



State of Tennessee
Division of Health Care Finance and Administration

**Tennessee Technical Advisory Services
(TN TAS)**

Extract – Quality Management Plan

Version: Extract 1.0
Submitted Date: March 31, 2016

Table of Contents

- 1. Introduction 3
- 2. Quality Management Overview..... 3
- 3. Project Lifecycle Phases & Quality Management 3
- 4. Contractor Expectations 4
- 5. Quality Management Roles and Responsibilities 4

1. Introduction

This document will serve as a precursor to the Quality Management Plan (QM) which will be finalized at a later date. In this extract, QM encompasses both Quality Assurance (QA) and Quality Control (QC). In this instance QA refers to the review of deliverables and QC refers to the review of processes. The intent of this extract is to provide a contextual view of the approach and scope of QM activities that are anticipated to occur throughout the entire lifecycle of the Eligibility Modernization Project (EMP) implementation. This document includes an overview of QM and outlines the roles and responsibilities of all stakeholders, including the System Integrator (SI) roles and responsibilities. The SI should consider this content when defining their project activities and budgeting.

2. Quality Management Overview

QM is the process and philosophy of creating procedures that help ensure that the delivered solution matches the client's needs and that deliverables are produced and reviewed in a uniform manner that meets expected standards.

Specifically, the State defines "quality" as meeting or exceeding the defined requirement, need, or expectation of an activity or product. This applies to singular activities or products throughout the lifecycle and completion of the EMP. The QM Plan pertains to all components of the EMP. These components include program management and staff, contractors, and other participants in the project. It also spans the life of the project from the planning, development, implementation and eventually post-implementation phases.

The QM Plan will describe the review/checkpoint process, authorities, policies, tools, and techniques that will be followed to ensure that the technical solution satisfies requirements, complies with standards and best practices, ensures project excellence, reduces costs, and eliminates unnecessary corrections and/or changes. As the State's QM Plan is being created, the core QM team will be identified. This team will include key members of the State and supporting vendors. The State's QM Plan will evolve as the project progresses, and the Contractor should develop its QM Plan to be closely aligned.

As a public entity, the State regards active engagement of all stakeholders, with accountability to the Project's Executive Steering Committee, the State legislature, and the Federal government, to be essential. The State quality program will balance this external accountability with internal monitoring and controls of operating and administrative processes by developing a comprehensive approach to oversight, monitoring, and performance outcome measurement.

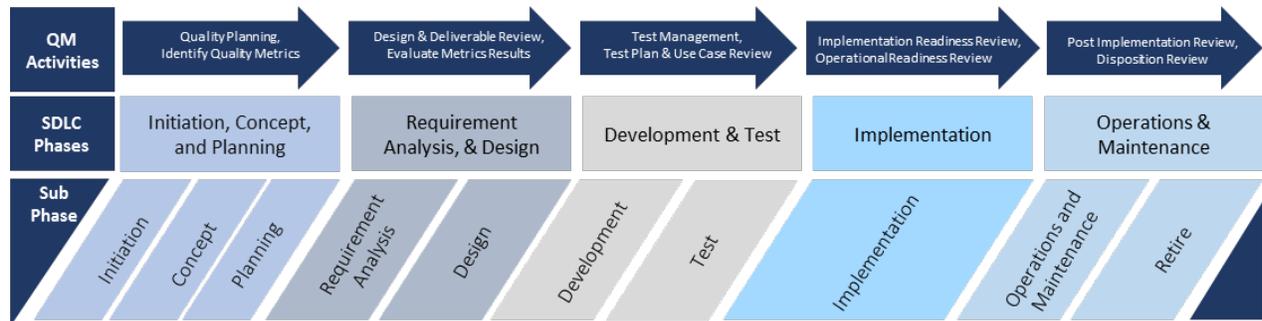
During project initiation, the State will operationalize monitoring activities of its QM function such as:

