the production environment for use in normal operations.

8.4 User Identification and Authentication

All users will have a unique identifier (user ID) for their personal and sole use so that activities can subsequently be traced to the responsible individual. User IDs will not give any indication of the user's privilege level or role within the service provider.

In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used upon approval. Authorization by management will be documented for such cases within the information system's Security Assessment. Additional controls may be required to maintain accountability.

Access to information systems must only be attainable via a secure log-on process that meets all policy requirements for access control.

8.5 Network Access Control

The SP has an operational requirement to provide and manage access to information over all communications paths, both public and private. Electronically transmitted information is also considered an asset and must be protected according to its classification level.

8.5.1 Segregation of Networks

The introduction of controls within the network is required to segregate groups of information services, users, and information systems. Networks will be segmented by a combination of the following at minimum:

- Gateways and Firewalls (See Section 8.14, *Gateways and Firewalls*)

- Virtual Local Area Networks (VLANS)
- Network address segmentation and routing controls
- Private addressing, (RFC 1918)

Operational controls are in place to separate network and system administrative functions. This is controlled by separate authentication mechanisms assigning different users, roles, and groups in relation to network devices and network servers. Network and connectivity diagrams have been detailed and included in *Appendix B, Diagrams.*

8.5.2 Network Routing Control (Gateways)

Shared networks, especially those extending across organizational boundaries require the incorporation of routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.

Routing controls will be based on positive source and destination address checking mechanisms. Network address translation is also a very useful mechanism for isolating networks and preventing routes to propagate from the network of one organization into the network of another. They can be implemented in software or hardware.

8.5.3 Sensitive Information System Separation

Sensitive systems require a dedicated (isolated) computing environment, otherwise referred to as a dedicated domain. A sensitive system is any system classified as SDU-Confidential (Class 3) or SDU-Restricted (Class 4), and/or has public exposure - see Chapter 4, *Asset Classification and Control* for detailed information. The sensitivity and associated risks may indicate that the application system will run on a dedicated computer and will only share resources with trusted applications systems.

The use of Virtual Local Area Networks (VLAN's), firewalls and/or network segmentation will be used so that sensitive systems do not reside on the same subnet or network segment as other information systems of lower classification. This ensures logical domain separation.

All traffic within the SDU domain is restricted to that which is required to perform SDU services only.

Each information system must be defined by an owner and given a classification as a part of the Security Assessment process. Differing information systems may communicate as deemed necessary, but must use authorized communication channels that are adequately protected by restriction of protocols, access controls and authorization.

Access to network devices is controlled through strict access controls and centralized authentication. Where possible, devices utilize role based access controls to segment administrators from those users requiring only limited permissions. All authentication services have been centralized and utilize the RADIUS protocol to communicate with the authentication server.

Firewalls are utilized throughout the organization where connectivity to external networks has been provided. Firewalls must also be used to separate sensitive information from the applications utilizing such information and from other service provider and public information systems as defined by segmentation requirements.

The following requirements apply:

- The sensitivity of an application system will be explicitly identified and documented by the information system owner within Security Assessment documentation.
- When a sensitive application is to run in a shared environment, the applications with which it will share resources will be identified and agreed with the owner of the sensitive application.

- Public exposure and exposure to other geographically separated business units must be taken into account when considering segmentation and network security of sensitive systems.
- Sensitive information must be physically and logically separate from the application(s) that process such information. Separation must be in the form of network segmentation, physical segmentation, and network firewalls to separate the systems into a minimum of two processing tiers.
- Sensitive systems will be restricted to only one application or primary function per server.
- Access to separated environments/domains must only be granted to authorized users and must follow all policies concerning user registration and monitoring system access and use.

8.5.4 AccessNet Environment

The physical servers in AccessNet are shared by the various customers. Virtual separation is provided through the use of an Authentication, Authorization and Accounting (AAA) process, where each user on the system is assigned a roll and granted access to a client set. A SDU customer service representative (CSR) can be given access to the set of clients that they support but a CSR for a specific CA SDU function would be given access only to that particular set of CA SDU data. Each user is enrolled in AAA, given a profile and password, and the profile is assigned a roll and client access.

The profile and password permits access, the roll determines what they can do, and the client access determines which clients/functions they can work with.

8.6 Use of System Utilities

Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. It is essential that their use is restricted and tightly controlled. The following controls are required:

- Use of authentication procedures for system utilities;
- Segregation of system utilities from applications software;
- Limitation of the use of system utilities to the minimum practical number of authorized users;
- Authorization for ad hoc use of systems utilities;
- Limitation of the availability of system utilities, e.g. for the duration of an authorized change;
- Logging of all use of system utilities;
- Defining and documenting of authorization levels for system utilities;
- Removal or disablement of all unnecessary software based utilities in accordance with system hardening procedures.

8.7 Limitation of Connection Time

Restrictions on connection times will provide additional security for high-risk applications. Limiting the period during which terminal connections are allowed to computer services reduces the window of opportunity for unauthorized access. Such controls are required for sensitive computer applications, especially those with terminals installed in high-risk locations, e.g. public or external areas that are outside the organization's security management. Examples of such restrictions include:

- Using predetermined time slots, e.g. for batch file transmissions, or regular interactive sessions of short duration;
- Restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation.

8.8 User Enrollment and Registration

Formal procedures for enrolling (setting-up for access) a user on a system have been developed and will be followed when granting and revoking access to all business objects. The SDU User Enrollment Form available from your manager will be used for all user access change requests.

The following are required as a part of Enrollment/Registration procedures:

- Unique User ID's must be used for each user. Users will be instructed that they must never share their ID or password.
- Validate and communicate access grants and revoke events with the business object owner (the Information Resource or Asset Owner).
- Verify with the user's manager that the access is commensurate with the job function, providing least privilege for each user, and the access control rules of the business object.
- Require users to sign a form or statement that indicates they understand their obligations as a SDU Employee with computer and network access.
- Ensure that access right changes to all business objects (including third-party and outsourced service providers) are executed as the last step in the enrollment/registration process, after all validations and checks have been completed.
- The user's manager is required to approve and maintain a written record of all access rights and any changes.
- All temporary access shall expire on a regular interval not to exceed 180 days. This applies to regular employees (regular and Temporary), consultants and vendors. Management approval shall be required for an extension.

8.8.1 User De-Registration

Whenever a user's access requirements change to warrant removal from a particular system (i.e.: the user changes departments or job-roles and will not have access to some previous systems) or all systems (i.e.: the user leaves the service provider), a user de-registration process must be carried out. Responsibility for notification of user de-registration falls under each manager of employees that must notify human resources and system administrators of personnel changes.

- The User's Manager, in coordination with the Human Resources Department, is responsible for ensuring that access rights are revoked or changed if the user changes job functions or leaves the organization.

8.9 Privilege Management

A privilege is any feature or facility of any system that enables a user to override system or application controls.

The following are required as a part of user and system privilege management:

- User access rights are reviewed regularly (minimally on a semi-annual basis, or after any changes to the access control rules of the business object).
- Systems and services (applications) accessing other systems will be subject to the same privilege management process as users. System privileges will be reviewed regularly (minimally on a semi-annual basis, or after any changes to the access control rules of the underlying platform).
- System administrators, or any user and/or system (including applications and services) that have special privileges will be reviewed more frequently (minimally on a quarterly basis, or after any changes to the access control rules of the business object).
- Access control rules and business objects must be checked at regular intervals to ensure unauthorized privileges have not been obtained.

8.10 Group Accounts

Group accounts by definition are a password or a User ID and password that is shared among a group of more than one user. While this is a violation of policies requiring unique user identifiers it is necessary to employ group accounts in certain situations.

Systems monitoring services within the AccessNet environment utilize a group account for system monitoring so that rotating employees assigned responsibility for systems monitoring on a read-only basis may login universally. This is the only allowed exception to policies concerning unique user identifiers.

8.11 Passwords

Controlling access to SDU systems is essential; both to protect the SDU's information resources and to protect personal privacy. This need becomes increasingly vital as the systems are entrusted with more sensitive and valuable information.

All users and information systems must adhere to the SP standard for password composition, change, and password uniqueness.

Password security extends to the functional screen level for all SDU applications where segregation of duty, security and privacy come into play. Appendix J, section J.12, demonstrates the functional levels of control that are present within each SDU subsystem. Each SDU subsystem was specifically designed to directly address the concept of least privileges and thus minimize information access and maximize system stability.

Administrators of passwords and authentication systems must adhere to policies regarding segregation of duties to limit the delegation and maintenance of the password system to a select number of user account administrators. For all SDU subsystems, the SP will designate a limited group of user account administrators for the SDU network and for each SDU subsystem. From a network user account perspective, all authentication creation, management and termination processes and events occur within the SP Network Engineering Group. As it pertains to all SDU application subsystems, all accounts are centrally managed through the SDU Technical Manager's office.

System Administration accounts on each application are controlled and managed directly by the SDU Technical Manager.

All General User accounts are controlled and managed by the SDU System Administrator.

Further information on the procedures for managing access to the network and each SDU subsystem can be found in *Appendix J – California SDU User Management Procedures*.

8.11.1 Password Policy

Procedures must be used to ensure that only the password owner and the information system the user uses/operates knows the password.

- Passwords shall be a *minimum length of eight (8) characters* in a combination of alpha, numeric, or special characters. The only exceptions to this rule are legacy systems that may not natively have the capability to implement defined minimums.
- Passwords must meet complexity requirements as determined by the ability of the authenticating application. All passwords must utilize, at a minimum, lowercase AND uppercase characters and at least a single numeric character with no repeating characters.

- Regular changing of passwords shall be systemically enforced, where possible. Passwords shall be changed at least every sixty (60) days, whenever a compromise is suspected, or when an individual with knowledge of passwords is terminated or otherwise has no further need for the information accessible by the use the password.
- Authentication mechanisms must employ account lockout with no more than five (5) incorrect passwords before user account lockout occurs. Accounts must be suspended until reset by an administrator or for duration of no longer than thirty (30) minutes.
- Temporary or initial passwords must be forced to change upon first logon. All temporary or initial passwords must equally meet all requirements set herein.
- The system shall automatically suppress or fully blot out the clear-text representation of the password on the data entry device.
- The system shall block out any demonstration of password length (i.e., the cursor shall not move during input), *if so allowed by the authenticating application*.
- Procedures and controls must be established to immediately disable passwords and remove user access (after a specified period of time) when an authorized user no longer needs access to the system.
- The system shall provide a mechanism that notifies the user to change their password.
- Passwords shall not be reusable by the same individual for a minimum period of at least six months and/or five unique successive passwords.
- Forgotten passwords shall be replaced, not reissued.
- Users shall not share passwords, in any way.
- The system, by default, shall not allow use of null passwords.
- All vendor supplied passwords, including those for software packages and maintenance accounts, shall be changed upon installation.
- Passwords shall not be allowed to change within a minimum of 24 hours.

Additionally, when creating security parameters applications must ensure that tables containing passwords and/or restricted information are encrypted when stored or transmitted, if so allowed by the authenticating mechanism.

Additional guidance on passwords can be found in FIPS PUB 112, Standard on Password Usage, and in CSC-STD-002-85, Department of Defense Password Management Guideline, and the Rainbow Series.

8.11.2 Group Account/Password Prohibition

A group account/password is a password or a User ID and password that is shared among a group of more than one user. The Information Security Organization prohibits the use of group accounts and associated passwords, unless the CIO has granted a formal exception.

Group account and associated passwords assigned to system process or under third party agreements are allowed as necessary, but their use is highly discouraged and must follow all other guidelines for usage.

8.11.3 Account Locking

Authentication mechanisms must employ account lockout with no more than five (5) incorrect passwords before user account lockout occurs. Accounts must be suspended until reset by an administrator or for duration of no longer than thirty (30) minutes.

8.11.4 Password Management System

Password management systems will provide an effective, interactive facility which ensures quality passwords (see Section 8.11 for guidance on use of passwords).

An approved password management system shall:

- Enforce the use of individual passwords to maintain accountability;
- Where appropriate, allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
- Enforce passwords that meet or exceed policy requirements;
- Where users maintain their own passwords, enforce regular password changes;
- Where users select passwords, force them to change temporary passwords at the first log-on;
- Maintain a record of previous user passwords. A minimum of five(5) remembered passwords and to prevent re-use;
- Not display passwords on the screen when being entered;
- Store password files separately from application system data;
- Store passwords in encrypted form using a one-way encryption algorithm;
- Alter default vendor passwords following installation of software;
- Inactive sessions for more than 15 minutes of inactivity must require re-authentication.

8.12 Unattended User Equipment

The SP maintains a clear desk policy to prevent sensitive information from unauthorized disclosure. The following controls must be adhered to for all personnel with access to sensitive information:

- Where appropriate, paper and computer media must be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.
- Sensitive information, when printed, shall be cleared from printers immediately.

Users are made aware of the security requirements and procedures for protecting unattended equipment through the on-boarding process which includes specific training as detailed in *Appendix D: Training Matrix*. Security Awareness is reviewed and implemented by the Human Resources Manager and is updated as necessary through the addition or modification of SP or DCSS security related policies or procedures.

8.12.1 Screen Savers and Workstation Lockout

Screen saver software must be implemented that automatically locks or disconnects a workstation (includes terminals and PCs) session when inactivity thresholds are exceeded.

The maximum specified period of user inactivity must not exceed fifteen (15) minutes.

- The recommended time period for inactivity lockout is ten (10) minutes.
- The specified periods of time shall decrease as the level of sensitivity of the system accessed increases.
- Unlocking the display screen must require the user to enter a unique password.

8.13 Mobile Computing and Remote Access

The term "mobile systems" refers to any service provider information device that is in use and not in a fixed location (most commonly laptops, but it also includes PDA's, cell phones, etc., herein referred to as Portable Electronic Devices (PED's)). Throughout this policy, mobile systems may be quantified as "devices capable of mobile processing and storage of digital information", i.e. any device that is not fixed in its location and can leave a service provider physical environment.

The following controls have been established for mobile computing devices:

- Mobile computing devices require additional protection measures and must include the following:
  - Device identification mechanisms, whether software or hardware, must be capable of identifying a lost or stolen device. Identification mechanisms are required for all new mobile computing devices and must be maintained for a minimum of three years from date of purchase. For SDU purposes, the mechanism for identifying a device is multi-faceted. Each laptop is equipped with a 7 character alphanumeric combination that can be found on the bottom of the laptop (hardware), and also by entering the bios and viewing page 7 (software). In addition, devices are outfitted with an asset tag, which includes a service tag that contains a unique identification number which is maintained for the life of the device or three years from the date of purchase, whichever is longer.
  - Software firewalls capable of inspection must be employed on all mobile computing devices, when the capability exists. The ability to disable such software shall not be allowed.
  - Virus scanning software must be employed by all mobile computing devices and will be setup to automatically update virus definitions every 24 hours, at a minimum.
- The SP Information Security Group is responsible for establishing and maintaining a standard mobile computing security configuration, compliant with all policy requirements.
- All use of remote control software on any modem-connected or VPN-connected device, which is also attached to the SDU network must be approved before implementation.
- Configuration and maintenance of mobile computing devices is handled and maintained in accordance with all policies concerning patch management, system hardening, and authentication management. Specific SDU data on all approved laptops is secured/encrypted in accordance with those same policies mentioned above, as well as standard Windows XP authentication. Password protection on both a user and an operating system level is mandatory and governed by the SP Information Security Group.

8.13.1 Use of Privately Owned Mobile Computing Devices

Privately owned computers or mobile computing devices may only be used to process or store sensitive SDU information if such devices meet all the requirements set forth herein and the use is authorized by the supervisor and the SP Information Security Group.

8.13.2 Centralized Monitoring for Mobile Computing Devices

All mobile computing devices that participate in remote access to SDU networks and information systems must be monitored and controlled so that any changes in the status of their security is detected and managed. Non-compliance with the requirements for portable electronic devices will be detected and remote access disallowed until compliance has been met.

8.13.3 Remote Access

External connections provide a potential for unauthorized access to business information, e.g. access by dial-up or direct-connect methods. Therefore, access by remote users is subject to strict rules of authentication and accountability. Although remote system maintenance, monitoring activities and security functions (intrusion detection; intrusion prevention; patch installation) will occur outside of the SDU, remote access to the SDU systems at the operating system level has been disabled and is prohibited.

Authentication of remote users must be achieved using methods of strong authentication. This employs a cryptographic based technique, hardware tokens, or a challenge/response protocol. Dedicated private lines or a network user address checking facility can also be used to provide assurance of the source of connections. Strong authentication by means of acceptable two factors of authentication is required for all dynamic and/or employee based remote access.

Strong authentication is required for all SP Information Systems (Class 3) and above.

Definition of Strong Authentication

Strong authentication requires approval from the Information Security Department within each scenario that requires strong authentication. It is usually denoted by factors greater than only username and password authentication and includes two-factor, biometrics and items of personal ownership such as digital keys. To define strong authentication is reliant on variable factors of the connection, user, and information system that must be independently analyzed by Information Security prior to use.

Definition of Two-Factor Authentication

Two-Factor Authentication requires a primary factor, usually a username and password, combined with a unique secondary factor that must be related to "what you know" (username and password), "what you have" (SecureID token, certificate), or "what you are" (biometrics).

Strong Authentication for Dynamic Third Party Connections

Third party connectivity is often dynamic, for brief time periods, and usually for the purpose of remote problem diagnosis or training by an authorized vendor. The use of remote desktop services is a common requirement. The following remote access policy applies to such connection types, although two-factor authentication must be redefined as follows:

Two-Factor Authentication for dynamic third party connectivity to remote desktop services, (e.g. WebEx or Terminal Services for remote training or diagnostics) may be provided by a temporary, unique username and password combined with a SP employee that must authorize access, by means of manually accepting the remote connection and must monitor all access for the duration of connectivity. Employee presence with manual employee authorization qualifies as an acceptable form of two-factor/strong authentication.

External connectivity to Information Systems, whether as an employee or trusted partner, must adhere to the following requirements:

- The Information Security Officer must approve any implementations of a remote access device or service before production operations.
- All remote-access devices that provide authentication services shall be set to automatically logout a user account after ten (10) minutes of inactivity.
- All remote-access devices that provide authentication services shall be set to automatically disable a user account after five (5) logon failures.
- All external access to service provider information systems via public networks, (i.e., Internet or shared communications medium) must be encrypted, employing the minimum levels of encryption as specified in *Appendix H, Encryption Requirements*.
- Devices that are capable of simultaneous remote access connections to both the SDU network and any external network must be configured to meet SP standards for network security, including automatic disablement of split tunneling.
- Employee remote access must be conducted via an approved Virtual Private Networking (VPN) technology.
- Employee remote access authentication must utilize strong authentication mechanisms.
- Third parties must adhere to stipulations set forth in a Third Party Connection Agreement for all types of connectivity to service provider information systems.
- Third party connections must be assigned unique connection identifiers, authentication parameters, and must also adhere to all security requirements herein for the protection of external network connectivity.
- Temporary and/or infrequent third party connections (dynamic) must adhere to the same rules of connectivity applied to employees for remote access.

- Modems will only be used for static trusted and contracted third party connections and must follow all policies for remote access, external connectivity, access control, authentication, accounting, and passwords.
- Network attached devices that require or contain modems are permitted only if management approved and secured in accordance to security requirements presented herein.
- All devices that provide Remote Access connectivity, and/or are capable mobile usage, shall provide user identification, authentication, and audit logging in accordance with SP standards.
- Audit logs on devices that allow remote-access connectivity and/or mobile usage shall be reviewed at a minimum on a monthly basis by the Information Security Officer.
- Access controls must be used to control Remote Access-users' access to information and resources on the SDU network.

The implementation of any hardware or software that facilitates or initiates remote access connections to the SDU network shall be controlled and monitored under the following minimum requirements:

- User identification and authentication
- Audit trail
- Access control
- Cryptography

The remote access device's operating system journal or log shall be used to monitor all communications activity with the host to determine system and network usage and uncover intrusions.

8.14 Gateways and Firewalls

All SP information networks must be segmented by network traffic filtering devices from public networks, private networks, and third party connections. The following controls have been established to provide a baseline for secure network connectivity:

- All connections to the Internet must be protected, at minimum, by network layer gateway firewalls with application layer capabilities for common protocols that employ both extensive audit trails and real-time alarms. Certified firewall products that have passed professional evaluations such as Common Criteria 2.1 are advised.
- All trusted third party connections must have network access filtered and monitored by at least one filtering and monitoring device, i.e. firewall or router with access control lists and appropriate audit trail capabilities.
- Wide area connectivity between geographically separated business units, subsidiaries, or operating partners, or any other trusted service provider entity must be protected, at minimum, by network layer gateway firewalls with application layer capabilities for common protocols that employ both extensive audit trails and real-time alarms. Certified firewall products that have passed professional evaluations such as Common Criteria are advised.
- All firewalls must employ address spoofing controls and malicious activity deterrence for, at a minimum, Distributed/Denial of Service (D/DOS) attacks.
- Policies of default deny must be employed by all gateways/firewalls for both incoming and outgoing rules for all attached networks. No information shall pass through a gateway/firewall unless prior authorized by rules specific to, at a minimum, the network protocol to be utilized.
- Application layer inspection of protocols considered critical to the protected environment must be employed via firewall or gateway devices.
- Prohibit an external network direct public access to any system component that is storing bank account, routing, credit card holder data, and personally identifiable information.

- Implement Internet Protocol (IP) masquerading to prevent internal addresses from being translated and revealed on public networks. Use technologies such as Port Address Translation (PAT) or Network Address Translation (NAT).

8.15 Operating System Hardening

The SP Hardening Procedures are a compilation of security configuration actions and settings that "harden" operating systems. These procedures describe practices that counter common, known attacks on network installations that expose or modify user data maliciously.