- Periodic statistics on technical activities from IT Service Management
- Outside quality assistance in planning, implementing, monitoring, and executing the QM Plan by a Technical Advisor Vendor
- Independent periodic reviews of the system design, development, and implementation activities conducted by Independent Verification and Validation (IV&V) Vendor
- On-going compliance with laws, regulations, and policies
- Overall performance improvement

3. Project Lifecycle Phases & Quality Management

The QM approach will encompass both a focused review of System Development Lifecycle (SDLC) deliverables and an overall process improvement review for core project and SDLC disciplines and processes. The QM Plan will directly follow the phases laid out by the SLDC, as seen below. The SI contracted deliverables are cross-referenced and aligned to the SDLC and gate reviews, see Appendix B.

As part of the SDLC activities, the QM team will review the associated deliverables for each phase and provide feedback necessary to ensure the deliverables meet the quality expectations to pass the necessary phase and gate.



For a detailed view of the SDLC, which establishes the roles and responsibilities of each stakeholder, please reference Appendix A. Additionally, reference Appendix A to find the stage at which each stakeholder's role will be integrated into the project.

The State quality program will conduct ongoing evaluation of the project throughout its lifecycle to determine how well it is achieving essential goals. Ongoing evaluation will help State staff identify areas for improvement, make strategic decisions, and demonstrate successes to public officials, State partners, other MMP partners, and other stakeholders.

In addition to the focused effort supporting the gate review activities, the QM scope will be leveraged to drive continuous improvement within the program and project offices. The anticipated scope of these activities will assess the performance of the following functions: SDLC, Project Management, Operations and Maintenance, Governance, and Organizational Change Management. The SI may be required to participate in or supply documentation in support of these QM efforts.

4. Contractor Expectations

The Contractor will support QM reviews performed by the State and its contractors. The Contractor should incorporate QM review results in remediation plans for both current and future project deliverables. Additionally, the Contractor will ensure all supporting documentation is updated in a timely manner to accurately reflect changes required through the QM process.

5. Quality Management Roles and Responsibilities

All members of the project team will play a role in QM. It is imperative that the team ensures that work is completed at an adequate level of quality, from individual work packages to the final project deliverable. The following roles and responsibilities may change or be elaborated throughout the project. The following tasks are high-level and will be further detailed in the completed QM Plan.

System Integrator (SI) Vendor

The following outlines the QM tasks and responsibilities for the SI Vendor:

- Create an internal QM Plan that includes a minimum of QA and QC requirements mandated by the State QM Plan
- Communicate results and progress of build / design to all relevant stakeholders
- Follow all QC process measures within the design phase of the project build

- Participate and support deliverable reviews including walkthrough meetings, deliverable review sessions, and remediation of review feedback
- Participate in HCFA and CMS phase gate reviews, including planning up to six (6) weeks in advance of gate. This includes all pre-requisites to the gate including but not limited to walkthroughs, dry runs, demo days, and remediation of CMS requests.
- All sixty (60) SI deliverables outlined in the RFQ will be subject to the QM review process and CMS review

Technical Advisory Services (TAS) Vendor

The following outlines the QM tasks and responsibilities for the TAS Vendor:

- Assist the State in QM activities, including managing quality reviews and overseeing follow-up corrective actions
- Assist the State with planning, implementing, and executing the QM Plan throughout the duration of the project
- Support the State in carrying out approved remediation activities
- Draft the QM Plan to ensure all tasks, processes, and documentation are compliant with the plan
- Monitor quality and report exceptions to the executive sponsors (Steering Committee) and the project sponsor as part of monthly status reporting, or more frequently if conditions warrant
- Schedule regularly occurring meetings to review the findings of the QM activities. In these reviews, agenda items will include review of project processes, any discrepancies and/or findings from the deliverable reviews, and discussion of process improvement initiatives.
- Participate in deliverable review and gate review as requested by the State

The State/ Project Sponsor

The following outlines the QM tasks and responsibilities for the Project Sponsor:

- Sign-off authority on the final acceptance of project deliverables
- Approve all quality standards for the project
- Review quality reports and assist in resolution of escalated issues

State Project Management Office (SPMO)

The following outlines the QM tasks and responsibilities for the SPMO:

- Track project deliverable dates as well as project risks and issues that are reported from the State or any Project vendor throughout the quality review process
- Assess and report the impact of late deliverables that will push out the overall timeline or have an impact on other deliverables
- Track the deliverable review cycle to ensure that all vendors and State staff adhere to the correct review cycle timeframe
- Track to ensure that phase gates are met in a timely manner

Independent Validation and Verification (IV&V) Vendor

The following outlines the QM tasks and responsibilities for the IV&V Vendor:

- Review the SI's required reporting, specifically quality reporting and quality remediation reports
- Serve as a third party to ensure all quality remediation is executed
- Serve as a third party to assess on-going project progression
- Provide HCFA management an objective analysis to help manage system transition issues and make informed decisions
- Provide HCFA management with increased and objective visibility into the progress and quality of the transition/turnover effort

The RACI's below is an extract from A.25 Project and Systems Development Lifecycle Management Plan. For purposes of the Quality Assurance Plan all Items that the SI is responsible for are subject to review as described in the Quality Management Artifact.

- Provide HCFA management with increased oversight in requested and delivered turnover documents and other business products

APPENDIX A

RACI Participants Definitions		
State	Program and Project Management	The management team that includes the Medicaid Modernization Program (MMP) Director and assigned Project Managers.
	HCFA Business	Organizational units that oversee the policies and operations of HCFA business functions, such as member services.
	HCFA IS	HCFA IS provides support for planning, design, implementation and operation of information technologies and methodologies.
	HCFA Enterprise Security	HCFA's enterprise security, includes HCFA & contractor resources responsible for reducing the risk of unauthorized access to systems and data.
	STS (Infrastructure)	Strategic Technology Solutions provides direction, planning, resources, execution, and coordination in managing the information systems needs of the State of Tennessee. STS is a division within the Department of Finance & Administration.
MMP Contractors	TAS	Technical Advisory Services supports and advises the State in completing the Medicaid Modernization Program (MMP) by offering Organizational Change Management and Training, Operations & Maintenance Planning, System Development Life Cycle Guidelines and Governance, Quality Management, and Enterprise Architecture services.
	SPMO	The Strategic Program Management Office provides program and project management support to the State in completing the MMP
	IV&V	IV&V is responsible for assessing the correctness and quality of a project's product. IV&V reviews, analyzes, evaluates, and inspects the project's product and processes. This analysis can include the operational environment, hardware, software, interfacing applications, documentation, operators, and users to help ensure that the product is well-engineered, and is being developed in accordance with customer requirements. IV&V provides management with an independent perspective on project activities and promotes early detection of project/product variances. This allows the project to implement corrective actions to bring the project back in-line with agreed-upon expectations.
	SI	The System Integrator is responsible for the design, development, testing, implementation, and the operations and maintenance (O&M) of a new system to modernize and enhance eligibility determination, redetermination, and eligibility appeals for the State of Tennessee's Medicaid program (TennCare) and Children's Health Insurance Program (CHIP, known as CoverKids in Tennessee).