Hardening by definition is the process of securing a system. This work is especially done to protect systems against attackers. This would typically include removal of unnecessary usernames or logins and the disabling or removal of unnecessary services. On a typical Windows server, one example would be the disabling of the "print spooler" as this may not be needed

The goal is to make these platforms as secure as can *reasonably and practically* be configured. Some controls may impede operational capability; therefore their use must be carefully balanced against the security they offer. The following apply to hardening requirements for SP Information Systems:

- All server based information systems must be hardened to SP standards for hardening of each operating system.
- Information Security Officer must validate that the hardening procedures are enforced on all server-based information systems.
- The hardening procedures should be reviewed every 6 months and kept up to date as new vulnerabilities are discovered.
- If available, hardening requirements shall be based on recommended best practices published by the operating system vendor or the National Security Agency (NSA)/National Institute of Standards and Technology (NIST).

The Information Security Officer is responsible for reviewing, modifying, testing, and distributing all SP platform-hardening procedures. When conditions warrant an update to existing procedures, the Lab will perform the following actions:

- Update the appropriate procedure(s) within the database;
- Perform a new build of the operating system based upon the modified procedures;
- Perform comprehensive controlled penetration testing against the platform;
- Disseminate new procedures to Information Security Officers.

Multifunction devices, (i.e., printer/fax/copier) employing local area network connectivity must be hardened prior to deployment to ensure that default passwords have been changed to meet policy requirements and all remote management services, specifically Web and SNMP management, be disabled unless absolutely required.

8.16 Master File Protection

8.16.1 AccessNet Environment

Changes to database tables, often considered the master file, require database administrator authority; a security group as specified by role based access controls. Any changes required to the design structure of the database are performed by database administrators with full authority by means of approval through the change management process. All database administrators work independent of the data processing functions.

8.17 Information Storage Devices

The SP Policy prohibits personal information storage media devices in the SDU. This includes USB, CD-RW, floppy or any other portable device used to store computer data. Violation of this policy will be treated in accordance with the SDU Incident Management Procedures in Section 10.

In addition, USB ports and Disk drives will be disabled on each system where sensitive data can be accessed or stored and port/drive access is non-essential for the completion of daily tasks.

9.0 MONITORING SYSTEM ACCESS AND USE

9.1 OVERVIEW

System and policy monitoring allows the effectiveness of adopted controls to be checked, and conformity to an access policy model to be verified. System monitoring is required for all SDU-related information systems, as well as network segments with public exposure.

At all times the State and associated agencies including the Division of Child Support Services (DCSS) has the right to request and review all audit trails and monitoring information concerning SDU processing.

9.2 INTRUSION DETECTION REQUIREMENTS

Intrusion Detection (ID) is the process of detecting inappropriate, incorrect, or anomalous activity. ID systems that operate on a host to detect malicious activity on that host are called host-based ID systems, and ID systems that operate on network data flows are called network-based ID systems.

Host-based ID (HIDS) involves loading a piece or pieces of software on the system to be monitored. The loaded software uses log files and/or the system's auditing agents as sources of data. In contrast, a network- based ID system (NIDS) monitors the traffic on its network segment as a data source.

SDU HIDS will be accomplished through Entercept which is a software solution used to monitor activity to the host system, while SDU NIDS will use NFR's intrusion detection appliance which is a hardened device that monitors network traffic.

The following requirements pertain to all intrusion detection operations:

- Operating systems will be monitored to detect deviation from access control policy and record events to provide evidence in case of security incidents.
- Network segments with direct public exposure, i.e. Internet exposure, require the use of network intrusion detection services capable of detecting and reporting potential malicious activities and relevant events that could affect the security of the organization or its customers.
- Sensitive information systems, and their associated operating systems, with a classification level of Confidential (Class 3) or above require the use of host-based intrusion detection software and/or hardware and policy monitoring software capable of detecting and reporting local policy changes.
- All intrusion detection must be centrally monitored at the designated service provider facility and centrally controlled by the local business unit so that any changes in the status of their security, as well as the service provider systems being monitored, is detected and managed.
- Testing to validate the sufficiency of staff actions as it pertains to incident handling will be tested frequently, with duration of no less than annually.
- Responsible for subscribing to the Carnegie Mellon Computer Emergency Response Team (CERT) alerting service for instant notification of reported vulnerabilities and threats.
- The Department of Child Support Service (DCSS) must be notified upon any verified exploitation of a security vulnerability that has circumvented defense mechanisms, regardless of whether the action actually caused harm or loss. DCSS will be informed within two hours of security incident discovery. The designated DCSS contact will be notified according to SP escalation procedures.

In addition, Intrusion Detection systems must provide for the following capabilities:

- **Threat Management**: Real-time management of security threats, intrusions and policy violations.
- **Analysis**: Provide a solution for the historical analysis of intrusion detection logs enabling queries and analysis of logs from a central location.
- **Information Captured**: Capture of the IP address of the source and destination of the activity, timestamps, alert names, event data, as well as the names of the related files and objects that were grounds for the alert is mandatory. Capture of User ID's, MAC addresses, process ID's, event IDs, and other appropriate information if it is available for capture.
- **Automation**: Mitigate high-risk threats through the automation of key security processes and alerts.
- **Reporting**: Report security threats, intrusions and policy violations from a central location at the local business unit for local reporting and from the designated service provider facility for service provider-wide reporting.

	Unrestricted (Class 1)	Internal (Class 2)	Confidential (Class 3)	Restricted (Class 4)
Network Intrusion	No	No	Yes	Yes
Host Intrusion	No	No	Yes	Yes
Policy Monitoring	No	No	Yes	Yes

Table 9.1: Intrusion Classifications

9.3 Audit Trail Requirements

Audit logs recording exceptions and other relevant events shall be produced, reviewed, and followed up to determine if access control mechanisms are functioning as intended and the use of computer resources is authorized. The accepted SP policy for event logging is to ensure a minimum of system data is captured and archived for the following fields:

- User ID;
- Source IP address, destination IP address, protocol, and port, if applicable;
- Dates and times for logon and log off;
- Terminal and location identity;
- Successful and rejected system access attempts;
- Successful and rejected data and resource access attempts;

In addition to the above, and where applicable, logs record all batch and real time processing activities. Such items/activities include the operator's name (user ID), errors identified, correct and actions taken. This generally applies only to relations database systems.

Event or Audit Log review will be done in accordance with the separation of duties to avoid a single area of responsibility. The logging facility will be designed with the following:

- Logging facilities will be designed to prevent tampering
- Logging facilities will record deactivation events if de-activation is possible
- Logging facilities will record event or log-file deletion

Operator Audit logs will be monitored and checked by the Operations Manager, Information Security Officer, or a departmental delegate on a monthly basis or as needed.

9.3.1 Collections Audit Log

The Collections system maintains and archives a complete history of all transaction detail including all audit and activity information. The audit trail begins at the time of initial capture for every transaction processed by the Collections system. The critical details, including; Operator ID, Date Time Stamp, Process/Procedure, Action Taken, Data Captured or Entered and Module are all captured as part of the audit trail. Following the end of each processing day, all audit and activity detail is archived to the Collections Archive DB. The detail is then accessible via an interface or directly accessible from the DB itself. All of the archived data is included in the site backup and support plan to ensure completeness and accurate data.

9.3.1.1 Extra Audit detail

Auditing

- Capture
- Data Entry
- OCR
- Exceptions
- Archive

Auditing will be performed by every component of the collections process.

When a batch is scanned in the OPEX, not only is that audited, but the Date and Time are endorsed on the back of the financial instruments as well. As soon as that batch reaches the R&L OPEX Loader application to be added to the R&L database, details about the batch are audited. Every step up to and including batch archival is audited; this includes the time of the process and the operator involved (if the process was an operator attended process). Audits include the date and time that a batch entered a process in the workflow as well as which operator worked on the batch. Activities such as changing an item type (from correspondence to a check, for example) and rejecting an item or a transaction are audited.

The system will audit all activity on all batches/ items/ transactions processed. Auditing will include the operator and date and time of the following: capture, CAR reads, data entry, exception handling, balancing, rejecting and other batch and item processes.

9.3.2 Disbursements Audit Log

The DE web interface maintains logs to record all batch and real time processing activities such as requesting a payment to be stopped or voided. All real time processing activities capture the operator's ID, action taken, and date and timestamp and is viewable through the record specific audit trail. In addition, logs are generated and maintained on the application server for all batch processing.

9.3.3 Systems Logging Review

Systems Logging refers to the frequency of administrative review of active/archived system logs to be conducted by the administrator for the system or devices within the classified information system. In addition, all operating logs must be checked against documented operating procedures.

As it pertains to the SDU operation, operating system and application security log reviews are ultimately the responsibility of the SDU Technical Manager and the SDU ISO. The act of reviewing monitoring activities and system logs is a quality assurance process that supports the 24 hour a day monitoring performed by specific technical teams within the SP organization. Table 9.2 defines the quantity of time between reviews of monitoring activities by system security classification.

	Unrestricted (Class 1)	Internal (Class 2)	Confidential (Class 3)	Restricted (Class 4)
Operating System and Application Security Logs	Monthly	Semi-Monthly	Weekly	Daily

Table 9.2: Log Review Schedule

All SDU systems that handle money, social security numbers, bank account numbers and other confidential information are classified as "restricted". See section 4.6 through 4.9 of this document for a more detailed definition of information classification. The only SDU systems that do not fall into this category are the Avaya phone system, the Onyx ticketing system and the SDU web site (not including the Electronic Payment Engine, scheduled to be implemented in May 2006).

Although the SDU Technical Manager and SDU ISO are ultimately responsible to ensure that monitoring activities are actually carried out, these activities will be performed on a daily basis by the SP System Monitoring Team which operates 24/7/365.

9.3.4 Monitoring Procedures and Areas of Risk

Procedures for monitoring use of information processing facilities are established and utilized by the SP ISO. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities will be determined by a risk assessment. Areas that will be considered include:

- Authorized access, including detail such as:
  - The user ID;
  - The date and time of key events;
  - The types of events;
  - The files accessed; and
  - The program/utilities used.
- All privileged operations, such as:
  - Use of supervisor account;
  - System start-up and stop; and
  - I/O device attachment/detachment.
- Unauthorized access attempts, such as:
  - Failed attempts;
  - Access policy violations and notifications for network gateways and firewalls;
  - System alerts or failures such as:
    - Console alerts or messages;
    - System log exceptions; and
    - Network management alarms.

9.3.5 Review of User Access Rights

To maintain effective control over access to data and information services, management will conduct a formal process at regular intervals to review users' access rights so that:

- Users' access rights are reviewed at regular intervals (a period of every six (6) months is required at a minimum) and after any significant changes.
- Authorizations for special privileged access rights will be reviewed at more frequent intervals; a period of three (3) months is required at a minimum.
- Privilege allocations must be checked at regular intervals to ensure that unauthorized privileges have not been obtained.

- All user ID's shall have the associated privileges suspended after sixty (60) days of non-use and the user ID deleted after one hundred and twenty (120) days of non-use. Authorized employee extended leave beyond thirty (30) days requires that the account be disabled and not set for deletion.

9.4 Implemented Controls for Audit Trails

9.4.1 AccessNet Environment

AccessNet is an environment for payment processing hosted by the Service Provider and is a component to SDU information processing service. Controls and statements listed herein under the header of AccessNet apply only to that environment.

There is a dedicated log server in the AccessNet environment for logging messages. These messages include errors, warnings, informational, and debug messages. There is a capability to turn messages on/off by category. Because of volume concerns, error and warning logging are turned on but info and debug messages are turned off.

This sophisticated audit trail is created, maintained and stored within the SDU logging server mechanism for all components running in the Denver data center. It is responsible for storing and reporting on activity via monitors, reports, and real-time alerts. Communication of logging and auditing alerts will be feed to the tracking subsystem via Microsoft Message Queuing (MSMQ). The SP has chosen to utilize MSMQ because the communication server has the ability to log as much information as needed to support maintenance of the application, including sending auditing messages which produce alerts. With MSMQ, the communication server can place any number of messages on a queue very quickly and never has to check back to verify that the request was processed. MSMQ provides a guaranteed message delivery system with store forward capabilities.

The system is made up of one or more multi-threaded Services that are responsible for reading messages off of the queue and processing them to a Tracking database. In the case of logging, the details are just written and stored so that administrators can utilize a program to search and view details as shown below. In the case of Auditing messages the tracking system will update the activities to the tracking database and depending on the rules defined for the audit may also generate an automated notification.

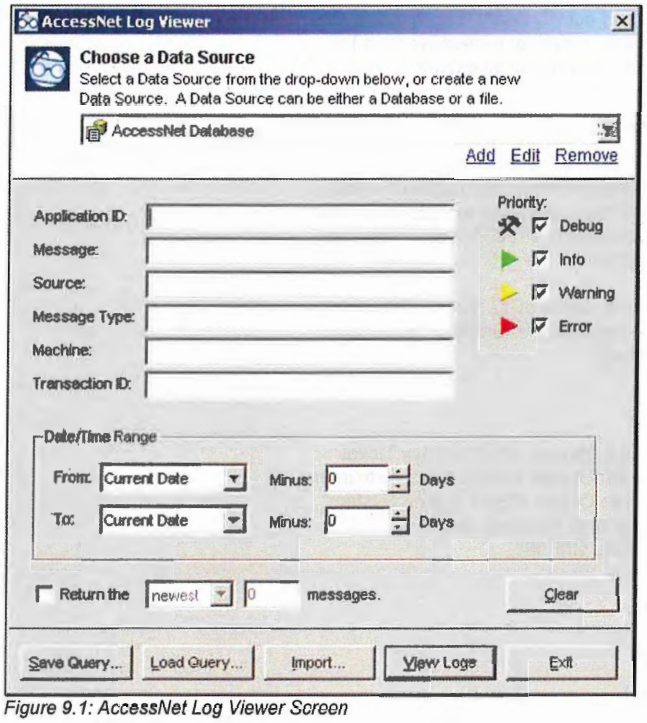


Figure 9.1: AccessNet Log Viewer Screen

There is also a dedicated stat server that records statistical messages. These include message showing the steps a payor uses to complete a payment and that they we successful.

Because of the size of this file, there are incremental backups done hourly in addition to the daily backup that is done for AccessNet as a whole. One week of daily backup are stored locally and two weeks are stored remotely. In addition, a monthly complete backup is done on the last Sunday of each month and the tape sent to remote storage for permanent retention.

Logs are incrementally backed up hourly to disk and daily to disk. The daily backup is written to tape also. Three weeks of daily backup to tape is retained, one week locally and two weeks remotely. Monthly complete tape backups occur on the last Sunday of the month and are permanently stored at a remote location.

All databases are transactional and subsequently maintain an auditable record of all changes to critical records and/or data fields inherently. Although this only applies to databases, all other transactions are recorded, at a minimum, by the SDU problem/change management system. Change records document what changes need to be made and when they will be done once approval is received.

9.4.2 Collections Environment

The Collections system maintains and archives a complete history of all transaction detail including all audit and activity information. The audit trail begins at the time of initial capture for every transaction processed by the Collections system. The critical details including; Operator ID, Date Time Stamp, Process/Procedure, Action Taken, Data Captured or Entered and Module are all captured as part of

the audit trail. Following the end of each processing day, all audit and activity detail is archived to the Collections Archive DB. The detail is then accessible via an interface or directly accessible from the DB itself. All of the archived data is included in the site backup and support plan to ensure completeness and accurate data.

9.4.3 Disbursements Environment

Delete, *Stop* and *Void* request functions, initiated through the DE web interface, are captured within a record specific audit trail. This audit trail includes a date and timestamp, along with the ID of the user who initiated the exception activity. An audit trail for batch file processing (Instruction and Response files) is captured through the Recent Activity portion of the web interface.

The SDU will retain transaction data related to Payments online for a period of 12 months following the date that the Payment was paid, stopped, voided or otherwise cancelled. Thereafter, transaction data will be retained by the service provider offline for seven (7) years.

9.4.4 Onyx Ticketing Environment

Calls received by the SDU Electronic Help Desk and the CSC will be tracked with the Onyx Ticket Tracking System to help ensure that all calls are resolved in accordance with the SLOs set forth in the SOWs, as well as provide intuitive auditing/tracking functionality. The Onyx Ticket Tracking System will monitor, track, validate and log SDU customer service and help desk functions and is further detailed within the California SDU Operations Management Plan CDL OM-001.

10.0 INCIDENT MANAGEMENT

10.1 OVERVIEW

Adequate planning is crucial in today's fast-paced, ever-changing business environment. It is essential that the SP and its Business Units have the ability to communicate and respond to potentially damaging incidents with a consistent and effective plan. This section the Plan provides the framework to identify, report, and manage all types of SDU security related incidents.

As part of standard operating procedure and in accordance with SOW requirements, security incidents are classified as high, medium, or low severity. These incidents may include fraud, theft, loss of data, physical destruction, unauthorized access to an information technology system, SDU facility intrusion, or other harm to agency activities. Security incidents will be reported in accordance with their severity classification.

OM 5.17, which states; "the SP shall report any security incidents on an urgent basis within 2 hours for all high level incidents including fraud, theft, loss of data, physical destruction, unauthorized access to an information technology system or SDU facility, intrusion, and harm to agency activities." For purposes of this Security Plan the term "High" is substituted for "urgent" which was used in the Statement of Work. In addition, the state will also be notified of all medium level incidents by the next business day. Notification will occur via a phone call and an email with an Incident Report attached (see *Appendix M, Incident Report*).

Incident Management includes, but is not limited to, response and investigation of all security related incidents that adversely affect the SP in an effort to minimize damages from security malfunctions. If there are conditions where the applicability of the standards is not clear, it is the responsibility of that individual to seek additional guidance from the Information Systems Security Group.

10.2 INCIDENT DEFINITION

An incident is defined as any event that has the potential to impact the confidentiality, integrity and/or availability of California State Disbursement Unit information, IT resources and services."

Table 10.1 provides examples of security related incidents.

Source	Description
Internal	• Security policy violations including attempts to bypass security controls • Violation of security procedures • Theft of information, data, or technology • Breach in system security • Transmission of unencrypted personal information • Misuse of SP resources that might result in a security infraction • Browsing or accessing personal information

- Intrusions
- Threats to IT resources (such as hacker threats and extortion attempts)

It is important that all incidents, regardless of the type or cause, be treated with the same methodical approach as outlined in section 10.3.3, Incident Management Procedures.

10.2.1 PERSONAL INFORMATION

"Personal information" means an individual's first name or initial and last name, plus any of the following:

- Social Security Number (SSN)
- Driver's license or state ID
- Account or card number, with any security code necessary for access to the account

If a security breach has occurred and the loss of personal information has been confirmed please refer to *Appendix K, Notice of Security Breaches*.

10.3 Incident Notification

Procedures have been developed for employees to report security incidents. The following are requirements for incident notification:

- All associates will report all incident notifications to their direct supervisor.
- All employees are required to report incidents or suspected incidents as quickly as possible.
- Procedures must be in place for managers to evaluate and escalate incidents, and to notify officials and organizations within specific timeframes.
- Report all security incidents immediately under the following conditions:
  - When there is financial exposure or a loss which exceeds $1,000.00, or
  - Incidents which are precipitated by the improper or negligent actions of a service provider employee, contract/temporary worker, or vendor services representative, or
  - Incidents that result in physical injury or harm to a service provider employee or other person.

10.3.1 Reporting of Incidents

It is the responsibility of any employee, contractor, or consultant to report suspected security incidents to their manager or security representative immediately.. Outside of normal business hours, the SP will provide a list of contacts and telephone numbers as shown in *Appendix A, Contact Lists*. Specific individuals and security representatives will be designated as "on-call" and be available to disseminate and escalate a security incident.

Appendix M, CA SDU Incident Report Form displays the report used to track and manage security incidents. *Appendix N, Computer Severity Threat Levels,* defines the criteria used to classify the severity of security incidents.

The initial notification must provide the following information, at a minimum:

- A general description of what occurred; - if appropriate,
- Characterization of perpetrator(s) thought to be involved (i.e., insider, outsider) - if appropriate,
- Corrective actions that have been taken, or that are planned, and
- Remediation Recommendations

The state will be notified within 2 hours for all high level incidents and by the next business day for all medium level incidents. Notification will occur via a phone call and an email with an Incident Report attached (see *Appendix M, CA SDU Incident Report Form*).

10.3.1.1 Anonymous Incident Reporting

Incidents may be reported anonymously if requested by the person reporting the incident. This policy is necessary because some incidents may result in administrative and/or legal action. To ensure that employees feel safe reporting such information, these reports may be done anonymously. Persons reporting such incidents are encouraged to use their name so investigators may contact them for

details, but are not required. If they choose to provide their name but still want anonymity they can request that their name not be published in any reports.

10.3.1.2 Procedure Override Authority

This policy allows the Information Security Officer to change or institute alternative procedures to deal with the uniqueness of each incident. It states, simply, that if situation dictates a need to change any procedure already documented, the SP Information Security Officer may do so. Any changes or alternative procedures used must be reviewed in accordance with section 10.4.8.

10.3.1.3 Reporting Incidents to Outside Agencies

Only the State of California under the auspice of Information Security representation and Bank of America may authorize the reporting of security incidents to outside agencies. These positions have the authority to delegate this responsibility on a case-by-case basis. The SP ISO will provide periodic updates throughout the investigation to allow for the earliest possible contacting of outside agencies when and if the security incident warrants it. In other words, reporting of incidents to outside agencies by the SP will occur only with State authorization unless the incident requires immediate law enforcement response.

A contact list containing contacts for law enforcement agencies, regulatory bodies, information services providers and telecommunications operators is maintained for use in incident reporting. All significant contact information is contained in the appropriate security and operations manuals provided to all SDU Managers and Supervisors.

10.3.1.4 Notifying Clients or Customers

Only the State of California under the auspice of Information Security and Bank of America may authorize the reporting of security incidents to clients or customers. Specific laws may require notifying clients or consumer customers. Many external standards also require notice to clients and/or consumers of security breaches. While not defined herein, procedures for proper notification under such circumstances are required and must be adhered to in accordance with the law.

10.3.1.5 Security Incident Database

The SP Information Security Group maintains a comprehensive database of service provider-wide security incidents for tracking and historical review purposes.

10.3.2 Isolation of Incidents

System and Network administrators will take necessary action to limit the effects of an incident by isolating and defining the problem as narrowly as possible. Senior Management must approve all corrective actions.