Key

Responsible	Accountable	Consulted	Informed	Shared Responsibility
R	A	C	I	SR



INITIATION PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
<i>Activities</i>									
Identify a State Business Owner responsible for formalizing a Business Case in collaboration with all State resources	A	C	C	R	I	-	I	I	I
Develop a Scope Definition that includes at a minimum: Detailed explanation of the business need Identification of key stakeholders High-level requirements Known risks or issues with the project High-Level Business Impact Goals and scope of the proposed project A Rough Order of Magnitude (ROM) estimate for the proposed project schedule, efforts, costs, materials, and equipment Alternatives Analysis	A	C	C	C	I	-	R	SR	I
Develop Statement of Work (SOW)	A	R	C	I	C	-	SR	C	I
Develop Risk Management Plan	A	C	C	C	I	-	R	SR	I
Develop Project Charter	A	C	I	I	I	-	C	R	I
<i>Deliverables Produced or Updated During This Phase</i>									
Project Charter	A	C	I	I	I	-	C	R	-
Stakeholder Register	C	A	C	C	C	-	R	SR	C
Acquisition Strategy (Final)*	A	C	I	C	I	-	R	I	I
Risk Analysis (Final)*	A	C	C	C	C	-	R	C	I
Scope Definition (Final)*	A	C	C	I	I	-	R	SR	I
Project Management Plan (Preliminary)*	C	A	C	C	I	-	R	SR	I
Concept of Operations (Preliminary)*	A	C	C	C	I	-	R	I	I
Alternatives Analysis (Final)*	C	A	C	C	I	-	R	I	I
Performance Measures (Final)*	C	A	C	SR	I	-	R	SR	I

* Needed for Project Startup Consult Gate

Phase Gate: Project Startup Consult Complete



CONCEPT PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
<i>Activities</i>									
Perform a detailed analysis to validate that the proposed project will deliver the desired business result (e.g., reduce risk, regulatory compliance, improved business performance, cost savings)	SR	A	C	C	C	-	R	I	I
Perform Security Impact Analysis	C	A	R	I	C	-	C	I	I
Perform Privacy Impact Assessment	C	A	R	I	C	-	C	I	I
Develop Business Risk Assessment	R	A	C	SR	I	-	R	I	I
Create Risk Register, Issue Log, Assumptions Log and Decisions Log	A	C	C	I	C	-	C	R	I
Collect initial Requirements	A	C	C	C	C	-	R	I	I
Finalize the Business Case	A	C	C	C	I	-	R	I	C
Finalize the Project Charter	A	C	C	I	I	-	C	R	C
Prioritize projects as part of the overall Portfolio	A	C	C	SR	C	-	C	R	I
Review Rough Order Magnitude (ROM)	A	C	I	I	I	-	R	R	I
<i>Deliverables Produced or Updated During This Phase</i>									
Advance Planning Document (APD) / Implementation Advanced Planning Document (IAPD)	A	C	C	I	I	-	R	I	C
Business Case	A	C	C	C	I	-	R	I	C
Project Charter	A	C	C	I	I	-	C	R	C
Risk Register (Preliminary)	A	C	C	I	C	-	C	R	I
Issue Log	A	C	C	I	C	-	C	R	I
Assumptions Log	A	C	C	I	C	-	C	R	I
Decisions Log	A	C	C	I	C	-	C	R	I
Security Impact Analysis	C	A	R	I	C	-	C	I	I
Privacy Impact Assessment	C	A	R	I	C	-	C	I	I
Business Risk Assessment	A	C	C	I	I	-	R	I	I
Concept of Operations (Baseline)*	A	C	C	I	I	-	R	I	I
Project Management Plan (Preliminary)*	C	A	C	C	I	-	SR	R	I

CONCEPT PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
Alternatives Analysis (Final)*	C	A	C	C	I	-	R	I	I
MITA Self-Assessment /MITA Roadmap (Updated)*	C	A	C	I	-	-	R	-	-
Architectural Diagrams (Final)*	C	A	C	I	I	-	R	I	I
Business Process Models (Final)*	R	A	C	I	I	-	R	I	I