10.4 Information Security Incident Management Procedures

This section outlines the recommended processes to follow when responding to an SDU Information Security related incident including computer crimes. A computer crime is defined as deliberate actions to steal, damage, or destroy computer data without authorization or any crime in which a computer plays an essential part. .

This section provides best practices that should serve as a guide for all security incidents, however since each incident is unique and may require different levels of action, deviation from these practices may be necessary. *Appendix M, CA SDU Incident Report Form,* displays the form that must be completed for each Medium-Level and High-Level security incidents. Table 10.2 describes the general procedures for incident reporting for all IT security personnel.

General Incident Reporting Procedures
1. Characterize the IT security incident as: a. Physical incidents b. Incidents that break a law (e.g. child pornography) c. All other IT security incidents 2. Gather information about the incident and systems. Use the Incident Report Form displayed in *Appendix M, CA SDU Incident Report Form.* 3. Analyze the threat level using the criteria defined in *Appendix N, Computer Security Threat Levels.* (High, Medium or Low) 4. Report the incident. a. Report physical incidents to the law enforcement entity responsible for your facility. b. Report incidents that break a law to law enforcement. c. Report all other IT computer security incidents to your local supervisor or directly to the site manager. 5. Follow the instructions from the entity that the incident is reported to above. 6. Eradicate 7. Recover

Table 10.2: General Incident Reporting Procedures

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Also refer to *Appendix K, Notice of Security Breaches* (as required by California law).

Details regarding the general incident reporting procedures are detailed in the following sections 10.4.1 – 10.4.8.

10.4.1 Identification/Prioritization

Identification involves determining whether or not an incident has occurred, and if one has what the nature of the incident is. Initial Identification will be the responsibility of the Point of Contact (POC). The POC (the person who initially discovers/identifies the incident) will determine whether or not the anomaly is symptomatic of an incident. This is often difficult because apparent evidences of security incidents often turn out to indicate something less---errors in system configuration or an application program, hardware failures, and, most commonly, user errors. The classifications described in *Appendix N, Computer Security Threat Levels* , offer general guidance on classifying an information security incident.

Table 10.3 describes the required response time for each security threat level as it relates to IT incidents.

Threat Level	Response Time
High	<1 Day
Medium	3 –7 Days
Low	7 –30 Days

Table 10.3: Threat Level Response Times for IT Incidents

10.4.2 Initial Impact Analysis

After a Security Event has been reported and the event has been classified, the next step is to determine the initial Level of Consequence or Impact. The level of consequence of a Security Event usually increases relative to the severity of the event. At this point, the escalation POC (usually the Information Security Officer) POC must gather information from the Notification Party and determine the initial impact to the organization.

10.4.3 Containment

Containment, the third stage of responding to incidents, involves limiting the scope and magnitude of an incident. It is the first priority to restore systems to an operational state but equally important is that the restore is accomplished in a manner that will allow the preservation of evidence. The Information Security Officer will work with the appropriate individuals or groups (and possibly law enforcement) to determine if forensic evidence will be required for particular incident. If the determination has already been made that administrative and/or legal action will be likely, the inspection and preservation of information systems should be completed, as well as perform due diligence to aid in a legal investigation.

10.4.4 Eradication

Eradicating an incident includes removing the cause of the incident. In the case of a virus incident, eradication simply requires removing the virus from all systems and media (e.g., floppy disks), usually by using virus eradication software. In the case of a network intrusion, eradication is more ambiguous. Network intrusions are best eradicated by removing the any access the intruder may have/had been using to gain access. This could be accomplished by restricting the violator's IP address from the internal network.

10.4.5 Recovery

Recovery means restoring a system to its normal mission status. In the case of relatively simple incidents (such as attempted but unsuccessful intrusions into systems), recovery requires only assurance that the incident did not in any way affect system software or data stored on the system. In the case of complex incidents, such as malicious code planted by insiders, recovery may require a complete restore operation from backups. In this case it is essential to first determine the integrity of the backup itself. Once the restore has been performed, it is also essential to verify that the restore operation was successful and that the system is back to its normal condition.

10.4.6 Damage Analysis

The Damage Analysis activities are to be initiated immediately after the Recovery Operations plan has been activated. The Information Security Officer will determine if the event is confined to one area or if multiple systems/areas are involved. The Information Security Officer will also work with any additional resources necessary to determine any monetary damages resulting from the event.

10.4.7 Post Event Impact Analysis

As part of the aftermath of recovering from the event, a formal analysis of the Impact to the business caused by the event should be completed. This analysis should take into account the approximate costs of recovery, including money spent on recovery services and equipment, cost of salaries/wages of people involved in recovery operations, and any other costs or losses of revenues incurred during the event.

In addition to monetary costs, a loss of productivity analysis should be completed. All managers of business areas impacted by the security event should be contacted to estimate the loss of productivity as a result of the event. A Reputation impact analysis should also be included in the post Event Impact analysis.

10.4.8 Lessons-Learned Analysis

The POC and Information Security Officer are responsible for scheduling a post-Security Event "Lessons-Learned" meeting with the appropriate personnel (typically this would include all involved with the event, any business processes or systems impacted by the event, and members of senior

management and the State). All circumstances that contributed to the Security Event should be considered during the analysis. Any circumstances that are part of the business or within the control of the business should be considered and changed if possible to prevent future events.

10.5 Reporting Security Weaknesses

Users of information services are required to note and report any observed or suspected security weaknesses in, or threats to, systems or services. They will report these matters either to their management or directly to their service provider as quickly as possible. Users will not, in any circumstances, attempt to prove a suspected weakness.

OM 5.17, which states; "the SP shall report any security incidents on an urgent basis within 2 hours for all high level incidents including fraud, theft, loss of data, physical destruction, unauthorized access to an information technology system or SDU facility, intrusion, and harm to agency activities." For purposes of this Security Plan the term "High" is substituted for "urgent" which was used in the Statement of Work. In addition, the state will also be notified of all medium level incidents by the next business day. Notification will occur via a phone call and an email with an Incident Report attached (see *Appendix M, Incident Report*).

10.5.1 Reporting Software Malfunctions

All software malfunctions will be reported to the local departments responsible for management and administration of desktops and/or servers. Procedures will be developed to respond to software malfunctions that appear potentially malicious in nature. The following actions will be considered:

- Document the symptoms of the problem and any messages appearing on the screen.
- The computer will be isolated, if possible, and use of it will be stopped. Equipment is to be examined; it will be disconnected from any organizational networks before being re-powered. Diskettes will not be transferred to other computers.
- The matter will be reported immediately to management. Users will not attempt to remove the suspected software unless authorized to do so.

10.5.2 Learning from Incidents

There will be mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored. This information will be used to identify recurring or high impact incidents or malfunctions.

10.6 Non-Information Security Incident Management Procedures

The following Incident Management responsibilities and procedures are required to ensure a quick, effective and orderly response to non IT incidents. These guidelines outline procedures for incident handling, and provides details regarding the content and type of incident management.

Procedures shall cover all potential types of non-information security incidents, including:

- Violation of Security Procedures
- Facility Maintenance Issues
- Physical Security Breach
- Vandalism
- Violence

In addition to normal contingency plans the procedures also cover:

- Analysis and identification of the cause of the incident;
- Planning and implementation of remedies to prevent recurrence, if necessary;
- Collection of audit trails and similar evidence;
- Communication with those affected by or involved with recovery from the incident; and
- Reporting the action to the appropriate authority.

Audit trails and similar evidence shall be collected and secured, as appropriate, for:

- Internal problem analysis;
- Use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation; and
- Negotiating for compensation from software and service suppliers.

Action to recover from security breaches is carefully and formally controlled. The procedures shall ensure that:

- Only clearly identified and authorized staff are allowed access to live systems and data;
- All emergency actions taken are documented in detail;
- Emergency action is reported to management and reviewed in an orderly manner; and

- The integrity of business systems and controls is confirmed with minimal delay.

10.6.1 Determining if a Violation has Occurred, and the Severity of the Violation

In general, a security violation is brought to the attention of Management, Human Resources, and Security personnel. The violation is investigated by Human Resources and Security to determine if a violation has actually occurred, the level of severity, and the parties involved.

Table 10.2 in Section 10.4 describes the General Incident Reporting Procedures for all security personnel, including non-information security incidents.

Table 10.4 provides examples of severity levels for non-IT incident security threats.

Classification	Definition and Guidelines
High-Level	High-Level Events are the most serious Events and considered "Major" in nature. Because of the gravity of the situation and the high potential for harm to SDU, these incidents should be handled as soon as possible. High-Level Non IT Events Include but are not limited to: • Physical Violence that requires law enforcement • Property Destruction related to a Security Event (greater than an estimated value of $1000) • Personal Theft related to a Security Incident (greater than an estimated value of $1000)
Medium-Level	Medium-Level Events are more serious and the notification/handling should begin the same day as the occurrence. The decision to escalate is up to the Point of Contact (POC), depending on the Impact of the Intrusion. Medium-Level Non IT Events include but are not limited to: • Unfriendly Employee Termination • Violation of Privileged Access • Vandalism • Property Destruction related to a Security Event (less than an estimated value of $1000) • Personal Theft related to a Security Incident (less than an estimated value of $1000)
Low-Level	Low-Level events are the least severe and should be handled within one working day after the event occurs by the incident response team. Escalation is rarely necessary and can usually be resolved by the incident response team Point of Contact: Low-Level Non IT Events include but are not limited to: • Loss of Access Badge • Maintenance Issue • Violation of clear desk policy

Table 10.4: Classification of Severity Levels for Non IT Incidents

Table 10.5 describes the required response time for each severity level as it relates to non IT incidents.

Threat Level	Response Time
High	<1 Day
Medium	3 –7 Days
Low	7 –30 Days

Table 10.5: Threat Level Response Times for Non IT Incidents

10.6.2 Disciplinary Process

Depending on the severity of the incident and prior incidents, employees can be reprimanded by the following means:

1. Verbal Warning/Written Warning:
   - Instruction given to the employee by their manager detailing proper procedures and consequences for future violations.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

2. Improvement Action Plan (IAP):
   - The IAP documents the conduct or performance issue and provides a plan and time limit for corrective action. Throughout the course of the IAP, the employee and supervisor review the employee's progress. If the employee corrects all performance issues outlined in the IAP, then the employee is removed from corrective action and the IAP remains in the employee file. If the employee fails to correct the performance issues, the IAP may either be extended or the employee may be terminated, depending on the severity of performance deficiency.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

3. Suspension/Termination:
   - Depending on the severity of the incident and/or past occurrences employees may be suspended and/or terminated. Human Resources will make the final determination as to whether an employee will be terminated. Legal counsel may be involved in the decision as well.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

All documentation must be maintained and stored in the employee's personnel file for future reference, as well as follow up on employee performance. At the SP's discretion, additional security controls may be placed on employees involved in security incidents.

11.0 Disaster Recovery & Business Continuity

11.1 Overview

The possibility of a serious interruption to the SP's ability to provide services to its customers is too significant to ignore. It would be unwise to assume that the SDU will never experience a major service interruption. Consequently, it is reasonable and prudent to guard against potential disasters and prepare plans that will enable the business areas to recover from such disruptions and resume business functions in a timely fashion. It is critical to note and understand that Disaster Recovery Planning focuses on the recovery of technical resources and Business Continuity Planning focuses on the recovery of business services that dictate the order of recovery of technical resources.

The objective of this Business Continuity and Disaster Recovery is to provide a framework within which the individual business areas, operating companies, and the SP as a whole can achieve:

- Prevention – Minimize the probability of business interruptions by integrating safeguards into business-as-usual (BAU) operations.
- Containment – Minimize the impact of any business interruption through a focus on keeping the business running at the highest level of service possible; and
- Recovery – Ensure a prompt restoration of normal operations following any incident that gives rise to a business interruption.

11.2 Data Storage and Backup Methodologies

Although we provide a high level overview of data storage and backup methodologies here, the detailed storage and backup methodologies (and procedures) can be found in the OM 005 – SDU Disaster Recovery Plan. This document will cover timing/frequency of data and program file backups, and will summarize specific information about each entity that is part of the collection of services provided by the SP. In addition, details guidelines on data retention can be found in 4.9.2 – Data Retention Requirements of this document.

Hot backup to disk is performed daily with the logging system being backed up hourly to disk due to the size of that database. The daily backups are moved off to tape each day. Three weeks of daily backups on tape are retained; one week is maintained locally and two weeks are maintained at a remote site. In addition, a complete backup is taken on the last Sunday of each month and sent to remote storage and retained for the life of the contract.

The data storage and recovery strategy is designed to support the SDU within the specified recovery time objectives with minimal data loss. The SP owns an off-site recovery facility know as CommSite2 where critical data for systems is recovered and replicated to storage subsystems. This process ensures that data is moved from the primary site to the secure secondary recovery location as quickly as possible. In the event of a disaster, the replicated storage subsystems are attached to a recovery server.

The plan is to recover non-mirrored data utilizing a tape based recovery strategy. Data copied to virtual tape systems in production are offloaded to virtual tape in the recovery site on a scheduled basis. Automated tape libraries at the recovery center are populated with less critical tapes shipped from the SP storage site at the time of disaster. Monitoring tools are in place to regularly evaluate criticality of all production files.

Backup process will be put in place to meet the data recovery and restoration objectives of the SDU. Data backup strategies will determine the timeframes, technologies, media and offsite storage of the backups and will ensure that recovery point objectives can be met.

Systems are backed up to enterprise class tape media which are rotated offsite to a third party data storage vendor on a regularly scheduled basis. These tapes will be utilized to restore the environment in case of a disaster. The remaining files of the distributed systems are replicated to virtual tape over the Storage Area Network (SAN) at the recovery site. The specific method of recovery will be based on SDU requirements.

11.3 Security Infrastructure

The logical and physical security infrastructure for operations at each disaster recovery site varies. Variances are outlined in the SDU Disaster Recovery Plan, CDL OM 005. We will use the production security plan as our guide.

11.4 Media Protection

Media is secured and protected on-site and off-site utilizing industry accepted practices. Controls are in place at both the on-site and off-site facilities to ensure controlled access to backed up data in compliance with all policies concerning information labeling and handling.

12.0 EXTERNAL DEPENDENCIES

It will be necessary for the SP to maintain close relationships with all CCSAS business partners throughout the SDU implementation and operation lifecycles. From a security perspective, these relationships will primarily be focused on either the communication of SDU security infrastructure events or data exchanges with all of our CCSAS data exchange partners. In addition, it will be important for the SP to synchronize our security efforts with all relative CCSAS entities, more specifically for us to coordinate documented efforts with the CCSAS BP's CDL TM078-01 CSE System Security Plan.

The following table outlines the security related touch points with each CCSAS entity that will have an ongoing relationship with the SP.

CCSAS Entity	Security Relationship
DCSS	The DCSS will maintain the role of primary communication point for all SDU security related documentation, management and events. In all cases, the SP will first communicate security events to the DCSS prior to communicating the specific event to any other CCSAS partner or external to the SP Team
FTB	As the primary project partner to DCSS during CCSAS implementation, the SP may at times be directed to work with FTB staff to discuss and resolve security issues. The SP will maintain that security issues be communicated through the DCSS directed paths, but the SP recognizes that this communication flow may include FTB employees and entities
HHSDC	As part of the HHSDC WAN, the SP will be required to maintain or co-maintain security related components that allow for ingress and egress traffic between the SDU and other CCSAS sub-system and individuals. The resolution of security issues will sometimes require communication between SP and HHSDC staff to resolve security issues and prevent future issues.
SWS/CSE (BP)	The SDU will have very close system and operational ties to the SWS/CSE subsystem. The SDU will exchange files with SWS/CSE on a daily basis, and SP staff will utilize SWS as a major operational tool throughout the SDU operations lifecycle. The resolution of security issues will sometimes require communication between SP and SWS/CSE staff to resolve security issues and prevent future issues
ARS	The SDU will exchange data files with ARS on a daily basis. The resolution of security issues will sometimes require communication between SP and ARS staff to resolve security issues and prevent future issues
CASES	The SDU will exchange data files with CASES on a daily basis. The resolution of security issues will sometimes require communication between SP and CASES staff to resolve security issues and prevent future issues
IDB	The SDU will exchange data files with IDB on a daily basis. The resolution of security issues will sometimes require communication between SP and IDB staff to resolve security issues and prevent future issues
CSR	The SDU will exchange data files with CSR on a daily basis. The resolution of security issues will sometimes require communication between SP and CSR staff to resolve security issues and prevent future issues

Table 12.1: Security Related Touch Points

13.0 THIRD PARTY SECURITY

13.1 OVERVIEW

A third party is defined as a separate business entity or individual with no legal association to the SP other than that of a contractual arrangement for services, is not an employee, authorized contractor, or subsidiary service provider. Examples would include clients of the SP and business partners in which physical network connectivity exists for the purpose of information exchange.

Where there is a business need for such third party access, a risk assessment will be carried out to determine security implications and control requirements. Controls will be agreed and defined in a contract with the third party.

13.2 IDENTIFICATION OF RISKS FROM THIRD PARTY ACCESS

Before access is granted to any third party requesting external connectivity, all risks of such connectivity must be evaluated and documented within the Security Plan for the system that is to be accessed by such third parties. Equally, identified risks and concerns will be noted within the connection agreement.

13.3 SECURITY REQUIREMENTS FOR THIRD PARTY ACCESS

- Logical connectivity to service provider information systems must employ the use of network traffic filtering firewalls for static connectivity, i.e. virtual circuits, leased line, static VPN.
- Logical connectivity to service provider information systems must employ the use of network intrusion detection devices to monitor traffic for suspicious activity.
- Logical connectivity to the service provider information systems through dynamic, (i.e., Infrequent or temporary connectivity to service provider networks remotely) remote access must be conducted through service provider approved Virtual Private Networks (VPN's) with a minimum of two-factor authentication.
- Legacy dynamic access via directly attached modems must follow guidelines set within for communications security, authentication, access control and third party security and must also receive written approval in the form of an exception request prior to granting third party access.
- Logical connectivity to the service provider information systems through static remote access must adhere to all requirements for third party access, (i.e. contractual agreements including NDA), plus all other requirements specified within that relate to communications security as specified throughout this policy. Equally, the data classification of the information system being accessed may require that additional access controls be employed prior to granting remote access.
- Physical access to SP Service provider facilities must follow all physical security requirements of the facility in question for approved temporary contractual access, i.e. some facilities may process restricted government information requiring all persons with physical access to complete a background investigation prior to access.
- Maintain responsibility for the connectivity, up to and including the network demarcation point. The demarcation point will be the LAN interface on the most distant SP router at which the Client Service provider connects.
- Network Address Translation (NAT) shall be utilized to conceal internal network addressing.
- It is required that the SP provides the non-SP service provider with Business Continuity and Disaster Recovery Plans for the connection, and procedures to address loss of primary service.
- Monitored access through the use of network device logging and/or intrusion detection monitors.

13.3.1 Types of Access

The type of access allowed to third parties will be explicit within written contractual agreements and associated Security Assessment addendums.

Types of access that will be considered are:

- Physical access, e.g. to offices, computer rooms, and filing cabinets;
- Logical access, e.g. to an organization's databases, and information systems. Two types of logical access exist as follows:
  - Dynamic access, e.g. infrequent or temporary logical access
  - Static access, e.g. permanent or long-term logical access

13.3.2 On-site Contractors and Temporary Employees

Third parties that are located on-site for a period of time as defined in their contract may also give rise to security weaknesses. Examples of on-site third party include:

- Hardware and software maintenance and support staff
- Cleaning, catering and other outsourced support services
- Student placement and other casual short-term appointments
- Consultants and temporary employees

It is essential to understand what controls are needed to administer third party access to information processing facilities. Generally, all security requirements resulting from third party access or internal controls will be reflected by a third party contract.

Access to information and information processing facilities by third parties will not be provided until a contract has been signed defining the terms for the connection or access.

13.4 Security Requirements for Third Party and Outsourcing Contracts

Arrangements involving third party access to organizational information processing facilities shall be based on a formal contract containing, or referring to, all the security requirements to ensure compliance with the organization's security policies and standards. The contract will ensure that there is no misunderstanding between the organization and the third party.

The following terms will be considered for inclusion in the contract:

- Security policy requirements specific to the type of access to be granted;
- Non-Disclosure Agreement (NDA);
- Asset protection, including:
  - Procedures to protect organizational assets, including information and software;
  - Procedures to determine whether any compromise of the assets, e.g. loss or modification of data, has occurred;
  - Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract;
  - Integrity and availability, including How the availability of services is to be maintained in the event of a disaster;
  - Restrictions on copying and disclosing information;
  - A description of each service to be made available;
- The target level of service;
- Provision for the transfer of staff where appropriate;
- The respective liabilities of the parties to the agreement;
- Intellectual Property Rights, copyright assignment and protection of any collaborative work;

- Access control agreements, covering:
  - Permitted access methods, and the control and use of unique identifiers;
  - An authorization process for user access and privileges;
  - A requirement to maintain a list of individuals authorized to use the services being made available and what their rights and privileges are with respect to such use;
- The definition of verifiable performance criteria, their monitoring and reporting;
- The right to monitor, and revoke, user activity;
- The right to audit contractual responsibilities and security posture or to have those audits carried out by a third party in respect to both the third party and the SP itself;
- The establishment of an escalation process for problem resolution; contingency arrangements will also be considered where appropriate;
- A clear and specified process of change management;
- Any required physical protection controls and mechanisms to ensure controls are followed;
- Controls to ensure protection against malicious software (see Section 7.5, *Protection Against Malicious Software, within this document);*
- What levels of physical security are to be provided for outsourced equipment;
- What arrangements will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities;
- How the integrity and confidentiality of the SP business assets are to be maintained and tested;
- Arrangements for reporting, notification and investigation of security incidents and security breaches; and
- Involvement of the third party with subcontractors.

14.0 OPERATIONS MANAGEMENT

14.1 OVERVIEW

Changes to information processing facilities and systems are controlled by a formal change management system that requires documentation of activities to be performed, potential impacts, applicable procedures, and peer review including authorized signature approval of reviewers.