* Needed for Architecture Review Gate

Phase Gate: Architecture Review Complete



PLANNING PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
<i>Activities</i>									
Finalize Project Process Agreement	C	A	I	C	C	R	C	SR	-
Prepare RFP & Evaluate responses	SR	A	C	C	I	I	R	C	C
Update Statement of Work	A	C	C	C	C	I	R	C	C
Finalize SI Contractor contract	C	A	C	C	C	I	C	C	C
Establish a Project organizational structure to execute the project including defined roles, responsibilities and approval levels.	A	C	C	C	C	C	C	R	C
Create Solution Alternatives Analysis	C	A	C	C	C	R	SR	C	I
Collect requirements needed to support the SI and solution procurement	A	C	C	C	C	I	R	I	I
Start the acquisition process, and determine key acquisition-related activities and items (e.g., costs for hardware, software, and service acquisitions)	C	A	C	C	C	C	R	R	I
Identify Resources (Internal / External / Hardware / Software) required for the Project.	A	C	C	C	C	C	R	SR	I
Develop High Level Work Breakdown Structure (WBS)	C	C	C	C	C	SR	C	R,A	C
Update Project Management Plan, including establishment of cost, scope and schedule baseline	C	A	C	C	I	C	R	R	I
Conduct Kick-Off meeting (Discuss Project Scope / Review Project Process Agreement / Approach)	C	C	C	A	I	R	C	SR	C
Set-up processes and standards to manage project risks, issues, assumptions, action items and constraints.	C	C	C	A	C	R	C	SR	C
Identify Solution Development Methodology (SDM) with supporting justification.	I	C	I	I	I	R	A	C	C
Develop all required Management plans for SDLC project activities for State approval.	C	A	C	C	I	R	C	C	I
Develop High-Level Solution Design	C	A	C	I	C	R	C	I	I
<i>Deliverables Produced or Updated During This Phase</i>									
Key Performance Indicator Management Plan	C	A	I	C	-	R	C	SR	C
Requirements Management Plan	A	C	C	C	C	R	SR	C	C

PLANNING PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
Business Rules Management Plan	A	C	C	C	-	R	C	C	C
Design Management Plan	C	A	C	C	C	R	C	C	C
Test Management Plan	C	A	C	C	C	R	C	C	C
Implementation and Deployment Plan	C	A	C	C	C	R	C	C	C
Data Conversion and Synchronization Plan	C	A	C	C	C	R	C	C	C
System Security Plan	C	C	A	C	C	R	C	I	C
Business Continuity and Disaster Recovery Plan	A	R	C	C	C	SR	C	C	C
Capacity Plan	I	A	C	C	C	R	C	I	C
Data Management Plan	C	A	C	C	C	R	C	C	C
Performance and Availability Plan	C	A	C	C	C	R	C	C	C
Work Breakdown Structure (WBS)	C	A	C	C	C	R	C	SR	C
Risk Register (Interim)	C	C	C	A	C	R	C	SR	C
Baselined Work Plan and Schedule	A	C	C	C	C	R	C	SR	C
Status Reports	C	C	C	A	-	R	C	SR	C
Financial Status Report	C	C	I	A	-	R	I	SR	I
Solution Alternatives Analysis	C	A	C	C	C	R	SR	C	I
Project Process Agreement	C	A	I	C	C	R	C	SR	I
Concept of Operations (Final)*	A	C	-	C	R	I	I	I	I
Project Management Plan (Baselined)*	C	A	-	C	R	SR	C	I	I
Privacy Impact Assessment (Baselined)*	C	A	-	R	C	-	I	I	C
Project Management Schedule (Baselined)*	C	C	C	A	C	R	C	SR	C
Project Process Agreement (Final)*	C	A	R	I	C	-	C	SR	C
Release Plan (Baselined)*	C	A	C	C	C	R	C	C	C

* Needed for Project Baseline Review Gate

Phase Gate: Project Baseline Review Complete
--



REQUIREMENTS ANALYSIS PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
<i>Activities</i>									
Establish “as is” and “to be” process and perform gap analysis.	A	C	C	C	I	R	C	C	I
Identify opportunities for process optimization/re-design consistent with State Enterprise Architecture.	A	C	C	C	I	R	C	C	I
Identify and document any new requirements including business, stakeholder, solution (functional and non-functional), project, and quality and transition requirements.	A	C	C	C	C	R	SR	C	C
Develop Detailed Requirements Traceability Matrix	A	C	I	C	I	R	C	I	I
Develop detailed requirement documents for State approval, such as Business Requirements Documents (BRD) and Business Process Flow Diagrams.	A	C	I	C	I	R	C	I	I
Enhance Business Process flows to align with changed requirements while staying in conformity with the State Enterprise Architecture	A	C	I	C	I	R	C	I	I
Requirements have been prioritized.	A	C	I	C	I	R	SR	C	I
<i>Deliverables Produced or Updated During This Phase</i>									
Requirements Specification Document	A	C	I	I	I	R	C	I	I
Detailed Requirements Traceability Matrix	A	C	I	I	I	R	C	I	I
Business Process Flow Diagrams	A	C	I	I	I	R	C	I	I
Project Management Plan (Updated)*	C	A	C	C	I	-	R	SR	I
Solution Alternatives Analysis (Baseline)*	C	A	C	C	I	-	R	I	I
Business Requirements (Updated)*	A	C	C	C	C	R	SR	I	C
Business Rules (Preliminary)*	A	C	I	C	I	R	SR	I	I
System Security Plan (Preliminary)*	C	C	A	C	I	R	C	I	I
Information Security Risk Assessment (Preliminary)*	C	C	A	C	I	R	C	I	I
Test Plan (Preliminary)*	C	A	C	C	C	R	C	I	C
Service Level Agreements (SLAs) / Memorandum of Understandings (MOUs) (Preliminary)*	C	A	C	C	SR	R	C	C	C
Requirements Document (Preliminary)*	A	C	I	C	I	R	SR	I	I

REQUIREMENTS ANALYSIS PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
Technical Architecture Diagrams (Baselined)*	C	A	C	C	C	R	SR	I	C
Logical Data Model (Preliminary)*	C	A	C	C	C	R	C	I	C

* Needed for Preliminary Design Consult Review Gate

Phase Gate: Preliminary Design Consult Complete



DESIGN PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
<i>Activities</i>									
Perform design sessions incorporating architecture, business, design, and IT resources to refine and review business requirements.	A	C	C	I	C	R	C	C	C
Develop Functional Design Document.	A	C	C	I	I	R	C	I	I
Develop Technical Design Document.	C	A	C	I	C	R	C	I	C
Develop Interface Control Document.	C	A	C	I	C	R	C	I	C
Develop screen mock-ups, layouts as applicable.	A	C	I	I	I	R	I	I	I
Identify Modular code snippets that could be placed in a State managed repository.	C	A	I	I	I	R	I	I	I
Develop any new requirements resulting out of the Design phase.	A	C	I	I	I	R	I	I	I
Perform data conversion for User Acceptance Testing (UAT)	C	A	C	I	I	R	C	I	I
<i>Deliverables Produced or Updated During This Phase</i>									
System Architecture Design Document	A	C	C	I	C	R	C	I	C
Data Dictionary	C	A	C	I	I	R	C	I	I
Service Oriented Architecture (SOA) Models	C	A	C	I	I	R	C	I	I
Functional Design Document (including Use Cases)	A	C	C	I	I	R	C	I	I
Technical Design Document	C	A	C	I	C	R	C	I	C
Project Management Plan (Updated)*	C	A	C	C	I	R	SR	SR	I
Solution Alternatives Analysis (Baseline)*	C	A	C	I	C	R	SR	C	I
Business Requirements (Updated)*	A	C	C	I	C	R	SR	I	C
Business Rules (Baseline)*	A	C	I	I	I	R	SR	I	I
System Security Plan (Updated)*	C	SR	A	I	I	R	C	I	I
Information Security Risk Assessment (Updated)*	C	SR	A	I	I	R	C	I	I
Test Plan (Updated)*	C	A	C	C	C	R	C	I	C
SLAs/MOUs (Updated)*	C	A	C	C	SR	R	C	C	C
Systems Design Document (Preliminary)*	C	A	C	C	C	R	I	I	I