14.2 DEPLOYMENT AND CONFIGURATION MANAGEMENT

All systems that process or store information assets, and the facilities in which those systems are located are subject to deployment and configuration management. The SP is in the process of completing an internal document called the SDU System Configuration Management Plan that provides further detail to the SP's approach for Configuration Management.

Anyone may request a deployment or change to an existing system. A formal request must be submitted to the owner in the case of a change request, and a formal request must be submitted to the system owner and to the SP Information Security Group in the case of a deployment or re-deployment.

A formal request for either deployment/re-deployment or configuration change must include the following information:

- Performance and capacity requirements
- Error recovery and contingency plans
- Identification of skills and resources required
- Identification of changes/system requirements
- Release plan for implementation including fallback procedures

14.2.1 CHANGE CONTROL

Change Control procedures will be used to ensure changes to applications and systems are authorized, tested, recorded, and maintained for version control.

A change management system is used to document problems and schedule code moves through Impact records. Impact records are required for any changes in the production environment and require management approval from several groups before work can proceed. Approved impact records are required for code moves and environment changes (firewall, network, etc). Monitoring is in place on all servers to detect problems and system utilization levels that may result in problems. Additional monitoring is in progress in other areas.

As part of a change control process the following controls must be adhered to:

- The SP must notify the State in advance of making any major system modifications that would have an affect on the security of the environment, service delivery or data flows. This includes, but is not limited to changes in network, facilities, infrastructure, equipment and software. Changes must not be implemented until authorized by the State.
- Developers shall not have access to production or operational systems, unless such access has been approved by the system owner and in all cases where developer access is granted to operational systems, access will be limited to read-only.
- Access to production or operational systems by development staff requires the use of secondary authentication, e.g. a "firecall" identifier, which is associated with a change control

record and used only temporarily for the purposes specified within the change control mechanism.

- Changes will never be made without proper versioning and authorization.
- Changes to operational or production systems is to be done by authorized staff only.
- All change requests and implementations shall be recorded in an audit trail.

Formal Change Control Procedures have been developed and followed for all development tasks. The procedures include, at a minimum:

- A process to ensure that changes are submitted by authorized users.
- Change Authorization processes to ensure changes are approved.
- A process to ensure all system documentation is updated in the event of a change.
- A process to ensure that implementation of the change will minimize interruption of business activities, including the business activity involved with the change.

15.0 COMPLIANCE

15.1 OVERVIEW

Compliance with all security policies and applicable laws, regulations and standards must be adhered to so that breaches of any criminal and civil law, statutes, regulatory or contractual obligations, or applicable security standards or rules is avoided.

The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements.

Advice on specific legal requirements will be sought from the SP General Counsel's Office which shall make the determination whether outside legal advisors will be consulted. Legislative requirements vary from country to country and may impose legal restrictions on information created in one country that is transmitted to another country (i.e. trans-border data flow).

15.2 SECURITY POLICY ENFORCEMENT

Security policy enforcement is a critical component to any security program. Without enforcement there is little to no effect on the SDU security posture.

Enforcement is controlled by several factors; the first being user awareness and education, followed by audit, review and subsequent sanctions. Incident reporting and forensic analysis are equally important, but often provide awareness only after an event has occurred prompting remediation.

15.2.1 TECHNICAL AUDIT REQUIREMENTS

Technical Audit is the enforcement engine for all Service Provider Information Security policies and procedures and must adhere to audit schedules for information systems set forth herein. A third party technical auditor may substitute for SP IT Audit as necessary.

Security Plans will serve as the baseline for the security of SDU information systems, and along with all applicable information security policies will serve as the basis for recurring audits of all information systems. Information system audits must confirm that the system meets the stated security controls within the information system's Security Plan and all applicable SP security documents. Additionally, Technical Audit must report on any discrepancies and assign a remediation/mitigation plan with deadlines for completion then update the Security Plan if necessary.

Moreover, OCSE will conduct an initial audit in line with SAS 55 and/or SAS 60 and in accordance with OCSE's *Guide for Auditing State Disbursement Units*. The purpose of this audit is to obtain reasonable assurance that the internal controls implemented by the IV-D agency to safeguard assets, including the recording, authorization, custody and execution of collections and the corresponding payments, are functioning effectively as intended. The Service Provider will also make use of independent auditors as described in *Section 1.4 Revision Control*, whom will perform the audits in accordance to SAS 55 and/or SAS 60.

Reviews of all SDU security policies, standards and procedures will be performed in the following areas:

- Collection Mail/Scanning
- Inbound Correspondence Processing
- Collection Data Entry
- Collection EFT Processing

- Collection – Web-based Payment Processing
- Collection Intraday Exception Processing
- Collection Balancing and Deposit Preparation
- Collection Exception (Suspense) Processing
- Collection Financial Management
- General Collection Data Processing
- Disbursement Instruction Processing
- Disbursement Check Processing
- Disbursement Electronic Processing (Direct Deposit and Electronic Payment Card)
- Disbursement Returned Items
- Disbursement Exception Processing
- Disbursement Financial Management
- Electronic Help Desk Support
- Non IV-D Customer Service Support
- Non IV-D Data Collect
- Technical –Network Engineering
- Technical – Server and Desktop Engineering
- Technical – Application Integration

15.2.1.1 Technical Audit Frequency

Information systems will be regularly checked for compliance with security implementation standards. Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. Audit frequencies are based on the date of the information system Security Plan and are dependent on the information system role and classification as defined below:

	Unrestricted (Class 1)	Internal (Class 2)	Confidential (Class 3)	Restricted (Class 4)
Internal Audit Review	None	Periodic	Periodic	Periodic
* Technical Audits will be performed as indicated in each information system's Security Assessment documentation.				

Table 15.1: Technical Audit Frequency

Additionally, the following requirements must be adhered to for all internal and third party technical audits of State Disbursement Unit processing systems and facilities:

- Audits must encompass information security, financial data and accounting practices;
- Audit documentation must be made available to the State within ten days of final report; and
- Audits must verify proper control of Child Support Program monies and data and compliance with the Guide for Auditing State Disbursement Units (OCSE DCL 02-06).

15.3 Sanctions for Non-Compliance

Failure to comply with this policy may subject the employee in question to disciplinary action up to and including termination of employment. Human Resources and management of users determines the final sanctions for non-compliance.

APPENDIX A – CONTACT LISTS

SDU CONTACT LIST

Role	Name	E-mail	Office Phone	Cell Phone
Day to Day SDU Operations				
SP Program Director	Laura Secondo	Laura.Secondo@bankofamerica.com	(916) 576-8047	(916) 201-6897
SP Site Director	Dave Viestenz	Dave.Viestenz@firstdatacorp.com	(916) 576-8874	(850) 339-2725
SP Executive Administrator	Tami Englehardt	Tami.Englehardt@bankofamerica.com	(916) 576-8868	
SP Executive Administrator	Elizabeth Callen	ecallen@fdgs.com	(916) 576-8881	
SP Control Manager (Finance)	Sabrina Clark	sclark@fdgs.com	(916) 576-8830	(916) 367-6245
SP Human Resource Manager	Angela Terry	aterry@fdgs.com		
SP Technology Manager	Matt Lenzi	mlenzi@fdgs.com	(916) 576-8828	(916) 397-3809
SP Network Engineering Lead	Noel Johnston	Noel.Johnston@firstdatacorp.com	916 576 8888	(415) 309-9480
SP Network and Desktop Lead	Chris Bailey	Chris.Baily@fdgs.com	(916) 768-6185	(916) 576-8788
SP Collection Engine Lead	Jason Dement	jdement@fdgs.com	(513) 489-9599 Ext. 142	(513) 675-7373
SP Disbursements Engine Lead	Wendy Terrien	Wendy.Terrien@firstdatacorp.com	(720) 332-3225	(720) 201-1236
SP CORE Interface Engine Lead	Kevin Winchester	kwinchester@fdgs.com	(614) 777-9029	(513) 266-8017
SP Web, IVR, Reporting Engine, Electronic Payment	Jacie Engle	jengle@fdgs.com	(513) 489-9599, Ext 106	(513)-607-1911
SP Operations Manager				
SP Collections Manager				
SP Disbursements Manager	Kevin Herman	Kevin.Herman@firstdatacorp.com	(720) 332-3521	(513) 266-8017
SP Print Facility Manager	Greg Evans	gevans@NDSC.COM		
SP Call Center Supervisor	Jeannie Pratt	jpratt@fdgs.com	(916) 576-8834	(530) 306-8157
SP Implementation/Corporate Contacts				
SP Executive Oversight	Alice Burnett	alice.burnett@bankofamerica.com	404 607-5251	678 642-0540
SP Executive Oversight	Larry Dreyer	Larry.Dreyer@bankofamerica.com	(404) 607-5656	
SP Executive Oversight	Chuck Kelso	ckelso@fdgs.com	(916) 576-8875	(704)756-6633
SP Executive Oversight	Mike Bloomfield	mbloomfield@fdgs.com	(916) 576-8861	(303) 725-1362
SP Disaster Recovery Oversight	Debbie Breen	Debbie.Breen@firstdatacorp.com	(631) 683-7001	
SP Business Continuity Oversight	Tom Austin	Tom.Austin@firstdatacorp.com	(303)967-8330	

Role	Name	E-mail	Office Phone	Cell Phone
SP Security Oversight	Sheryl Rose	Sherly.Rose@firstdatacorp.com	(303) 967-7141	
SP Information Security Officer	Rick Reed	Rick.Reed@firstdatacorp.com	(402)-777-3019	
SP Physical Security Lead	Adam Stanislaus	Adam.Stanislaus@firstdatacorp.com	(913) 940 1997	
SP Non IV-D System Lead	Frank He	fhe@fdgs.com	(513) 489-9599, Ext 106	
SP Telecommunications Lead	Tim Cahill	Tim.Cahill@firstdatacorp.com	(303) 967-7888	

Table A.1: SDU Contact List

CCSAS Contact List

Role	Lead Name	E-mail	Office Phone	Cell Phone
DCSS SDU Operations Manager	Audrey Mozaffari	Audrey.Mozaffari@dcss.ca.gov	(916) 464-5602	
DCSS Security Lead	Mike Kanemoto	Mike.Kanemoto@dcss.ca.gov	(916) 464-5392	
FTB Security Lead	Gary Canon	Gary.Canon@ftb.ca.gov	(916) 290-8728	
HHSDC Security Lead	NetWork Operations Center		(916) 739-7640	
SWS Project Lead Executive	Peggy Anthony		(916) 290-8703	
SWS Development Lead	John Nichols		(916) 290-8842	
SWS Security Lead	Susan Forbes		(916) 290-8851	
SWS Interface Lead	Greg Gromer		(916) 290-8793	
CASES Project Lead	Johannes Binnewies	Johannes.Binnewies@informatixinc.com	(916) 830-1429	(916) 300-2187
CASES Development Lead	Johannes Binnewies	Johannes.Binnewies@informatixinc.com	(916) 830-1429	
CASES Security Lead	Mark Hanon	Mark.Hanon@informatixinc.com	(916) 830-1004	
CASES Interface Lead	Johannes Binnewies	Johannes.Binnewies@informatixinc.com	(916) 830-1429	
ARS Project Lead	David Jacobson	David.Jacobson@childsupport.co.la.ca.us	(323) 832-7191	
ARS Development Lead	David Jacobson	David.Jacobson@childsupport.co.la.ca.us	(323) 832-7191	
ARS Security Lead	Frank Schiavone	Frank.Schiavone@childsupport.co.la.ca.us		
ARS Interface Lead	Laura Chavez	Laura.Chavez@childsupport.co.la.ca.us		
IDB Project Lead	Hon-Wai Kong	Hon-wai.Kong@dcss.ca.gov	(916) 464-1026	
IDB Development Lead	Hon-Wai Kong	Hon-wai.Kong@dcss.ca.gov	(916) 464-1026	

Role	Lead Name	E-mail	Office Phone	Cell Phone
IDB Security Lead	Hon-Wai Kong	Hon-wai.Kong@dcss.ca.gov	(916) 464-1026	
IDB Interface Lead	Hon-Wai Kong	Hon-wai.Kong@dcss.ca.gov	(916) 464-1026	
CSR Project Lead	David Kendall	David.Kendall@dcss.ca.gov	(916) 464-5625	
CSR Development Lead	David Lateano	David.Lateano@ftb.ca.gov	(916) 845-5361	
CSR Security Lead	Kathy Bridges	Kathy.Bridges@ftb.ca.gov	(916) 845-4179	
CSR Interface Lead	Gillian Friess	Gillian.Friess@ftb.ca.gov	(916) 845-3893	

Table A.2: CCSAS Contact List

SP Vendor Contacts

Role	Lead Name	E-mail	Office Phone	Cell Phone
American Sentry Alarm Monitoring Company	Security Support	Confidential	(913)829-1700	Confidential
Apple One	Jennifer Schmidt	Confidential	(916)483-9180	Confidential
Bank of America	Blossom Dunng	Confidential	(916)321-4718	Confidential
Bank of the West	Michael Fanous	Confidential	(925)942-8359	Confidential
Besam Sliding Door	Nate Carda	Confidential	(866)952-3726	Confidential
Boon Edam Revolving Door	Roger Lopez	Confidential	(801)892-4528	Confidential
B.T. Mancini Co., Inc.	Beth McShane	Confidential	(916)381-3660	Confidential
Building Maintenance	John Detwiler	Confidential	(818)292-2032	Confidential
California Bank & Trust	Brian Hodges	Confidential	(916)341-4912	Confidential
Capital City Designs, Inc. (Electrical Engineering)	Tony Baker	Confidential	(916)375-0135	Confidential
CH&D Architects	Alan Hom	Confidential	(916)446-7741	Confidential
EMCI Mechanical	Nick	Confidential	(916)361-0106	Confidential
Heery International (Construction Management)	Jim Black	Confidential	(916)220-4417	Confidential
Iron Mountain Tape Vaulting Vendor (Primary)	Terese Matterson	Confidential	(323) 869-0400	Confidential
Iron Mountain Tape Vaulting Vendor (Secondary)	Brian Matterson	Confidential	(916) 381-0600	Confidential
Kelly Services (Staffing Services)	Collette Morgan	Confidential	(916)441-2440	Confidential
Locksmith	Bob Kennedy	Confidential	(916)532-5502	Confidential
McClellan Park (Secondary)	Jamie McGuire	Confidential	(916) 570-5323	Confidential
McClellan Park (Exterior Building and Roads)	Wanda Thompson	Confidential	(916)570-5318	Confidential
McClellan Park	Jill Larson	Confidential	(916)570-5380	Confidential
OPEX (Primary)	Chuck Preas	Confidential	(856)727-1100	Confidential
OPEX (Secondary)	Michael Massey	Confidential	(856)727-1100	Confidential
Pro-Tech (Fire Protection) – Sprinklers		Confidential	(916)388-0255	Confidential

Schetter Electric Inc.	Jim Spencer	Confidential	(916)446-2521	Confidential
Sierra Valley Movers	Ray Martinez	Confidential	(916) 649-3400	Confidential
Siemens (Physical Security Vendor)		Confidential	(800)560-8335	Confidential
TMSA	Richard McKinnom	Confidential	(530)241-8672	Confidential
Turley and Associates (Mech. & Plumbing design)	John Thompson	Confidential	(916)325-1065	Confidential
Union Bank of California	Paul Lindsay	Confidential	(916)321-3190	Confidential
Unisys (Account Manager)	Glenn Devall	Confidential	(205) 980-2647	Confidential
Unisys (SDU Service Manager)	Ross Stockweather	Confidential	(916) 646-5296	Confidential
Unisys (Client Rep – Document Processing)	Mike Okusako	Confidential	(916) 646-5398	Confidential
Unisys (Client Rep – Servers and SAN)	Tim O'Connell	Confidential	(916) 549-2014	Confidential
Unisys (SW Development Project Manager)	Pat Kotecha	Confidential	(248) 231-8813	Confidential
Unisys (Operations Situation Manager)	Jerry Blidy	Confidential	(480) 668-0171	Confidential
Unisys (West Region Field Operations)	Becky Foster	Confidential	(602) 224-4232	Confidential
Universal Fire Protection		Confidential	(916)563-1700	Confidential
US Bank of California	David Kepper	Confidential	(925)472-5815	Confidential
USPS	Dan Black	Confidential	(916)373-8176	Confidential
Valley Commercial Contractors	John Correa	Confidential	(916)781-8116	Confidential
Wells Fargo Bank	Tom Nugent	Confidential	(415)396-2456	Confidential
Westamerica Bank	Annette Burrell	Confidential	(916)449-8300	Confidential

Table A.3: SP Vendor Contacts

APPENDIX B - DIAGRAMS

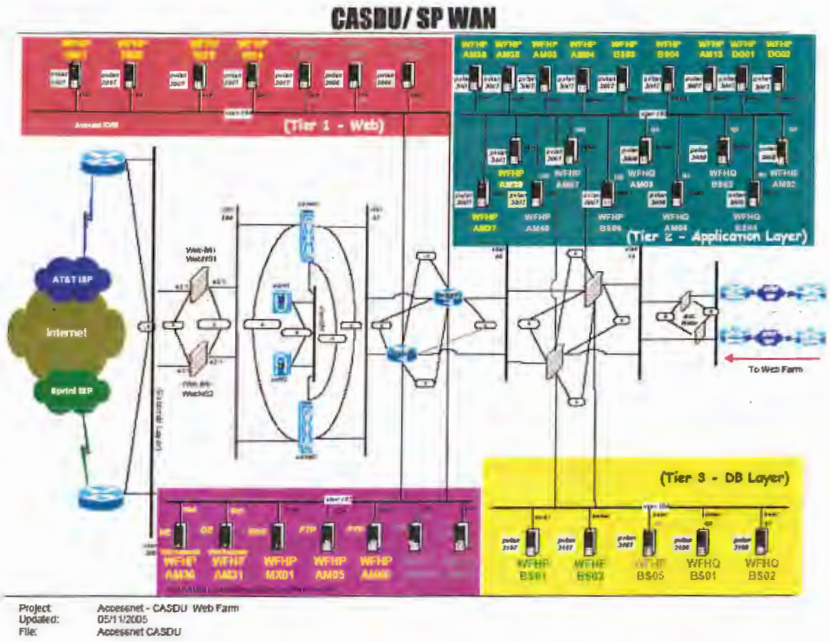


Figure B.1: CASDU WAN

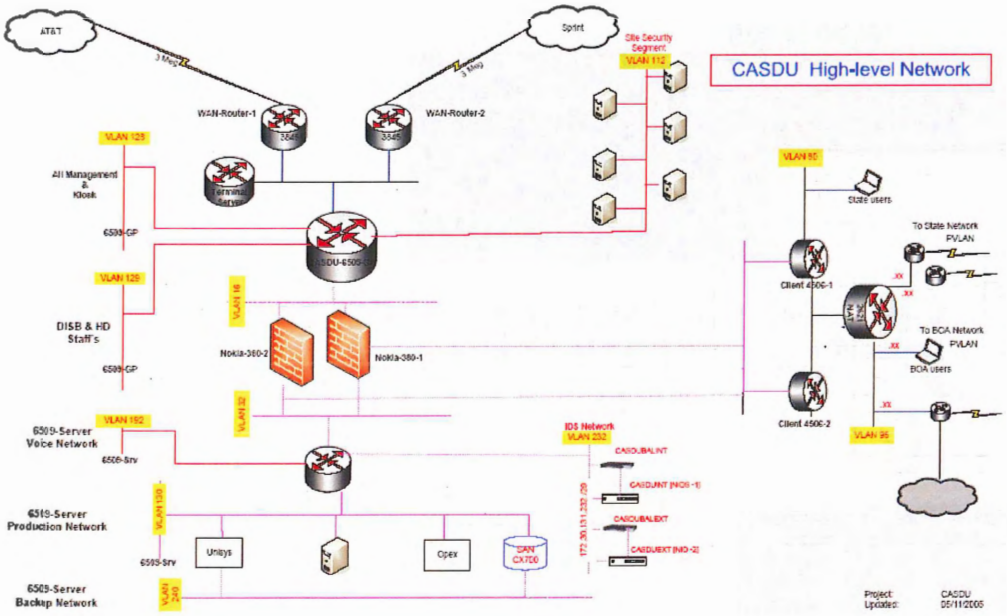


Figure B.2: CASDU High-Level Network

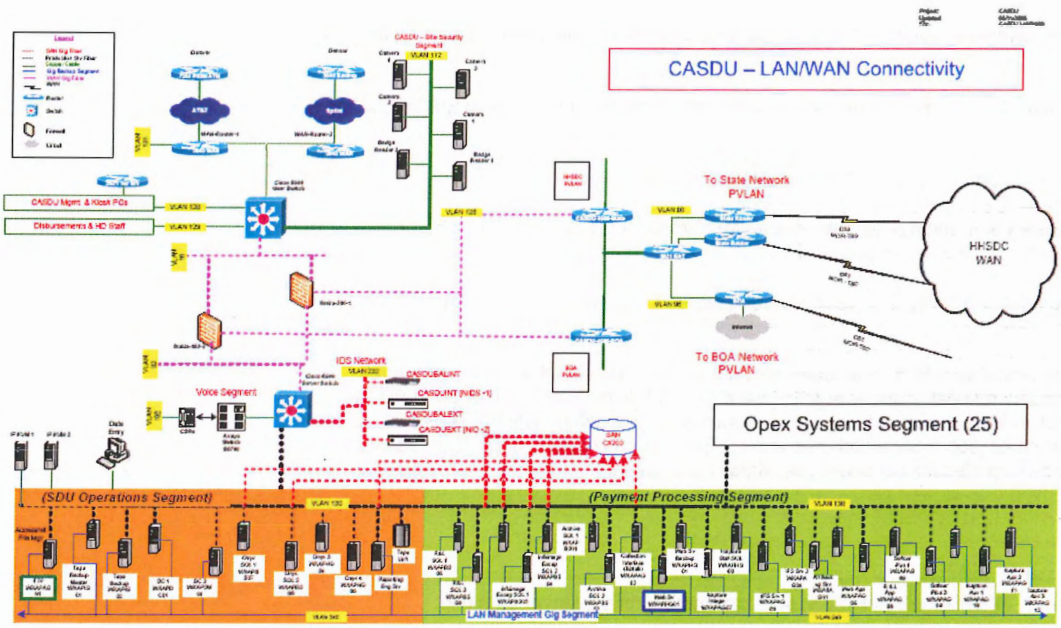


Figure B.3: CASDU – LAN/WAN Connectivity

APPENDIX C – GLOSSARY OF TERMS

A

AAA — Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies and auditing usage.

Access — The rights given specific users to use specific programs and utilities on the computer system.

ACH — Automated Clearing House.

Assets — Refers to all hardware, software, data, processing equipment, communications, and the physical facility.

Attacks — Is any attempt to enter the system or use authorized features of the system without proper authorization.

Availability — Refers to information being there when you need it.

Audit — Is any automated or manual processes employed to monitor the use of the computer facilities and its resources for security reasons only.

Authorization — The administrative act of determining whether a person (i.e. user) is trusted to act for a given purpose.

Awareness, Training, and Education — Includes (a) Awareness programs that set the stage for training by changing organizational attitudes toward realization of the importance of security and the adverse consequences of its failure; (b) The purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and (c) Education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in information technology.

B

Banner — Display on an information system that sets parameters for system or data use.

Boundary of a System — The boundary of a system encompasses all those components of an information system or network that are to be accredited. As a rule, separately accredited components are not included within the boundary -- those components are within the boundary. For purposes of identifying the mode of operation of an information system to be accredited, the information system has a conceptual boundary that extends to all intended users of a system, both directly and indirectly connected, who receive output from the system without a reliable human review by an appropriately cleared authority.

Boundary of a Network — For purposes of identifying the mode of a network to be separately accredited (including a LAN), the boundary of a network extends to (but does not include) the information technology systems or other separately accredited networks that attach thereto.

Browser — A client program that allows users to read hypertext documents on the World Wide Web an navigate between them. (e.g., Netscape Navigator, Lynx, Microsoft Internet Explorer). Browsers can be text-based or graphic.

Browsing — The act of searching through information technology systems storage to locate or acquire information, without necessarily knowing the existence or format of information being sought.

Bulletin Board System (BBS) — Software that supports multiple simultaneous callers (usually running terminal emulation software on PCs) to send and receive files and e-mail.

C

CCD — Cash Concentration/Disbursement

Certification — The comprehensive evaluation of the technical and non-technical security features of an information system or network and other safeguards, made as part of and in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Chief Information Officer (CIO) — Senior official designated to carry out the information resource management functions of the service provider. Responsible for implementing information policy, principles standards, and guidelines with respect to all areas of information resource management.

Clearing — The removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capability (i.e., keyboard strokes); however, the data may be reconstructed using laboratory methods. Cleared media may be used at the same classification level or at a higher level. Over writing is one method of clearing. Note: Volatile memory can be cleared by removing power to the unit for a minimum of one minute.

Client — A device or application that makes use of services provided by a server in a client/server architecture.

Common Criteria — The Common Criteria (CC) for Information Technology (IT) Security Evaluation standard provides a common, world-wide basis for vendors and consumers to specify and evaluate the security features or properties of IT products and systems.

Compromise — The disclosure of sensitive information to persons who are not authorized to receive such information.

Computer — A machine capable of accepting, performing calculations on, or otherwise manipulating, or storing data. It usually consists of arithmetic and logical units and a control unit, and may have input and output devices and storage devices.

Computer Hardware — The physical equipment or machinery used in information technology systems.

Computer Program — A series of instructions used to solve a problem or process information on a computer.

Computer Resources — Computer programs, data, other information, users and equipment.

Computer Room — A room in which computer operations are performed and physical access is controlled.

Computer Security — The measures and controls that ensure confidentiality, integrity, and availability of information technology systems assets including hardware, software, firmware, and information being processed, stored and communicated.

Computer Security Incident — The attempted or actual compromise of the confidentiality, integrity, or availability of a computer system or its information.

Computer Software — Computer programs, procedures, and associated documentation which addresses the operation of a data processing system.

Computer Virus — A program that infects computer systems in much the same way as a biological virus infects humans. The typical virus reproduces by making copies of itself and inserting them into other programs, either in systems software or in application programs.

Confidentiality — Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Confidentiality Protection — Requires access controls such as user ID/passwords, terminal identifiers, restrictions on actions like read, write, delete, etc. Examples of confidentiality-protected information are personnel, financial, proprietary, trade secrets, internal service provider, and investigations.

Configuration Control — Process of controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.

Configuration Management — Management of security features and assurances through control of changes to hardware, software, firmware, telecommunications, documentation, test, test fixtures, and test documentation throughout the development and life cycle of the information system.

Connection: Is a direct or telecommunication process which establishes an electronic attachment to the computer system

Contingency Management — Management of all the actions to be taken before, during, and after a disaster (emergency condition), along with documented, tested procedures which, if followed, will ensure the availability of critical information technology systems and which will facilitate maintaining the continuity of operations in an emergency situation.

Contractor Employee — Refers to all employees working on an SP contract, including subcontractors, requiring staff-like access to SP owned or controlled facilities, or work, wherever located, on those contracts which involved the design, operation, repair or maintenance of information systems and access to sensitive but unclassified information.

Control Objectives — A statement of intent with respect to the oversight of some aspects of an organization's resources or processes, or both. In terms of information technology systems, control objectives provide a framework for developing a strategy for fulfilling security requirements for any given system. The three basic control objectives for securing information system are security policy, accountability, and assurance.

Controlled Access Protection — A level of protection that can be used to deny unauthorized access to information stored in information technology systems and prevent outside intruders from electronically accessing sensitive but unclassified information by way of supporting telecommunications in networked information technology systems.

Cookie — A data file or directory used by a web server to store an information "place holder" on the web browser for future reference. Cookies may be either transient (lasts for the duration of the session) or persistent (retained beyond the end of the session).

Countermeasures — The action, device, procedure, technique, or other measure, that reduces the vulnerability of an automated information system. The means or measures might be physical (fences, rooms, containers, locks, alarms, etc.), systemic (passwords, user profiles, terminal profiles, terminal lockouts, etc.), or regulatory (laws, regulations, policy, IRM instructions, managerial approval, inspections, reviews, etc.).

Critical Information System — An information system that is essential to continued effective operations. The loss of or damage to the system would have serious implications to the authorized users or information system owner.

Critical Resources — Those physical and information assets required for the performance of the site mission.

Criticality — This is determined by the importance of the asset to an organization. The level of criticality is determined by the organization's need for asset's confidentiality, integrity, and availability. The level of criticality is directly related to the level of security protection required.

Cryptography — Principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

CTX — Corporate Trade Exchange

D

Data — A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by humans or by an information system.

Database — A structured collection of largely unique data items or records of information maintained in one or more computer files, which may be processed by one or more system.

Data Communications — A general data processing term that refers to communications among computers. Data communications, a component of telecommunications associated with information technology systems and networks, is included within the scope of this manual and will generally make use of telecommunication systems and/or facilities that may have been separately accredited under other national plans.

Data Encryption Standard — A cryptographic algorithm for the protection of unclassified data and published by the NIST in FIPS PUBS 140–2 and 46–2 or their replacements.

Data Integrity — Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Data Owner — The authority, individual, or organization who has original responsibility for the data by statute, executive order, or directive.

Data Scope — A hardware device that monitors data on a network to ensure the data is arriving as it will and that everything on the network is working properly.

Data Security — The protection of computerized data information from accidental or malicious modification, destruction, or disclosure.

Dedicated Remote Access — Permanently enabled remote access usually in the form of private wide area network data lines that are connected to trusted third parties.

Debug — The removal of malfunctions or errors in a computer program.

Decryption — The process of converting encrypted data (called ciphertext) into original text (called plaintext). Sometimes called deciphering.

Degausser — A device that can generate a magnetic field for degaussing magnetic storage media.

Degaussing — To demagnetize magnetic media in a way that leaves a very low residue of magnetic induction on the media, the electromagnetic destruction of data or information on magnetic media. Also called demagnetizing. This process effectively erases the magnetic media.

Denial of Service — Action or series of actions that prevents any part of a secure telecommunication or automated information system from functioning in accordance with its intended purpose, either by loss or degradation of operational capability.

Destruction — The physical alteration of information system media or of information system components such that they can no longer be used for storage or retrieval of information.

Digital Signature — An unforgeable electronic signature that authenticates a message sender and also guarantees the integrity of the protected message. It is an authentication tool that verifies the origin of a message and the identity of the sender and receiver. A digital signature is unique for every transaction.

Digital Subscriber Line (DSL) — A public network technology that delivers high bandwidth over conventional copper wire at limited distances.

Direct User (also referred to as a directly connected user) — A user who is electronically connected to an information system typically via an interactive link and whose access is automatically limited in real time by the information system on some basis (e.g., security clearance, need-to-know). The directly connected user has access to the various capabilities of an information system (e.g., data bases, programs, system output) and interacts with the information system in near-real-time. In addition to protecting the data processed on the information system from inadvertent system spillage and misroutes, the information system must provide adequate near-real-time controls to limit the direct users access to those processing capabilities for which the user has been authorized and to withstand potential direct attacks against the system's security controls. The means of electronic connection for this type of user may include one or more of the following: (a) a point-to-point link, (b) a local area network (LAN), or (c) a global network. There are no geographic restrictions on how far a directly connected user may be from the information system. A given computer system may have both direct and indirect users. Direct users present a significantly higher risk of security compromise in an information system than do indirect users who do not have interactive access to an information system (see definition of Indirect User).

Directory — A directory is specially coded to identify and control data used by the information system to group files which the operating system uses to search for established data or will build files for newly established data. It is a means by which the operating system locates particular files or data.

Disclosure — An unauthorized and unlawful release of controlled information.

Discretionary Access Control — An access policy that restricts access to system objects (e.g., files, directories, devices) based on the identity and need-to-know of the users, processes or groups to which they belong. Discretionary means that a user with a certain access permission is capable of passing that permission to another user (e.g., letting another user modify a file).

Document — Any prepared record regardless of physical form or characteristics which may contain official and sensitive information. This includes, but is not limited to: handwritten, printed or typed information; sound or voice recordings; information on magnetic media; or a reproduction of any of the foregoing regardless of the process used.

Dynamic Remote Access — Remote access used on a temporary basis usually for the intention of remote administration or work from remote locations.

E

Electronic Mail (E-mail) — A form of electronic messaging. Simple Mail Transport Protocol (SMTP) is a widely used method of transporting E-mail across the Internet, RFC 822 define protocols and message formats for Internet E-mail.

Electronic Mail (E-mail) Message — A document created or received on an e-mail system, including brief notes, more formal and substantive documents and any attachments, such as work processing documents transmitted, but not created, on an e-mail system.

Electronic Signature — A technology neutral term indicating various methods of signing an electronic message that identifies and authenticates a particular person as source of the electronic message and indicates such person's approval of the information contained in the electronic message (definition form GPEA, P.L. 105–277). Examples of electronic signature technologies include personal identification numbers, user identifications and passwords, digital signature, digitized signatures, and hardware and biometric tokens.

Encryption — To convert plain text into unintelligible form by means of a cryptosystem.

Encryption Algorithm — A formula used to turn data into a secret code. Each algorithm uses a string of bits known as a key to perform the calculations. The larger the key (the more bits in the key), the greater the number of potential patterns that can be created, thus making it harder to break the code and unscramble the contents. Most encryption algorithms use the block cipher method, which codes fixed blocks of input that are typically from 64 to 128 bits in length. Some use the stream method, which works with the continuous stream of input.

Environmental Threat — Any surrounding unintentional or natural accident, incident, or malfunction that may cause damage to IT resources, information, and personnel (i.e., structural failure, power fluctuation, temperature/humidity fluctuation, heating/cooling system failure).

EPC — Electronic Payment Card

Erasure — Process intended to render stored data irretrievable by normal means.

Escort Access (Refers to contract and temporary employees) — Escort access to an SP facility is accomplished by the accompaniment of the contract/temporary employee by an authorized SP employee. During work performance and movements throughout the facility, the escort must at a minimum, maintain visual contact with the contract/temporary employee.

External Network — Any network residing outside the security perimeter established by the firewall system.

Extranet — A private data network that uses the public telephone network to create a secure Internet like network among chosen organizations, companies, business partners, suppliers, etc.. An extranet extends a private network (often referred to as an intranet) to outside parties in situations in which both sides can benefit by exchanging information quickly and privately.

F

Facility — A physically definable area consisting of a controlled space which contains national security or sensitive information-processing equipment.

Facsimile (FAX) — The process by which fixed graphics images, such as printed text and pictures, are scanned and converted into electrical signals that may be transmitted over a telecommunications system and used to create a copy of the original or an image.

Field Review — The review of the technical and non-technical security features employed by a system within its operational environment to insure that the provisions of this manual are implemented. Field reviews may include penetration testing and are often used to certify to the accrediting authority that appropriate security measures have been implemented in order to protect the information processed within an acceptable level of risk.

File Permissions — A method of implementing discretionary access control by establishing security application (software) that identifies system users and system components (e.g., data bases, data records, application programs, etc.) and selectively allows accesses based upon correlation between users and components encoded in a file, for example, user profiles.

File Security — The protection of files stored on a computer system through discretionary access control.

File Server — A local area network computer dedicated to providing file and mass data storage to other network stations. Usually the base location/control point for a network operating system.

File Transfer Protocol — A Transmission Control Protocol (TCP) used to transfer files from a server to a client. In conjunction with local software, FTP allows computers connected to the Internet to exchange files, regardless of the computer platform.

File/Write Protect — A protective feature to prevent accidental overwriting of data on magnetic media already containing reserved or saved data.

Firewall — System components (gateway, bridge, router, or front-end processor) that limit access between networks in accordance with established security policy.

Firmware — A term usually related to micro-programming and those specific software instructions that have been more or less permanently burned into a Read Only Memory control block. Firmware is a machine component of a computer system, similar to a computer circuit component.

Functional Security Coordinator — The individual who is responsible for the day-to-day security responsibilities for a particular functional area or unit.

G

Gateway — Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures.

General Support System — An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

H

Handled By — The term handled by denotes the activities performed on data in an information system, such as collecting, processing, transferring, storing, retrieving, transmitting, disseminating, and controlling.

Host — A computer that provides services directly to users (in a TCP/IP network it is a device with an assigned Internet Protocol address); or A large computer that serves many users (e.g., mainframe or minicomputer).

Human Threat — A person or an organization with the capability and intention to do damage to the service provider mission.

I

IDB — Integrated Database

Identification — The process of telling a system the identity of a subject (e.g., a user or another system). This is usually done by entering a name or presenting a token to the system. See authentication.

IMPS — Collections Engine image archive software.

Indirect Users (also referred to as indirectly connected users) — In contrast to a direct user, an indirect user receives system output produced outside his control either: (a) by an automatic mechanism within the information system, or (b) from a process initiated by a direct user. An indirect user is precluded from initiating a process on the information system and receiving the output there from. An indirect user is one who is electronically connected to the information system by other than a direct, interactive link. An information system supporting indirect users does not have to withstand direct attacks against the system's security controls because an intervening process(or) between the user and the information system affords some protection and control. The information system must protect the processing capabilities of the information system from inadvertent system spillage and misroutes and generally provides some control over indirectly connected users who may attempt to gain unauthorized access to the processing capabilities of the information system. While there are a wide range of security risks associated with this type of user, such risks are not considered to be as significant as those associated with directly connected users. As with a direct user, the means of electronic connection for this type of user may include one or more of the following: (a) a point-to-point link, (b) a LAN, or (c) a global network. There are no geographic restrictions on how far an indirectly connected user may be from the information system. Indirect users of the information system also include those who receive system output that has been generated electronically on the information system and forwarded to a user without first undergoing a reliable human review of the data to determine whether it is appropriately classified and marked (e.g., to protect against system spillage and misroutings). Examples of indirect users include those who receive (without a reliable human review) printed output, and floppy or hard disks.

Individual Accountability — Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Information — The terms data, information, material, documents, and, matter, are considered synonymous and used interchangeably in this manual. They refer to all data regardless of its physical form (e.g., data on paper printouts, tapes, disks or disk pack, in memory chips, in random access memory (RAM), in read only memory (ROM), on microfilm or microfiche, on communication lines, and on display terminals).

Information Security Policy — The aggregate of directives, regulations, rules, and practices that regulate how an organization manages, protects, and distributes information.

Information System — An information system is an assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. It is an entire infrastructure, organization, personnel, and

components for the collection processing, storage, transmission, display, dissemination, and disposition of information. Examples include information storage and retrieval systems, mainframe computers, minicomputers, personal computers and workstations, and office automation systems.

Information Systems Security (INFOSEC) — The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Information Systems Security Officer — An individual formally appointed by the CIO to ensure that the provisions of all applicable directives identified within the scope of this manual are implemented throughout the life cycle of each information system.

Information Technology (IT) — The hardware and software operated by the service provider or by a contractor of the service provider or other organization that processes information on behalf of the service provider or accomplishes a service provider function, regardless of the technology involved, whether computers, telecommunications, or others.

Infrastructure — Includes investments that will provide hardware, software, databases, networking, storage, and/or communications capabilities. While some bureaus centrally manage infrastructure, some bureaus manage infrastructure systems as major categories of equipment or systems (e.g., different mainframe systems or telecommunications network). This system category will reflect the bureau's approach, but the ultimate goal is to better understand and plan for the major infrastructure components.

Integrated Services Digital Network (ISDN) — An international telecommunications standard for transmitting voice, video, and data over digital lines running at 64 Kbps.

Integrity — The quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrences of the stored data. In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Intelligent Terminal — A terminal that is programmable, able to accept peripheral devices, able to connect with other terminals or computers, able to accept additional memory, or which may be modified to have these characteristics.

Interim Authority To Operate — Temporary authorization granted by a designated accrediting authority for an information system to process information based on preliminary results of a security evaluation of the system.

Internet — Two or more networks connected by a router; the world's largest network using TCP/IP protocols to link government, university, and commercial institutions.

Internet Service Provider (ISP) — An organization that provides access to the Internet. Individuals and corporations subscribe to ISPs. Most ISPs provide additional services, including giving each subscriber space on their server for an electronic mail box, access to new groups, and maintaining a Web page that can be used as their browser's home page.

Intranet — Use of TCP/IP, Internet, and world wide web technology for networks internal to an organization.

K

Key — Information used initially to set up and periodically change the operations performed in cryptographic equipment for the purpose of encrypting and decrypting electronic signals.

Keying Material — A sequence of symbols or their electrical or mechanical equivalents which, in machine or auto-manual cryptosystems, is combined with plain text to produce cipher text.

Key Management — Process by which key is generated, stored, protected, transferred, loaded, used, and destroyed.

Key Management Plan — A strategy that addresses how keying material will be generated, stored, protected, transferred, loaded, used and destroyed. The plan includes format of key, cryptoperiod, forecasting quantitative requirements, and classification/sensitivity of keying material. A key management plan is concerned with systems security, physical security, personnel security, interoperability, manageability, and user friendliness.

L

Label — The marking of an item of information to reflect its security classification. (a) Internal Label. The marking of an item of information to reflect the classification of the information within the confines of the medium containing the information. (b) External Label. The visible and readable marking on the outside of the medium or the cover of the medium that reflects the classification of the information resident within the medium.

Least Privilege — A security principle stating that a user or a process will be granted the most restrictive set of privileges needed to perform a particular task and to keep those privileges only for the duration of the task. Least privilege limits the damage that can occur because of accident or system attack.

Log-on — The process of identifying oneself to, and having one's identity authenticated by, a computer system.

M

Magnetic Readable Media — Media that can convey data to a given sensing device, e.g., diskettes, disks, tapes, computer memory.

Major Application — An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Major System — Any information system in operation, under development, or planned new initiative that requires special and continuing management attention because of its importance to a bureau's mission; its high development, operating, or maintenance costs; or its significant role in the administration of bureau programs, finances, property, or other resources. Large infrastructure investments (e.g., major purchases of personal computers or local area network improvements) are consider major systems. All major systems must be included in either the core business process systems category, mission support systems category, infrastructure category, or other category, either as a stand-alone system or as part of a larger "umbrella" system.

Malicious Software — Any of a family of computer programs developed with the sole purpose of doing harm. Often malicious code is embedded in software programs that appear to provide useful functions but, when activated by a user, cause undesirable results.

Mission Critical Information — Information which must be protected from loss or disclosure to keep an adversary or competitor from gaining a significant operational, economic, political, or technological advantage and prevent adverse impact on a classified or unclassified mission accomplishment.

Mission Support Systems — Systems used by human resource management, payroll, finance, accounting, facilities management, or document management.

Modem — Acronym for modulator/demodulator. It is a device that converts data back and forth between digital and analog formats to allow the data to be sent over analog portion of the public telephone network.

Most Restrictive — The term "most restrictive" in relation to information security policies is defined as any statement, or statements, that are reasonably determined to be more limiting in nature, requiring an additional or advanced set of controls in relation to conflicting policy statements with an end result being a reduced level of associated risk.

N

NDP — Document imaging system

Need-to-Know — The necessity for access to, or knowledge or possession of specific information required to carry out official duties.

Network — A network comprises communications media and all components attached thereto whose responsibility is the transfer of information among a collection of information technology systems or workstations. Network components include packet switches, front-end computers, network controllers, technical control devices, and other networks. Networks include both wide-area and local-area technologies. Within the scope of this manual, point-to-point dedicated secure communications circuits and other telecommunications systems such as AUTODIN and Diplomatic Telecommunications Service (DTS) are not considered networks; however, the accreditation process for each sensitive system must consider the security features and vulnerabilities of such telecommunications systems when they are used to provide information system and/or network connectivity.

NIST (National Institute of Standards & Technology) — Organization within the U.S. Department of Commerce responsible for setting standards to promote effective commerce. The Computer Security Act of 1987 gave NIST the responsibility for setting security standards for the non-defense side of government.