DESIGN PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
Data Conversion Plan (Preliminary)*	C	A	C	C	I	R	C	I	C
Implementation Plan (Preliminary)*	C	A	C	C	SR	R	C	I	C
Requirements Document (Baseline)*	A	C	I	I	I	R	SR	I	I
Interface Control Document (Preliminary)*	C	A	C	I	C	R	C	I	C
Database Design Document (Preliminary)*	C	A	C	I	C	R	C	I	C
Data Management Plan (Preliminary)*	C	A	C	C	C	R	C	I	C
Physical Data Model (Preliminary)*	C	A	C	C	C	R	C	I	C
Project Management Plan (Updated)§	C	A	C	C	I	-	R	SR	I
Solution Alternatives Analysis (Baseline)§	C	A	C	I	C	R	SR	C	I
Business Requirements (Baseline)§	A	C	C	I	C	R	SR	I	C
Business Rules (Baseline)§	A	C	I	I	I	R	SR	I	I
System Security Plan (Baseline)§	C	SR	A	I	I	R	C	I	I
Information Security Risk Assessment (Baseline)§	C	SR	A	I	I	R	C	I	I
Test Plan (Baseline)§	C	A	C	C	C	R	C	I	C
SLAs/MOUs (Updated)§	A	C	C	I	SR	R	C	C	C
Implementation Plan (Baseline)§	C	A	C	C	SR	R	C	I	C
Contingency / Recovery Plan (Preliminary)§	C	A	C	C	SR	R	C	C	I
Manuals and Training Materials (Preliminary)§	A	C	C	I	C	C	R	C	C
Data Use / Exchange Interconnection Security Agreement (Preliminary)§	C	A	SR	I	I	R	C	I	I
Requirements Document (Updated)§	A	C	C	I	C	R	SR	I	C
System Design Document (Baseline)§	C	A	C	C	C	R	I	I	I
Interface Control Document (Baseline)§	C	A	C	I	C	R	C	I	C
Database Design Document (Baseline)§	C	A	C	I	C	R	C	I	C
Data Management Plan (Baseline)§	C	A	C	C	C	R	C	I	C
Logical Data Model (Baseline)§	C	A	C	C	C	R	C	I	C
Physical Data Model (Baseline)§	C	A	C	C	C	R	C	I	C
Data Conversion Plan (Baseline)§	C	A	C	C	I	R	C	I	C
System of Record Notice (Preliminary)§	R	A	I	I	I	I	I	I	I

* Needed for Detailed Design Consult Review Gate

§ Needed for Final Design Review Gate

Phase Gate: Detailed Design Consult Complete
Final Detailed Design Review Complete



DEVELOPMENT PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
<i>Activities</i>									
Configure and integrate necessary infrastructure and associated products.	I	A	C	I	R	R	C	I	I
Ensure adequate time for construction, peer review, unit testing and walkthrough; as well as adequate time for rework and unit testing of defective code.	I	A	I	I	I	R	C	I	C
Implement changes needed to business product (E.g., code, configuration change)	C	A	I	I	I	R	C	I	I
Perform Development Testing to include: <ul style="list-style-type: none"> Unit Testing Application Integration Testing Section 508 Testing and Accessibility Testing 	I	A	I	I	I	R	C	I	C
Transfer solution to Testing Team	I	A	I	I	I	R	C	I	C
Identify personnel and/or review teams responsible for approving test results as appropriate	C	A	I	C	I	R	C	I	C
Define unit test review process with objectives and criteria for migrating from unit test to the integration test environment.	C	A	I	C	I	R	C	I	C
<i>Deliverables Produced or Updated During This Phase</i>									
Automated Code Review Results	I	A	C	I	C	R	C	I	C
System Configuration Document	I	A	C	I	I	R	C	I	C
Unit, System and Integration Test Scripts	I	A	I	I	I	R		I	C
Project Schedule (Interim)*	C	C	C	A	C	C	R	SR	C
Risk Register (Interim)*	C	C	C	A	C	C	R	SR	C
Issues List (Interim)*	C	C	C	A	C	C	R	SR	C
Action Items (Interim)*	C	C	C	A	C	C	R	SR	C
Decision Log (Interim)*	C	C	C	A	C	C	R	SR	C
Lesson Learned Log (Interim)*	C	C	C	A	C	C	R	SR	C
Privacy Impact Assessment (Interim)*	C	A	R	I	C	-	C	I	I
System Security Plan (Interim)*	C	SR	A	I	I	R	C	I	I