Node — A system connected to a network.

Non-repudiation — Steps taken by a service provider to provide assurance, via the use of an audit trail, that a sender cannot deny being the source of a message, and that a recipient cannot deny receipt of a message.

O

Object Reuse — The reassignment to a subject (e.g., a user) of a medium (e.g., disk, diskette, magnetic tape) that previously contained an object (e.g., a file). The danger of object reuse is that the object may still contain information that the subject may not be authorized to access.

OCSE — Office of Child Support Enforcement.

Official Use Only — The legend used to identify officially limited information that is important or sensitive.

Off-Premises Storage — The storage of media (i.e., programs, data files, documentation, etc.) that is needed to successfully restore an information system in the event of a disaster. The storage facility must be a survivable distance from the normal place of use and must meet minimum environmental and physical security standards.

Operating Controls — Controls that address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

OPEX — Mail extraction and processing system.

Other System — Includes IT investments that may not easily fit into the core business process systems, mission support systems, or infrastructure category of major systems. Normally, this may include major IT systems that may be managed as a separate program, such as a centrally managed component (e.g., telecommunications).

P

Packet — A unit of data sent across a network.

Packet Filtering — The process of screening Internet Protocol packets based on some combination of the source Internet Protocol address, destination Internet Protocol address, User Datagram Protocol source port, User Datagram Protocol destination port and incoming network interface.

Packet Switching — A communications paradigm in which message packets are individually routed between hosts, with no previously established communications path.

Password — A protected/private alphanumeric string used to authenticate and identify or to authorize access.

Penetration Testing — A type of testing in which testers attempt to circumvent the security features of a system in an effort to identify security weaknesses.

Permission — A type of interaction a subject can have with an object. For example, file permissions specify the actions particular users or classes of users can perform on the file.

PGP — Pretty Good Privacy

Physical Security — The use of locks, guards, badges, alarms, procedures, and similar measures (alone or in combination) to control access to the sensitive information system and related equipment. The measures required for the protection of the structures housing the sensitive information system, related equipment, and their contents from espionage, theft, waste, fraud, abuse, or damage by accident, fire, and environmental hazards.

PPD — Prearranged Payment and Deposit

Privacy — A security principle that protects individuals from the collection, storage, and dissemination of information about themselves and the possible compromises resulting from unauthorized release of that information.

Private Branch Exchange (PBX) — A subscriber owned telecommunications switch, usually owned by an organization and located on their property that usually includes access to the public switched network. A PBX is used to direct calls among internal lines and between internal and outside lines through the public telephone network.

Private Key Cryptography — A form of cryptography that uses the same key to encrypt and decrypt a message. Users have the same key that they share, but the key remains secret from other users. Also called asymmetric cryptography.

Privileges — Authority to access a database or application resource (object) or to perform a function (e.g., create new user accounts).

Proprietary/Copyrighted Software — Software that is protected by an exclusive right inferred by authorship and ensured by the Federal Government.

Protocol — A set of rules or standards that describe ways that two network entities can communicate with one another.

Public Key Infrastructure — An IT infrastructure that enables users of a basically unsecured public network such as the Internet to secure and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

Public Switched Telephone Network (PSTN) — The global landline telephone network accessible to everyone with an active connection who pays the required access fees.

Purge — Removal of data from an information system, its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed.

R

Remanence — Residual information remaining on storage media after clearing.

Remote Access Feature — A feature that permits authorized callers from the public network to access the system and use its features and services.

Residual Risk — Portion of risks remaining after security measures have been applied.

Risk — The possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an information system or activity. It is a combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact.

Risk Assessment — Process of analyzing threats to and vulnerabilities of an information system, and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective measures.

Risk Management — The ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Router — A networking device that can send (route) packets to the correct LAN segment, based on addressing at the Network Layer.

Rules of Behavior — The rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules will cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal government equipment, the assignment and limitation of system privileges, and individual accountability.

S

Safeguard — Any action, device, procedure, technique, or other measure that reduces a system's vulnerability to a threat.

Sanitization — The elimination of sensitive information from an information system or media associated with an information system to permit the reuse of the information system or media or to permit the release to uncleared personnel or personnel without the proper need-to-know authorizations.

Scan — To examine computer coding/programs sequentially, part by part. For viruses, scans are made for virus signatures or potentially unsafe practices (e.g., changes to an executable file, direct: writes to specific disk sectors, et al.).

Security — Measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

Security Controls — The controls that mitigate a risk of a system or provide a level of protection to reach an acceptable level of risk.

Security Features — The security-relevant functions, mechanisms, and characteristics of information system hardware and software (e.g., identification, authentication, audit trail, access control) that implement security controls.

Security Incident — An attempt to exploit an information system such that the actual or potential adverse effects may involve fraud, waste, or abuse; compromise of information; loss or damage of property or information; or denial of service. Security incidents include penetration of computer systems, exploitation of technical and administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code.

Security Incident Response — Actions conducted to resolve information technology security incidents.

Security Policy — The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Requirements Baseline — Description of the minimum requirements necessary for an information system to maintain an acceptable level of risk.

Security Review — An assessment of an information system that identifies threats and vulnerabilities that could affect the confidentiality, integrity, availability, of a system. Security controls are identified to mitigate the risk based on cost and benefits.

Security Safeguards — The protective measures and controls that are prescribed to meet the security requirements specified for an information system. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices.

Security Test and Evaluation — Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of the system.

Sensitive Application — See Sensitive System.

Sensitive System — A system containing information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of the service provider to accomplish its mission.

Sensitivity — In an information technology environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability which is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.

Separation of Duties — A security principle that assigns security-related tasks to several distinct individuals. Usually, each of them has the least number of privilege needed to perform those tasks. Duties and responsibilities in critical functions must be divided among different individuals to ensure that no individual has all the necessary authority or access which could result in a fraudulent activity and/or corruption of a critical process.

Server — Device or process that provides service to clients in a client/server architecture.

SFTP — Secure version of the FTP protocol, also written as S/FTP. SFTP uses SSL to encrypt the entire user session, thereby protecting the contents of files and the user's login name and password from network sniffers. Through normal FTP, usernames, passwords and file contents are all transferred in clear text over the wire. If you have a choice, always use SFTP over FTP.

Site — One or more operational facilities, usually geographically contiguous, operated by or for the service provider under the management and administrative direction of the SP or SP contractor.

Sniffer — A network diagnostic tool used to monitor communications packets passing through a network. It is software tool for auditing and identifying network traffic.

Software License Agreement — A contractual agreement between a software developer and an authorized user that stipulates the reproduction and usage restrictions.

Staff-Like Access — Refers to unescorted access to service provider owned or controlled facilities, information systems, security items and products and/or sensitive information by contractor personnel.

Stand-Alone System — A system that is physically and electronically isolated from all other systems, and intended to be used by one user at a time, with no data belonging to users remaining in the system (e.g., a personal computer with removable storage media such as a floppy disk).

Subcontract — Any contract entered into by a contractor to furnish supplies, goods or services for performance of a prime contract on a subcontract. Any contract, subcontract, purchase order, lease agreement, service agreement, request for quotation, request for proposal, solicitation or other agreement or procurement action between one or more contractors which requires access to classified information to fulfill the performance requirements of a prime contract.

Subcontractor — A supplier, distributor, vendor, or firm that furnishes supplies, goods or services to or for a prime contractor or another subcontractor, or who enters into a contract with a prime contractor.

Superuser — Special user who can perform control of processes, devices, networks, and file systems.

Switch — A computer on a telecommunications or data network that chooses the next destination on the network for a voice call or digital transmission, locates an open circuit to that destination, and sends the call or data to that location. It is described as a mechanical, electro-mechanical, or electronic device for making, breaking, or changing the connections in or among circuits.

System — A generic term used in this manual to include both information technology systems and networks. A system may be either a major application or a general support system.

System Integrity — Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System of Records — Any information that is electronically retrievable by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to an individual.

System Operational Status — A system is either (a) Operational - system is currently in operation, (b) Under Development - system is currently under design, development, or implementation, or (c) Undergoing a Major Modification - system is currently undergoing a major conversion or transition.

T

Technical Controls — Consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Technical Vulnerability — A hardware, firmware, or software weakness or design deficiency that leaves an information system open to potential exploitation, either externally or internally, thereby resulting in risk of compromise of information, alteration of information, or denial of service.

Telecommunications — Preparation, transmission, communication, or related processing of information (writing, images, sounds or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

Telemetering — A technology used for remote monitoring and control. It typically uses wire or radio communications to instruments and metering and control equipment. In the SDU it would include intrusion detection systems, access control, video and audio monitoring, and building heating and cooling control.

Telnet — The TCP/IP standard network virtual terminal protocol used for remote terminal connection service that allows a user at one site to interact with systems at other sites as if that user terminal were directly connected to computers at those sites.

Threat — An activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

Time Bomb — Computer code that is preset to cause a later malfunction after a specific date, time or a specific number of operations. The □Friday the 13th□□computer virus is an example. This virus infects the system several days or even months before and lies dormant until the date reaches Friday the 13th.

Transmission Control Protocol (TCP) — The connection-oriented, transport-level protocol for the TCP/IP suite.

Transmission Control Protocol/Internet Protocol (TCP/IP) — A standard high-level protocol for transferring files from one computer to another, usually implemented as an application level program, and uses the Telnet and TCP protocols. It is a set of communication protocols that encompass media access, packet transport, session communications, file transfer, electronic mail, terminal emulation, remote file access, and network management. TCP/IP provides the bases for the Internet.

Trap Door — Hidden software or hardware mechanism used to circumvent security controls. Synonymous with back door.

Trojan Horse — Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information.

Trusted Computer System — A system that uses sufficient hardware and software integrity measures to allow its use for concurrently processing a range of classified or sensitive information.

Trusted System — An automated information system that has been certified by technically qualified personnel as having been properly designed and implemented to effectively use protection mechanisms to provide the appropriate level of trust. Trusted computer systems are components of a trusted system, but may not constitute the entire trusted system.

U

Unauthorized Disclosure — Exposure of information to individuals not authorized to receive it.

Unauthorized Software — Software not obtained or developed through authorized procurement channels or the System Control Point for any system.

User — Person or process authorized to access an information technology systems.

User-ID — A unique code or string of characters that a system uses to identify a specific user.

User Profile — A specialized record of authorization(s) allowing the user specific accesses to applications, files, data, software, or machines.

V

Vendor — (See Contractor)

Virus — Self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.

Virus Detection Software — Software written to scan machine-readable media on computer systems. There are a growing number of reputable software packages available that are designed to detect and/or remove viruses. In addition, many utility programs can search text files for virus signatures or potentially unsafe practices.

Virus Signature — A unique set of characters which identify a particular virus. This may also be referred to as a virus marker.

Vulnerability — Any weakness in a telecommunications system, information system, or cryptographic system, or system security procedures, hardware design, internal controls, denial of

service, etc., that could be exploited in attempting to gain unauthorized access to classified or sensitive information.

Vulnerability Assessment — Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness or proposed security measures, and confirm the adequacy of such measures after implementation.

W

Web Browser — A user interface (usually graphical) to hypertext information on the World Wide Web) or on private data networks such as intranets or extranets. Netscape and Microsoft Internet Explorer are two popular browsers.

Wide Area Network (WAN) — A communication network that covers a wide geographic area, such as a state or country.

Workstation — In networking, any personal computer (other than a file server) attached to the network; workstation computers may be desktop or portable.

World Wide Web (WWW) — Distributed heterogeneous document and multimedia information system based on standard protocols and accessible from the Internet.

Worm — Independent program that replicates from machine to machine across network connections, often clogging networks and computer systems as it spreads.

APPENDIX D – TRAINING MATRIX

			Employees:	Doe, John
Document Title	**Rev.**	**Revision Date**	**Schedule**	DOH
On-Boarding Materials				
CCSAS Project Overview Video	A	02/10/2005	Initial	
CCSAS Data Security Training ppt.	A	02/21/2005	Initial/Annually	
CCSAS Appendix A Document	B	03/21/2005	Initial	
CCSAS SDU RFP Acronyms Document	A	03/21/2005	Initial	
CCSAS SDU RFP Glossary Terms & Definitions Document	A	03/21/2005	Initial	
DCSS Internet/Electronic Mail (E-Mail) Policy	A	01/18/2005	Initial	T 01/18/2005
DCSS Mandated Reporting/Security Breach Notification Policy	A	01/18/2005	Initial (ICs)	T 01/18/2005
DCSS Confidentiality Training Session	A	01/18/2005	Initial/Annually	T 01/18/2005
DCSS Confidentiality Statement Form	B	03/03/2005	Initial/Annually	RT 02/24/2005
OCSE Video: Securing the Future	A	01/18/2005	Initial	T 01/18/2005
CA SDU On Boarding Guide (Deloitte)	B	03/28/2005	Initial	
UNAX: Safeguarding Federal Tax Information	A	01/18/2005	Initial/Annually	
Orientation Items:				
FDC Orientation Video	A	03/01/2005	Initial	

KEY:		
		Training Required
		Revision:Re-training Required
	T	Trained
	RT	Re-trained

Figure D.1: Training Matrix

APPENDIX E – CERTIFICATE OF INSURANCE

ACORD™ CERTIFICATE OF LIABILITY INSURANCE 03/31/2006

DATE (MM/DD/YY) 04/06/2005

PRODUCER
Locklon Companies
444 W 47th Street, Suite 900
Kansas City Mo 64112-1906
(816) 960-9000

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW.

INSURERS AFFORDING COVERAGE

INSURED
1054591
FIRST DATA CORPORATION
5660 NEW NORTHSIDE DRIVE
ATLANTA GA 30328

INSURER A: CONTINENTAL CASUALTY COMPANY (CNA)
INSURER B:
INSURER C:
INSURER D:
INSURER E:

COVERAGES FIDAC01 WF

THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. AGGREGATE LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	POLICY NUMBER	POLICY EFFECTIVE DATE (MM/DD/YY)	POLICY EXPIRATION DATE (MM/DD/YY)	LIMITS	
	GENERAL LIABILITY COMMERCIAL GENERAL LIABILITY CLAIMS MADE / OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: POLICY / PRO-JECT / LOC	NOT APPLICABLE			EACH OCCURRENCE	$ XXXXXXX
					FIRE DAMAGE (Any one fire)	$ XXXXXXX
					MED EXP (Any one person)	$ XXXXXXX
					PERSONAL & ADV INJURY	$ XXXXXXX
					GENERAL AGGREGATE	$ XXXXXXX
					PRODUCTS - COMP/OP AGG	$ XXXXXXX
	AUTOMOBILE LIABILITY ANY AUTO ALL OWNED AUTOS SCHEDULED AUTOS HIRED AUTOS NON-OWNED AUTOS	NOT APPLICABLE			COMBINED SINGLE LIMIT (Ea accident)	$ XXXXXXX
					BODILY INJURY (Per person)	$ XXXXXXX
					BODILY INJURY (Per accident)	$ XXXXXXX
					PROPERTY DAMAGE (Per accident)	$ XXXXXXX
	GARAGE LIABILITY ANY AUTO	NOT APPLICABLE			AUTO ONLY - EA ACCIDENT	$ XXXXXXX
					OTHER THAN AUTO ONLY: EA ACC	$ XXXXXXX
					AGG	$ XXXXXXX
	EXCESS LIABILITY OCCUR / CLAIMS MADE DEDUCTIBLE / UMBRELLA FORM RETENTION $	NOT APPLICABLE			EACH OCCURRENCE	$ XXXXXXX
					AGGREGATE	$ XXXXXXX
						$ XXXXXXX
						$ XXXXXXX
						$ XXXXXXX
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY	NOT APPLICABLE			WC STATUTORY LIMITS / OTHER	
					E.L. EACH ACCIDENT	$ XXXXXXX
					E.L. DISEASE - EA EMPLOYEE	$ XXXXXXX
					E.L. DISEASE - POLICY LIMIT	$ XXXXXXX
A	OTHER CRIME	268093252	03/31/2005	03/31/2006	$15,000,000 LIMIT	

DESCRIPTION OF OPERATIONS/LOCATIONS/VEHICLES/EXCLUSIONS ADDED BY ENDORSEMENT/SPECIAL PROVISIONS
COVERAGE INCLUDES EMPLOYEE DISHONESTY AND FIDELITY BOND

CERTIFICATE HOLDER ☐ ADDITIONAL INSURED; INSURER LETTER: ____

2101584
INFORMATION ONLY
5660 NEW NORTHSIDE DRIVE
ATLANTA GA 30328

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, THE ISSUING INSURER WILL ENDEAVOR TO MAIL 30 DAYS WRITTEN NOTICE TO THE CERTIFICATE HOLDER NAMED TO THE LEFT, BUT FAILURE TO DO SO SHALL IMPOSE NO OBLIGATION OR LIABILITY OF ANY KIND UPON THE INSURER, ITS AGENTS OR REPRESENTATIVES.

AUTHORIZED REPRESENTATIVE

ACORD 25-S (7/97) For questions regarding this certificate contact the number listed in the 'Producer' section above and specify the client code 'FIDAC01' © ACORD CORPORATION 1988

Figure E.1: Proof of Bonding

APPENDIX F – ACCOUNTABILITY

Employee Accountability Form

Name: _____
(Please Print)

Your job responsibilities require you to have access to the First Data on-line data processing system, therefore we have issued you a password and unique sign-on to the system. To protect the cardholder information in the system and to ensure proper use of First Data's systems, we ask that you read, understand, and sign this form as an agreement to comply with all policies outlined in this form.

ON-LINE SYSTEM ACCESS

Your password should not be disclosed to anyone for any reason. Do not write your password on anything.

Only you know your password. Therefore, you are responsible for any activity performed under your sign-on. You are required to logoff whenever you leave any terminal you have been using. You must not access any terminal with another person's sign-on and password.

You must not perform any on-line transaction to your own account, family member's account, or personal friend's account. You must not review or access any accounts, including those mentioned in the previous sentence, unless required to do so under your job responsibilities.

Confidential Information is intended for restricted use within certain bankcard units. Unauthorized disclosure could adversely affect First Data, our customers, and our employees. Disclosure of this confidential information to unauthorized parties is prohibited.

ALL COMPUTING PLATFORMS AND WORKSTATIONS

You understand that all data residing in all First Data computing resources is vital to the well being of the company and must not be created, modified, or deleted without proper authorization. You must take every effort to ensure the confidentiality integrity, authenticity, and availability of all information that you may encounter during your employment at First Data. You understand the use of First Data computing resources is for approved First Data business-use only. You will not install a) illegal (non-First Data licensed) copies of software such as trial copies, applications, games, shareware or freeware; or b) hardware, on any First Data personal computer or workstation. You will routinely scan your PC or workstation for viruses using a First Data approved virus-scanning software.

You understand that messages and documents created and stored on First Data computers or networks are property of First Data and are not considered private. First Data retains the right to access information /computers or networks for business, security, or investigating purposes or as required by law. Similarly, employees have no expectation of privacy in work areas, such as desks or work provided lockers. First Data may search such areas without employee consent or knowledge. Refusal to permit such searches may result in discipline.

DIAL-IN/DIAL-OUT ACCESS

You understand that all remote dial-in access must be done through a First Data approved secure dial-in system and that all approved PC or workstation modems used on dial-up lines must be turned off at the end of the workday.

INTERNET AND E-MAIL AND WORKSPACES ACCESS

You understand that all access to the Internet must be done through a secured firewall approved by the PC/LAN Technical Group and Information Security departments. All access to the Internet is limited to business-use-only. Accesses to non business-related locations are prohibited and you should not send or receive any First Data information through the Internet unless it is encrypted with approved First Data encryption techniques and First Data management has approved the transmission.

You understand that the use of First Data's e-mail for purposes such as: participating in private commercial use: pornography; chain letters; or to make unwelcome references to a person's race, color, religion, sex, sexual orientation, age, national origin, disabilities, or physique, is prohibited.

PHYSICAL SECURITY

You understand that you will receive an access card allowing you access to First Data locations and that you will not allow anyone else to use such card to gain un-authorized access. You also understand that if you are assigned the duties of escorting a First Data visitor, you will not allow the visitor to walk around un-escorted. You will not grant access to restricted locations such as the Data Center/Tape Library, PBX Room UPS Complex, or any other location designated as a restricted area. Also, you must prominently display this badge at all times while at Company facilities.

I have read, understand, and intend to comply with the above provisions. I understand that failure to follow the guidelines listed above will result in corrective action up to and including immediate termination of my employment with First Data.

_____
Employee Printed Name

_____ Date:_____
Employee Signature

_____
First Data Representative Printed Name

_____ Date:_____
First Data Representative Signature

Figure F.1: Employee Accountability Form

APPENDIX G – CONFIDENTIALITY

STATE OF CALIFORNIA
DEPARTMENT OF CHILD SUPPORT SERVICES

Confidentiality Statement

Confidential information is information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code, Sections 6250-6265), or other applicable state or federal laws. Examples of confidential information might include names; addresses; social security numbers; financial information including income, deductions, credits, federal or state tax returns, debt collection information for child support, and/or court fees; personnel records; and criminal offender record information, including attorney-client information/work products. Protecting confidential information is in the public's interest, the state's interest, and your own personal interest.

State employees, contractors and contractors' employees must protect the following types of confidential information:

- Information about individuals that relates to their personal life or identifies or describes an individual.
- Tax account information
- Taxpayer and feepayer information
- Claimant and employer information
- Internal Revenue Service's confidential and proprietary information
- Other agencies' confidential and proprietary information
- Criteria used for initiating audit selection
- Methods agencies use to safeguard their information, including computer systems, networks, server configurations, etc.
- Any other information that is considered proprietary, a copyright, or otherwise protected by law or contract
- Information contained in DCSS databases utilized for testing which contain any of the above information

State employees, contractors and contractors' employees shall protect confidential information by:

- Accessing, inspecting, using, disclosing or modifying information only for the purpose of performing official duties
- Never accessing, inspecting, using, disclosing, or modifying information for curiosity, personal gain, or any non-business related reason
- Securing confidential information in approved locations
- Never removing confidential information from your work site without authorization

As a State employee, contractor or contractors' employee, you are required to know whether information you have been granted access to is confidential. If you have any questions, contact your agency's Disclosure Officer or your employer's Information Security Officer.

Unauthorized access, inspection, use, or disclosure of confidential information is a crime under state and federal laws, including but not limited to: California Family Code section 17212; California Revenue and Taxation Code sections 19542, 19542.1, and 19552; California Penal Code section 502; California Unemployment Insurance Code sections 1094, 2111, and 2714; California Government Code section 15619; California Labor Code section 1198.6; and United States Internal Revenue Code sections 6103, 7213, 7213A and 7431 (see disclosure penalties). Unauthorized access, inspection, use, disclosure, or modification of confidential information can result in:

- Administrative discipline, including but not limited to: reprimand, suspension without pay, salary reduction, demotion, and/or dismissal from State service,

- Criminal prosecution,
- Civil lawsuit, and/or
- Termination of contract.

PROTECTING IRS TAX RETURNS AND RETURN INFORMATION - DISCLOSURE PENALTIES

IRC SEC 7213. UNAUTHORIZED DISCLOSURE OF INFORMATION

(a) RETURNS AND RETURN INFORMATION

(1) FEDERAL EMPLOYEES AND OTHER PERSONS. It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)]. Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) STATE AND OTHER EMPLOYEES. It shall be unlawful for any person [not described in paragraph (1)] willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)] acquired by him or another person under subsection (d), (i)(3)(B)(i), (1)(6), (7), (8), (9), (10), (12), (15), or (16) or (m)(2), (4), (5), (6), or (7) of section 6103. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000 or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(3) OTHER PERSONS. It shall be unlawful for any person to whom any return or return information [as defined in section 6103(b)] is disclosed in any manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of the paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000 or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(4) SOLICITATION. It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information [as defined in 6103(b)] and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000 or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(5) SHAREHOLDERS. It shall be unlawful for any person to whom return or return information [as defined in 6103(b)] is disclosed pursuant to the provisions of 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000 or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

IRC SEC 7213A. UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION

(a) PROHIBITIONS

(1) FEDERAL EMPLOYEES AND OTHER PERSONS. It shall be unlawful for –

(A) any officer or employee of the United States, or

(B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.

(2) STATE AND OTHER EMPLOYEES. It shall be unlawful for any person [not described in paragraph (1)] willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).

(b) PENALTY

(1) IN GENERAL. Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1,000 or imprisonment of not more than 1 year, or both, together with the costs of prosecution.
(2) FEDERAL OFFICERS OR EMPLOYEES. An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) DEFINITIONS. For purposes of this section, the terms "inspect," "return," and "return information" have respective meanings given such terms by section 6103(b).

IRC SEC 7431. CIVIL DAMAGES FOR UNAUTHORIZED DISCLOSURE OF RETURNS AND RETURN INFORMATION

(a) IN GENERAL
(1) INSPECTION OR DISCLOSURE BY EMPLOYEE OF UNITED STATES. If any officer or employee of the United States knowingly or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United states in a district court of the United States.
(2) INSPECTION OR DISCLOSURE BY A PERSON WHO IS NOT AN EMPLOYEE OF UNITED STATES. If any person who is not an officer or employee of the United States knowingly or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) EXCEPTIONS. No liability shall arise under this section with respect to any inspection or disclosure
(1) which results from good faith, but erroneous interpretation of section 6103, or
(2) which is requested by the taxpayer.

(c) DAMAGES. In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of
(1) the greater of
(A) $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or
(B) the sum of
(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus
(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus
(2) the cost of the action.

(d) PERIOD FOR BRINGING ACTION. Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) NOTIFICATION OF UNLAWFUL INSPECTION AND DISCLOSURE. If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of
(1) paragraph (1) or (2) of section 7213(a),
(2) section 7213A(a), or
(3) subparagraph (b) of section 1030(a)(2) of Title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

(f) DEFINITIONS. For purposes of this section, the terms "inspect," "inspection," "return," and "return information" have the respective meanings given such terms by section 6103(b).

(g) EXTENSION TO INFORMATION OBTAINED UNDER SECTION 3406. For purposes of this section
(1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and
(2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103.

For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 3406.

CERTIFICATION

I expressly consent to the monitoring of my access to computer-based confidential information by the Department of Child Support Services, the Department of Justice, the Franchise Tax Board, the Employment Development Department, the State Board of Equalization, or any other agency designated by DCSS or by my employer.

I understand unauthorized access, inspection, use, modification, or disclosure of confidential information is punishable as a crime and/or can result in disciplinary and/or civil action being taken against me.

My signature verifies that I have received and read this confidentiality statement and have been provided a copy of the CCSAS data security reminders.

My signature also verifies that I have read and understand the civil and criminal penalties associated with unauthorized disclosure of information provided to DCSS by the IRS.

Employee/Contractor Name (Print)

Signature	DATE

I have reviewed and discussed this Confidentiality Statement and the DCSS policies with the employee named above.

Supervisor's Name (Print)	
Supervisor's Signature	DATE

Figure G.1: Confidentiality Statement

APPENDIX H – ENCRYPTION REQUIREMENTS

Encryption Requirements

Encryption is an important part of secure communications; the following rules apply to all sensitive information requiring encryption as defined by sensitivity levels as described in Section 4.7:

a. Encryption during storage of data may be required for specific highly sensitive fields (see g. below), but is not required for the whole of databases or network storage unless separation of highly sensitive fields is not possible.

b. All administrative communications for the purpose of system or application administration require encryption such as SSH, VPN, or Terminal Services utilizing medium to high encryption levels.

c. Sensitive information shall be encrypted using either AES, NIST approved Triple Data Encryption Standard (3DES), or 3DES devices and/or applications determined to be compliant with Federal Information Processing Standards Publications 140-2 and 46-3, or their replacements.

d. Sensitive information transiting a public network via HTTPS must use, at a minimum SSL v3/TLS v1 128bit or greater, 3DES is recommended. RC2 and 40bit keys are prohibited.

e. Cryptography shall be implemented in hardware, firmware, software, or combination thereof.

f. Acceptable Symmetric Key Algorithms:

- Triple-DES (DES-EDE, as per spec - 168 bit key derived from 192)
- CAST5 (128 bit key minimum, as per RFC 2144)
- Blowfish (128 bit key minimum, 16 rounds) [BLOWFISH]
- AES with 128-bit key minimum

g. Render unreadable stored highly sensitive information such as passwords, cardholder data, personally identifiable information, and banking information by using any of the following approaches:

- One-way ciphers (hashed indexes), such as SHA-1, but not MD5
- Truncation
- Index tokens and PADs, with the PADs being securely stored
- Strong cryptography, such as Triple-DES or AES with associated key management processes and procedures.

h. Cryptographic solutions must be implemented so that:

- Secret data may not be disclosed
- Conforms to applicable international and national standards, as well as legal and regulatory controls

Encrypted PIN Management Requirements

All information systems employing encryption of Personal Identification Numbers (PIN) used for retail financial services such as POS and ATM must adhere to industry-accepted best practices, as described in the *Accredited Standards Committee (ASC) TG-3-1997 PIN Security Compliance Guideline*, or international equivalents. TG-3-1997 is a procedure and control guideline based upon requirements set forth in *X9.8 (PIN Management and Security)* and *X9.24 (Financial Services Retail Key Management)*.

APPENDIX I – VISITOR ACCESS LOG

DATE	VISITOR PRINT NAME VISITOR SIGNATURE	COMPANY NAME	PERSON TO VISIT PURPOSE OF VISIT	ID HELD Y / N	BADGE #	TIME-IN TIME-OUT	AUTHORIZED EMPL PRINT NAME AUTHORIZED EMPL SIGNAUTURE

Figure I1: Visitor Access Log

APPENDIX J – CA SDU USER MANAGEMENT PROCEDURES

SDU User Management Procedures

SDU system access is divided into two primary user management models. The first model supports systems that are physically located in the SDU operations facility in McClellan, CA. The second model supports systems located in the SP's secured data center in Denver, CO. Both of these user management models are governed by the SP's standard security policies as well as the California SDU Statement of Work (RFP).

This appendix represents the high level user management procedures for each of the following primary SDU systems:

- SDU Network Access
- Collection Engine (CE)
- Disbursements Engine (DE)
- Reporting Engine (RE)
- CORE Interface Engine (CIE)
- Onyx Ticketing
- Non IV-D Data Collection
- SDU IVR
- SDU Web

In addition, each system is subdivided into user types as they pertain to the system being addressed. These user types are as follows:

- System Administrators
- General SDU System Users
- LCSA/DCSS Group Managers
- LCSA/DCSS General Users
- Public Users

Table J.1 identifies the types of users that are associated with each primary SDU system:

	System Administrators	General SDU System Users	LCSA/ DCSS Group Managers	LCSA/ DCSS General Users	Public Users
SDU Network Access	X	X			
Collection Engine	X	X	X	X	
Disbursements Engine	X	X	X	X	
Reporting Engine	X	X			
CORE Interface Engine	X				
Onyx Ticketing	X	X			
Non IV-D Data Collection	X	X			
SDU IVR	X				X
SDU Web	X				X

Table J-1 – System User Types

J.1 – SDU Network Access

SDU network access is managed and administered by the SP Network Engineering Group. The process of administering SDU network access is initiated through the completion of the SDU LAN Access Form and is typically completed upon hire. Refer to *Section K.11* for an example of the SDU LAN Access Form.

The following processes support the initiation, renewal and termination of SDU network access accounts.

Create a New SDU Network Account

1. When a new SDU Network User is identified:
   a. Human Resources staff completes the *SDU Network Access Request Form (Section K.11)* and submits to the SP Network Engineering Group for initiation.
   b. The SP Network Engineering Group initiates the new SDU network account and provides the specific level of access defined in the Access Request Form for each pertaining segment of the SDU LAN.
   c. The SP Network Engineering Group files the hard copy of the *SDU Network Access Request Form* in a locked file cabinet.
   d. The new Network Account Holder is provided with their username and password via hard copy and is required to change their password upon initial login.

Terminate SDU Network Account

~~1)~~1. When an SDU employee is terminated or an SDU employee network account must be suspended, the following steps must occur:
   a. The SDU Technical Manager or SDU System Administrator is notified.
   b. The SDU Technical Manager or SDU System Administrator works with the SP Network Engineering Group to immediately disable the SDU LAN account on all pertaining SDU/SP subsystems.

SDU Network Account Holder Forgets Password or Account Becomes Disabled

~~1)~~1. In any case where an SDU Network Account Holder forgets their password, the SDU Network Account Holder contacts the SDU Technical Manager or SDU System Administrator and explains the problem.
~~2)~~2. The SDU Technical Manager or SDU System Administrator works with the SP Network Engineering Group to reset the password.
~~3)~~3. The SDU Network Account Holder is provided with their reset username and password via hard copy and is required to change their password upon initial re-login.

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

J.2 – System Administrator Users

From a System Administrator perspective, all SP systems are similarly governed to ensure that the highest levels of security are maintained. System Administrator users include: Code Migration Engineers, Database Administrators, User Administrators, Computer Operators/Monitors, System Support Engineers and any other role driven by the SDU Information Technology Group are included in the category of System Administrator. This procedure does not govern development or other SP corporate subsystems.

For all systems within the SDU facility and SP Denver Data Center, the SDU System Administrator completes the following user procedures.

SDU System Administrator User Accounts

Create a New SDU System Administrator

1. When a new SDU System Administrator is identified:
   a. Human Resources staff completes the *California SDU System Access Request Form (Section K.12)* and submits it to the SDU Technical Manager.
   b. The SP Technical Manager initiates a new System Administrative user and provides the specific level of access defined in the access request form for each SDU subsystem.
   c. The SDU Technical Manager files the hard copy of the *California SDU System Access Request Form (Section K.12)* in a locked file cabinet.
   d. The new user is provided with their username and password via hard copy and is required to return the hard copy to the SDU Technical Manager after initial entry into the system.

Terminate SDU System Administrator

1. When an SDU System Administrator is terminated or there is a need to suspend an SDU System Administrator the following steps must occur:
   a. The SDU Technical Manager is notified.
   b. The SDU Technical Manager works with the SDU System Administrator to immediately disable the user accounts on all pertaining SDU subsystems.

SDU System Administrator User Forgets Password or Account Becomes Disabled

1. In any case, when an SDU System Administrator forgets their password, they contact the SDU Technical Manager who retrieves the username and password from the on site SDU fireproof safe and provides it to the SDU System Administrator.

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Beyond the System Administrator role, each SDU system is uniquely managed to support General SDU Users, LCSA/DCSS Users and Public users. The following sections identify each of the systems identified in Appendix J.

J.3 – Collections Engine Users

General CE Users

Create a New General CE User

1. When a new employee is identified:
   a. Human Resources staff completes a *California SDU System Access Request Form (Section K.12)* and submits it to the SDU System Administrator or an assigned delegate.
   b. The SDU System Administrator initiates a new user and provides the specified level of access defined on the System Access Form. General CE User types include the following:
      - ~~1.~~ Icapture Define Template
      - ~~2.~~ Icapture Supervisor
      - ~~3.~~ Icapture OCREdit
      - ~~4.~~ Icapture Key From Image
      - ~~5.~~ R&L Supervisor
      - ~~6.~~ R&L DP Operator
      - ~~7.~~ R&L Workstations (general data entry)
      - ~~8.~~ Infolmage Production
      - ~~9.~~ Archive General User (Read Only)
      - ~~10.~~ EFT Editor User
   c. The SDU System Administrator files the hard copy of California SDU System Access Request Form (Section K.12) in a locked file cabinet
   d. The new user is provided with their username and password via hard copy form and is required to return the form to the SDU System Administrator after initial entry into the system, where it is shredded.

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Bulleted + Level: 1 + Aligned at: 1" + Tab after: 1.25" + Indent at: 1.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Terminate Current General CE User

1. When a current user is terminated or a current user must be suspended, the following steps must occur:
   a. The SDU System Administrator or an assigned delegate is notified.
   b. The SDU System Administrator immediately logs onto the CE and disables the user.

General CE User Losses Password or Becomes disabled

1. In any case where a General SDU User forgets their password or becomes disabled:
   a. The user contacts their SDU System Administrator and explains the problem.
   b. Assuming the user is still authorized to use the system, the SDU System Administrator resets the user's password and provides the user with a new password.

LCSA/DCSS CE Archive Group Manager

Create a New LCSA/DCSS CE Archive Group Manager

1. When a new Group Manager is identified by an LCSA or DCSS, an authorized LCSA or DCSS manager:
   a. Completes the *California SDU LCSA/DCSS System Access Request Form (Section K-13)* and submits it to the SDU System Administrator or an assigned delegate.
      ~~11.~~ The SDU System Administrator initiates a new LCSA/DCSS Group Manager account on the CE Archive System.
   b. The SDU System Administrator files the hard copy of California SDU System LCSA/DCSS Access Request Form in a locked file cabinet.
   c. The new user is provided with their username and password via email.

Terminate Current LCSA/DCSS CE Archive Group Manager

1. When a current LCSA/DCSS CE Archive Group Manager is terminated or there is a need to suspend their account the following steps must occur:
   a. An authorized LCSA/DCSS manager notifies the SDU System Administrator or an assigned delegate.
   b. The SDU System Administrator immediately logs onto the CE and disables the user account.
   c. The System Administrator also works with the authorized LCSA/DCSS manager to assign a new Group Administrator to replace the terminated user, so that the LCSA or DCSS group can resume user account management under the standard Group Manager/User model.

LCSA/DCSS CE Archive Group Manager Forgets Password or Becomes Disabled

1. In any case where an LCSA/DCSS Group Manager forgets their password or it becomes disabled:
   a. The user contacts the SDU Electronic Help Desk and explains the problem.
   b. Assuming the user is still authorized to use the SDU CE Archive system, the Electronic Help Desk (EHD) staff member contacts the SDU System Administrator to reset the Group Manager's password and provides the Group Manager with a new password via e-mail.

LCSA/DCSS CE Archive User

Create a New LCSA/DCSS CE Archive User

1. The LCSA/DCSS Group Manager is responsible for managing LCSA/DCSS CE Archive User accounts.
2. The LCSA/DCSS Group creates their own polices and procedures around the creation, termination, tracking and resolution of all LCSA/DCSS CE Archive User management

Formatted: Indent: Left: 0.25", Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75", Tab stops: Not at 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Bulleted + Level: 1 + Aligned at: 1" + Tab after: 1.25" + Indent at: 1.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

efforts.

3. The SP assists all LCSA and DCSS managers upon request.

J.4 – Disbursements Engine Users

General DE User

Create a New General SDU User

1. When a new employee is identified:
   a. Human Resources staff completes the *California SDU System Access Request Form* (Section K.12) and submits a copy to the SDU System Administrator
   b. The SDU System Administrator initiates a new user and provides the specific level of access to that user.
   c. The SDU System Administrator files the hard copy of *California SDU System Access Request Form* (Section K.12)
   d. The new user is provided with their username and password via email.

Terminate Current General SDU User

1. When a current user is terminated or a current user must be suspended, the following steps must occur:
   a. The SDU System Administrator is notified.
   b. The SDU System Administrator immediately logs onto the Disbursement Engine (DE) and disable the user.
   c. The SDU System Administrator also removes all profiles from the user ID.

General SDU User Forgets Password

1. In any case where a General SDU User forgets their password:
   a. The General SDU user clicks the "I forgot my password" link and enters their username and email address.
   b. A randomly generated password is emailed to the user.
   c. The user is prompted to change their password when they first log in again.

General SDU User becomes Disabled

1. In the event a General SDU User becomes disabled, the user contacts the SDU Group Administrator who performs the following steps:
   a. Verifies the General SDU User is still an employee of the SP.
   b. Logs onto the DE and enables the user.
   c. Generates a new password and emails it to the user.

LCSA/DCSS DE Group Manager

Create a New LCSA/DCSS DE Group Manager

1. When a new LCSA/DCSS Group Manager is identified by an LCSA or the DCSS, an authorized LCSA or DCSS manager:
   a. Completes the *California SDU LCSA/DCSS System Access Request Form (Section K-13)* and submits it to the SDU System Administrator or an assigned delegate.
      ~~12.~~ The SDU System Administrator initiates a new LCSA/DCSS Group Manager account on the DE Archive System with the proper level of access.
   b. The SDU System Administrator files the hard copy of California SDU System LCSA/DCSS Access Request Form in a locked file cabinet.
   c. The new LCSA/DCSS Group Manager is provided with their username and password via email.

Terminate Current LCSA/DCSS DE Group Manager

1. When a current LCSA/DCSS DE Group Manager is terminated or their account must be suspended, the following steps must occur:

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Indent: Left: 0.25", Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25", Tab stops: 0.5", List tab + Not at 0.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Tab after: 1" + Indent at: 1"

Formatted: Indent: Left: 0.25", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25", Tab stops: 0.5", List tab + Not at 0.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Tab after: 1" + Indent at: 1"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Bulleted + Level: 1 + Aligned at: 1" + Tab after: 1.25" + Indent at: 1.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

a. An authorized LCSA/DCSS manager notifies the SDU System Administrator or an assigned delegate.
b. The SDU System Administrator will immediately log onto the DE and disable the LCSA/DCSS Group Manager account.
c. The System Administrator also works with the authorized LCSA/DCSS manager to assign a new Group Administrator to replace the terminated user so that the LCSA or DCSS group can resume user account management under the standard Group Manager/User model.

LCSA/DCSS DE Group Manager Forgets Password

1. In any case where a LCSA/DCSS Group Manager forgets their password:
   a. The General SDU user clicks the "I forgot my password" link and enters their username and email address.
   b. A randomly-generated password is emailed to the user.
   c. The user is prompted to change their password when they first log in again.

LCSA/DCSS DE Group Manager Becomes Disabled

1. In any case where a LCSA/DCSS Group Manager forgets their password or becomes disabled:
   a. The user contacts the EHD and explains the problem.
   b. Assuming the user is still authorized to use the SDU DE Archive system, the EHD staff member contacts the SDU System Administrator to reset the Group Manager's password and provides the Group Manager with a new password via email.

LCSA/DCSS DE User

Create a New LCSA/DCSS DE Archive User

1. The LCSA/DCSS Group Manager is responsible for managing LCSA/DCSS DE User accounts.
2. The LCSA/DCSS Group creates their own polices and procedures around the creation, termination, tracking and resolution of all LCSA/DCSS DE Archive User management efforts.
3. The SP assists all LCSA and DCSS managers on request.

J.5 – Reporting Engine (RE)

Reporting Engine Users

Create a New SDU RE User

~~1.~~1)When a new employee is identified:
   a. Human Resources staff completes the *California SDU System Access Request Form (Section K.12)* and submits it to the SDU System Administrator or an assigned delegate.
   b. The SDU System Administrator initiates a new user within the RE and provides the specified level of access defined on the System Access Form. General RE User types include the following:
      ~~13.~~▪ Report Author
      ~~14.~~▪ General User
   c. The SDU System Administrator files the hard copy of *California SDU System Access Request Form* (*Section K.12*) in a locked file cabinet.
   d. The new user is provided with their username and password via hard copy form and is required to return the form to the SDU System Administrator after initial entry into the system.

Terminate Current General RE User

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Indent: Left: 0.5", Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Tab after: 1" + Indent at: 1", Tab stops: Not at 1"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Bulleted + Level: 1 + Aligned at: 1" + Tab after: 1.25" + Indent at: 1.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

1. When a current user is terminated or must be suspended, following steps must occur:
   a. The SDU System Administrator or an assigned delegate is notified.
   b. The SDU System Administrator immediately logs onto the RE and disables the user.

General RE User Losses Password or Becomes disabled

1. In any case where a General SDU User forgets their password or becomes disabled:
   a. The user contacts their SDU System Administrator and explains the problem.
   b. Assuming the user is still authorized to use the system, the SDU System Administrator resets the users password and verbally provides the user with a new password.

J.6 – CORE Interface Engine (CIE) Users

CIE Users

Beside System Administrator Users (Section K.1), there currently are no other User Management needs for the CIE.

J.7 – Onyx Ticketing Users

Onyx Users

Create a New Onyx User

1. When a new employee is identified:
   a. Human Resources staff completes the *California SDU System Access Request Form (Section K.12)* and submits it to the SDU System Administrator or an assigned delegate.
   b. The SDU System Administrator initiates a new user within the Onyx system and provides the specified level of access defined on the System Access Form. General Onyx System User types include the following:
      - ~~15.~~ Report Author
      - ~~16.~~ General User
   c. The SDU System Administrator files the hard copy of *California SDU System Access Request Form* (*Section K.12*) in a locked file cabinet.
   d. The new user is provided with their username and password via hard copy form and is required to return the form to the SDU System Administrator after initial entry into the system.

Terminate Current General Onyx System User

1. When a current user is terminated or must be suspended, the following steps must occur:
   a. The SDU System Administrator or an assigned delegate is notified.
   b. The SDU System Administrator immediately logs onto the Onyx System and disables the user.

General Onyx System User Losses Password or Becomes disabled

1. In any case where a General SDU User forgets their password or becomes disabled:
   a. The user contacts their SDU System Administrator and explains the problem.
   b. Assuming the user is still authorized to use the system, the SDU System Administrator resets the users password and verbally provides the user with a new password.

J.8 – Non IV-D Data Collection

Non IV-D Data Collection

Formatted: Indent: Left: 0.25", Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25", Tab stops: 0.5", List tab + Not at 0.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Bulleted + Level: 1 + Aligned at: 1" + Tab after: 1.25" + Indent at: 1.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Indent: Left: 0.25", Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25", Tab stops: 0.5", List tab + Not at 0.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Create a New Onyx User

1. When a new employee is identified:
   a. Human Resources staff completes the *California SDU System Access Request Form (Section K.12)* and submits it to the SDU System Administrator or an assigned delegate.
   b. The SDU System Administrator initiates a new user within the Non IV-D Data Collection system and provides the specified level of access defined on the System Access Form. General Non IV-D Data Collection System User types include the following:
      ~~17.~~ Supervisor/Manager
      ~~18.~~ General CSR
   c. The SDU System Administrator files the hard copy of *California SDU System Access Request Form* (*Section K.12*) in a locked file cabinet.
   d. The new user is provided with their username and password via hard copy form and is required to return the form to the SDU System Administrator after initial entry into the system.

Terminate Current General Non IV-D Data Collection System User

1. When a current user is terminated or must be suspended, the following steps must occur:
   a. The SDU System Administrator or an assigned delegate is notified.
   b. The SDU System Administrator immediately logs onto the Non IV-D Data Collection System and disables the user.

General Non IV-D Data Collection System User Losses Password or Becomes disabled

1. In any case where a General SDU User forgets their password or becomes disabled:
   a. The user contacts their SDU System Administrator and explains the problem.
   b. Assuming the user is still authorized to use the system, the SDU System Administrator resets the users password and verbally provides the user with a new password.

J.9 – SDU IVR

SDU IVR Users

Beside System Administrator Users (Section K.1), there currently are no other User Management needs for the SDU IVR.

J.10 – SDU Web

Web Users

Beside System Administrator Users (Section K.1), there currently are no other User Management needs for the SDU Web Site.

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Bulleted + Level: 1 + Aligned at: 1" + Tab after: 1.25" + Indent at: 1.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Indent: Left: 0.25", Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25", Tab stops: 0.5", List tab + Not at 0.25"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Tab at 0.5" + Indent at: 0.5"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"

J.11 – California LAN Access Request Form

LAN / LOTUS NOTES USERS
SYSTEM ACCESS REQUEST FORM

ALL FIELDS ARE REQUIRED FIELDS - IF DATA IS MISSING PROCESSING MAY BE DELAYED

ACTION	***EMPLOYEE STATUS***	***EXISTING USER?***
☐ NEW	☐ REGULAR	☐ YES ☐ NO
☐ DELETE	☐ TEMPORARY: EFTPS Letter of assurance on file?	☐ YES ☐ NO
☐ CHANGE	☐ CONSULTANT: EFTPS Letter of assurance on file?	☐ YES ☐ NO

EXPIRATION DATE _____ **(REQUIRED IF TEMPORARY OR CONSULTANT)**

USER ID _____ (REQUIRED IF NOT NEW USER)

USER INFORMATION:

Last Name _____ First _____ Middle Initial ___

Preferred Email Name If Different From Above:

Last Name _____ First _____ Middle Initial ___

Title: _____ **Location:** _____ **Suite:** _____

Work #: _____ Ext _____ Cost Center # (8 Digit Code) _____

Department _____ Manager _____

E-Mail Dial-in User ☐ Yes ☐ No Does user share a PC with other users? ☐ Yes ☐ No

System #: _____ PC Type: ☐ Laptop ☐ Desktop

Operating System: ☐ Windows XP ☐ Windows 2000 ☐ Other _____

NEW USER ACCESS REQUEST

User Access: ☐ **Executive** ☐ **Finance** ☐ **Human Resource** ☐ **Production** ☐ **Helpdesk** ☐ IT

Does user need an E-Mail account? ☐ Yes ☐ No **Does user have E-Mail account with in FDC** ☐ Yes ☐ No **"IF Yes" Location** _____

ADDITIONAL ACCESS REQUEST

User needs access to the following Server/Directory (please include the entire path to the directory or file):

_____

_____

Type of Access: ☐ Read Only ☐ Read/Write ☐ Read/Write/Create/Erase

PLEASE DO NOT SUBMIT FORM WITHOUT USER AND MGR SIGNATURE
PLEASE ALLOW 3 WORKING DAYS FOR THIS REQUEST TO BE COMPLETED

I acknowledge my responsibility as a user of the FDC computer system. I will not share my password with any other users. I understand that I am accountable for all accesses made by my logon ID (user ID) and that this logon ID may be revoked and appropriate steps may be taken if it is abused.

USER'S SIGNATURE: _____ DATE _____

MANAGER'S NAME (PRINT): _____ PHONE _____

MANAGER'S SIGNATURE: _____ DATE _____

HR SIGNATURE (if required): _____ DATE: _____

THIS SECTION FOR FDC-LANS USE ONLY

LAN ADMINISTRATOR: _____ DATE: _____

LAN ID: _____ MAIL ID: _____ CONTEXT: _____

J.12 – California SDU System Access Request Form

- ***For all System Administrator User requests, please deliver this form to SDU Technical Manager for processing.***
- ***For all General SDU User requests, please deliver this form to the SDU Systems Administrator for processing.***
- ***The requestor must be an SDU Manager.***
- ***This form assumes that SDU network access has been granted, and all security clearances have been met.***

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Date of Request:_____ Requester Name:_____ Requestor Title _____

Requestor Signature: _____ Date: _____

User First Name: _____ User MI: _____ User Last Name: _____

User Title: _____ User Location: _____

User E-mail: _____ User Work Phone: _____ User Cell Phone: _____

Department:_____ Manager: _____

☐Existing User ☐New User ☐Remove User Expiration: _____

☐General Staff ☐Supervisor ☐Manager ☐Tester ☐Technical Staff ☐Auditor

User Signature: _____ Date: _____

Systems to be Accessed and Level:

Collections Engine	**Disbursements Engine**
☐Icapture Administrator ☐Icapture Define Template ☐Icapture Supervisor ☐Icapture OCREdit ☐Icapture Key From Image ☐R&L Supervisor ☐R&L DP Operator ☐R&L Workstations (general data entry) ☐R&L Server (IT Only)	☐DE Group Administrator ☐SWS SDU Read Only User ☐ARS SDU Read Only User ☐CASES SDU Read Only User ☐SWS SDU Finance User ☐ARS SDU Finance User ☐CASES SDU Finance User **Reporting Engine** ☐System Administrator ☐Report Author ☐General User

☐R&L Admin (IT Only) ☐InfoImage Production ☐Archive Administrator ☐Archive General User (Read Only)	**CORE Interface Engine** ☐CIE System Administrator ☐CIE Monitor/Operator
EFT Editor ☐System Administrator ☐General User	**Onyx Ticketing** ☐System Administrator ☐Supervisor/Manager ☐General CSR
Employer Database (not yet deployed) ☐System Administrator ☐General User	**Avaya Phone System** ☐Standard Phone ☐Customer Service Phone
TestTrack Pro ☐System Administrator ☐General User	**Non IV-D Data Collection** ☐General User

J.13 – California SDU LCSA/DCSS System Access Request Form

- ***Please fax completed request from to (916) 567-8881.***
- ***The requestor must be an authorized LCSA/DCSS Manager.***

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Tab after: 0.5" + Indent at: 0.5"

Date of Request:_____ Requester Name:_____ Requestor Title _____

Requestor Signature: _____ Date: _____

User First Name: _____ User MI: _____ User Last Name: _____

User Title: _____ User Location: _____

User E-mail: _____ User Work Phone: _____ User Cell Phone: _____

Department:_____ Manager: _____

☐Existing User ☐New User ☐Remove User Expiration: _____

☐General Staff ☐Supervisor ☐Manager ☐Tester ☐Technical Staff ☐Auditor

User Signature: _____ Date: _____

Systems to be Accessed and Level:

Collections Image Archive	**Disbursements Engine**
☐ LCSA/DCSS Archive Group Manager	☐ LCSA/DCSS Group Manager

APPENDIX K – NOTICE OF SECURITY BREACHES

California Law Regarding Notice of Security Breaches

Legislation: California bills AB 700 and SB 1386, Approved by the Governor 9/25/02

Effective Date: July 1, 2003

Requirements: Persons or businesses maintaining computerized personal information must notify affected persons of any breach of system security. Details are described below.

~~1.~~(1) Data Owners

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.38" + Indent at: 0.38"

General requirement:

Any person conducting business in California who owns or licenses computerized data that includes "personal information" must provide notice of any breach of system security to affected individuals.

What triggers it:

If the data owner

- Discovers of is notified of a breach in system security, and
- Knows or reasonably believes that unencrypted personal information of a California resident was acquired by an unauthorized person, and
- The breach compromises the security, confidentiality or integrity of the personal information.

What data:

"Personal information" means an individual's first name of initial and last name, plus any of the following:

- Social Security Number (SSN)
- Driver's license or state ID
- Account or card number, with any security code necessary for access to the account

Who must be notified:

Any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Form of notice:

May include any of the following methods:

- Written notice
- Electronic notice, if you meet the requirements of the E-Sign Act
- Substitute notice, if cost of notice > $250,000, or if affected persons > 500,000, or if data owner does not have sufficient contact information. Substitute notice requires:
  - E-mail notice if you have e-mail address, and
  - Conspicuous posting on business website, and
  - Notification to major statewide media.
- If you maintain your own notification procedures as part of an information security policy for the treatment of personal information, consistent with *timing* requirements of this law, you may notify persons in accordance with those procedures

Timing of notice:

In the most expedient time possible and without unreasonable delay, but:

- Can first take any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system
- If a law enforcement agency determines that the notification will impede a criminal investigation, can delay notice until the law enforcement agency determines it will not compromise the investigation

~~2.~~(2) Data Maintainers - Not Owners

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.38" + Indent at: 0.38"

General Requirement:

Any person who maintains computerized data that includes personal information the person does not own must comply with all the above requirements, except that notice must be given only to the owner or licensee of the data, not to the individual consumer. The owner or licensee then has the obligation described above to provide notice to consumers.

Remedies:

Any customer injured by a violation of the law can initiate a civil lawsuit to recover damages. In addition, anyone can bring an action to enjoin further violation.

APPENDIX L – SECURITY EVENT FORM

Security Event Report

Event#_____

Event Report:_____/_____/200__ Time:___:___AM / PM

☐ Low Level Event | ☐ Medium Level Event | High Level Event

1.Notification Party Information:

_____ (_____)_____
First MI Last Telephone
E-mail

_____ (_____)_____
First MI Last Telephone
E-mail

_____ (_____)_____
First MI Last Telephone
E-mail

_____ (_____)_____
First MI Last Telephone
E-mail

2. POC Information: _____ (_____)_____
First MI Last POC Telephone
POC E-mail

3. Event Investigation Team Information: ☐ Primary POC ☐ Secondary POC

_____ (_____)_____
First MI Last Telephone
E-mail

_____ (_____)_____
First MI Last Telephone
E-mail

_____ (_____)_____
First MI Last Telephone
E-mail

_____ (_____)_____
First MI Last Telephone
E-mail
Team Findings:_____

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

_____
_____
_____
_____

1.☐ Report Attached

4. Assessment and Containment Manager: _____ (____)_____
_____
First MI Last

Telephone E-mail

Initial Actions Taken:
_____
_____
_____
_____
_____
_____ 1.☐ Report Attached
_____

Notifications:
_____
_____
_____
_____ 1.☐ Report Attached
_____

Recovery Operations:
_____
_____
_____
_____
_____ 1.☐ Report Attached
_____

Lessons Learned:_____
_____
_____
_____
_____
_____ 1.☐ Report Attached
_____

Security Event Report

Event#_____

Event Report:_____/_____/200__ Time:____:____AM / PM

1.☐ Low Level Event	2.☐ Medium Level Event	High Level Event

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

5. POC Information: _____ (_____)_____

_____ First MI Last POC Telephone

POC E-mail

6. Host Information:		2. ☐ Primary POC	2. ☐ Secondary POC
Location of the incident		Time zone for host unit	
Host system name(s)		Host is source/victim or both	
Host system address(s)		Was the host compromised	
Location on the network		What software changed preceded the attack	
Nature of information at risk		Vendor hardware	
Function of the host system		Operating System (ver.)	

7. Incident Type			
	1. ✓		1. ✓
Anonymous FTP abuse		Telnet attack	
Intruder gained privileged access		TFTP attack	
Intruder installed a Trojan horse program		Denial of service attack	
Packet sniffer installed		Email bombardment	
Cracked password or easily guessed password		Email spoofing	
FTP attack		IP spoofing	
NIS attack		Worm	
NFS attack		Other	
Rlogin or rsh attack			

8. Intruder Information	
Intruder(s) MAC address	
Intruder(s) IP address	
Intruder(s) Host name	
Intruder(s) Username	
Trace results	
Finger results	
Netstat results	
Ping results	
Find results	
Who results	
W results	
Last results	
PS results	

9. Additional Notes

Figure L.1: Security Event Form

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

Formatted: Bulleted + Level: 1 + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25"

APPENDIX M – INCIDENT REPORT

CA SDU
Incident Report Form

This form is to be completed by the IT security personnel handling the IT security incident. The report must be filed with the CA SDU Information Security Officer.

Site Name: _____

Name of Person Reporting the Incident: _____

Title of the Person Reporting the Position: _____

Phone Number (s) of Incident Reporter: _____

Email address of Incident Reporter: _____

Date of Incident: _____

Time of Incident: _____

Time Zone (in which incident occurred): _____

What is the operating system, version and patch level of the affected system?
_____

What is the primary function of the affected host?
_____
_____
_____

What primary functions of the host have been impacted by the incident?
_____
_____
_____

What secondary functions have been impacted?
_____
_____
_____

What is the total number of systems attacked _____, number of systems affected (all systems impacted not just those directly attacked)? _____

Type and Criticality of Incident

To determine the incident type and criticality determination refer to "Appendix N" of this document:

High **Medium** **Low**

Criticality (choose from following list):

___ 1. Need assistance immediately
___ 2. Need assistance before the next business day
___ 3. Need assistance early in the next business day
___ 4. Need assistance by the end of the next business day
___ 5. Assistance not required during the next business day or not at all

Using the guidance in section 10.4 of this document to provide a brief description of the **type** of incident below:

_____
_____
_____

If possible record the following information for each system:

Affected systems (Repeat for each system)

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

IP Address (es)

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

Network Locations

_____ _____
_____ _____
_____ _____

GEOGRAPHIC LOCATIONS

_____ _____

_____ _____

Source

Was the source of the attack internal, or external of the local network?

_____

What was the attacker's sources IP address? _____

Was it a source from outside of the United States? Yes / No/Not sure

Other Supporting Information

Ensure all information that might be useful in an investigation of the incident is recorded and preserved. Deletion, modification or destruction of forensic evidence should be avoided at all cost. Examples of such information is but is not limited to:

Log files from systems, firewalls, IDS, network sniffers, mail severs, etc.

Files such as .doc, ,jpg. .imp, etc.

Email messages

Observed behavior

- Corrective actions that have been taken, or that are planned, and Remediation Recommendations

APPENDIX N – COMPUTER SECURITY THREAT LEVELS

Incidents are segregated into three levels. These levels are described below. It should be noted that the examples below are not intended to cover every possible security incident scenario, but moreover to convey what should be considered in the event of an incident. Several factors should also be considered including the scope of the incident (e.g., is the threat wide-spread or localized) and the risk imposed on the affected system.

High-Level Events are the most serious Events and considered "Major" in nature. Because of the gravity of the situation and the high potential for harm to SDU, these incidents should be handled as soon as possible.

High-Level Events Include:

- Suspected Compromise of an Information Resource, Information Asset, or the systems upon which they depend
- Successful Denial of Service Attacks
- Destructive and/or wide-spread Viruses/Worms (high organizational impact)
- Unauthorized use of an Information Asset, Information Resource, or the systems upon which they depend that results in the misuse of SDU Sensitive data
- Property Destruction related to a Security Event (greater than an estimated value of $1000)
- Personal Theft related to a Security Incident (greater than an estimated value of $1000)

Medium-Level Events are more serious and the notification/handling should begin the same day as the occurrence. The decision to escalate is up to the Point of Contact (POC), depending on the Impact of the Intrusion.

Medium-Level Events include:

- Unfriendly Employee Termination
- Violation of Privileged Access
- Unauthorized use of a system for processing or storing SP data
- Property Destruction related to a Security Event (less than an estimated value of $1000)
- Personal Theft related to a Security Incident (less than an estimated value of $1000)

Computer Viruses/Worms (depending on the impact to the Operating Company or staff office and if the Impact affects other Operating Companies or staff offices

Low-Level events are the least severe and should be handled within one working day after the event occurs by the incident response team. Escalation is rarely necessary and can usually be resolved by the incident response team Point of Contact:

Low-Level Events include:

- Loss of Password, either of a particular User, or the loss of a password to a service such as an out-sourced service.
- Suspected sharing of User Accounts
- Misuse of computer equipment, this includes workstations or laptops, servers, Information Resources, Information Assets, or the systems upon which they depend
- Violation of Security Procedures
- Unintentional routine computer activities, such as accidental destruction of files or records.
- Unsuccessful Scans/Probes, for example, if an Intrusion Detection System reports that an Intruder is/has scanned or probed one or more connected systems
- Computer Viruses/Worms (depending on the impact to the Operating Company or staff office)

Appendix 11

Project Security Plan Template

1.0 Introduction

The project security plan outlines security measures to be taken by the project team to secure client information while in custody of the project team. These security measures will apply to First Data employees and contractors.

1.1 Process

Gather Project Security Requirements

- **Identify Information Protection Needs** - The project team works with the client to document the types of information that the team will use. This should be captured in the security planning matrix of this document.

- **Categorize Information by Risk Levels** - Using the standard FIPS 199 security categorization, categorize the information:

Potential Impact			
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring	The disruption of access	The disruption of access	The disruption of access

Potential Impact			
Security Objective	**LOW**	**MODERATE**	**HIGH**
timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

- **Plan Secure Communications** - First Data provides the following common security controls for secure communications:

  ✓ Email is secured via the following means:

  - Email can only be accessed on approved devices. Mobile devices require a secure client app, with prior approval of the device by First Data internal security. Laptop and desktop devices must be connected to the First Data secure network, either directly or via a VPN. Such devices must be a part of a First Data domain.
  - Email has a classification. These are NONE, PUBLIC, PUBLIC RELEASE, RESTRICTED, UNCLASSIFIED, UNOFFICIAL, PROTECTED, SECRET, and TOP SECRET.
  - Email sent to addresses outside of First Data requires confirmation of the email addresses.

  ✓ Email is sent and received (by First Data email client software) over secured (SSL/TLS) connections only.

  In the planning matrix, identify any additional secure communications requirements.

- **Plan Secure Storage** - First Data provides the following common security controls for secure storage:

  ✓ Laptop devices employ full disk encryption.

  ✓ Mobile devices employ full device encryption and passwords.

  In the planning matrix, identify any additional secure storage requirements.

- Identify Team Training Needs - For each information type identified in planning matrix, determine whether additional training is required. An important aspect of this training will be any periodic refresher training.

- Document Rules of Behavior Expectations - In the planning matrix, identify specific expectations for the information types identified.

Implementation

- **Prepare Team** - During the project kick off, discuss project information security requirements as identified in the training matrix.

- **Deliver Necessary Training** - Deliver training as required for the project. Track team member training.

- **Secure Rules of Behavior Agreement** - Develop documented rules of behavior for project team members. Have each team member sign the Rules of Behavior document.

1.2 Security Planning Matrix

This matrix is used for planning the project security. HIPAA PHI is provided as an example.

Information Type	Information Categorization	Requirements			
		Communications	Storage	Training	Rules of Behavior
PHI	{H, M, L}	Communications must be encrypted, either end to end or by encrypted document.	Must be stored encrypted.	Specific HIPAA training is required.	May only be used and communicated for specified purposes. Must be deleted after project completion and end of record retention period.

ORIGIN ID:OXDA (513) 489-9599
JULIE PATEL
FIRST DATA CORPORATION
11311 CORNELL PARK DR

CINCINNATI, OH 45242
UNITED STATES US

SHIP DATE: 16MAY16
ACTWGT: 10.00 LB
CAD: 100563643/INET3730

BILL SENDER

TO J CROUSE /R THOMPSON
NE STATE PURCHASING BUREAU
1526 K ST
SUITE 130
LINCOLN NE 68508
(402) 471-6500
REF: 06275-063960-7671000
INV:
PO:
DEPT:

540J1/6323/727F

FedEx Express

J1610160205 01uv

TUE - 17 MAY 10:30A
PRIORITY OVERNIGHT

TRK# 0201 7830 8138 9610

NA LNKA

68508
NE-US OMA

2016 MAY 17 PM 8 E1

4