DEVELOPMENT PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
Information System Risk Assessment (Interim)*	C	SR	A	I	I	R	C	I	I
Information System Description (Interim)*	C	A	C	I	C	R	C	C	C
Monitoring Strategy (Updated)*	C	A	C	I	C	R	C	I	C
Security Control Description (Final)*	C	C	A	I	C	R	C	I	C
Software Assurance Misuse Cases (Interim)*	C	C	A	I	C	R	C	I	C
Contingency Plan (Final)*	C	A	C	I	C	R	C	C	C
Section 508 Assessment Package (Interim)*	C	A	C	I	I	R	I	I	I
Test Plan (Baseline)*	C	A	C	C	C	R	C	I	C
Database Design Document (Final)*	C	A	C	I	C	R	C	I	C
Data Use Agreement (Interim)*	C	C	A	I	I	R	C	I	I
Test Case Specification (Final)*	C	A	C	I	C	C	R	I	C
Data Conversion Plan (Final)*	C	A	C	C	I	R	C	I	C
Implementation Plan (Interim)*	C	A	C	I	SR	R	C	I	C
User Manual (Interim)*	A	C	C	I	C	R	C	C	C
Operations & Maintenance Manual (Interim)*	I	A	C	I	C	R	C	C	C
Performance Test Plan and Results Template (Interim)*	C	A	C	I	C	R	C	C	I
Business Product/Code (Preliminary / Baseline)*	I	A	C	I	C	C	R	C	C
Version Description Document (Preliminary)*	I	A	C	I	C	C	R	C	C
Training Plan (Preliminary)*	A	I	C	I	C	SR	R	C	C

* Needed for Validation Readiness Review Gate

Phase Gate: Validation Readiness Review Complete
--



TEST PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
<i>Activities</i>									
Perform functional testing to include : <ul style="list-style-type: none"> Unit Testing System Testing 	C	A	C	I	C	R	SR	C	C
Ensure readiness for Infrastructure (non- functional) testing: <ul style="list-style-type: none"> Performance Testing Security Testing Capacity Testing Accessibility Testing Volume Testing Recovery Testing Stress Testing Penetration Testing 	C	A	C	I	C	R	SR	C	C
Manage defects through the Defect Management Process, outlined in the Test Management Plan.	C	A	C	I	C	R	C	C	C
Perform System integration testing to include testing at <ul style="list-style-type: none"> Functional level Inter module level 	C	A	C	I	C	R	SR	C	C
Perform End-to-End testing	C	A	C	I	C	R	SR	C	C
Perform User Acceptance Testing	A	R	C	I	I	SR	C	I	C
Perform Operational Readiness Testing to validate: <ul style="list-style-type: none"> UAT certified solution can be supported by the infrastructure Business continuity and disaster recovery procedures Infrastructure and network troubleshooting procedures 	C	A	C	I	C	R	SR	C	C
Execute all test steps within each test case and provide proof for the test results.	C	A	I	I	-	R	-	-	C
Document and re-test all defect remediation, perform regression testing in conjunction with all defect remediation releases	C	A	C	I	C	R	C	C	C

TEST PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
Identify and document any new risks and issues as part of test execution.	C	A	C	I	C	R	C	C	C
<i>Deliverables Produced or Updated During This Phase</i>									
Unit, System & Integration Testing Test Results	C	A	C	I	C	R	C	C	C
System Readiness Certification for UAT	C	A	C	I	C	R	C	I	I
Formal Acceptance Testing Report	A	C	C	I	C	R	C	C	C
Contingency/Recovery Plan	C	A	C	I	C	R	C	C	C
Beta Test Plan	A	C	C	I	C	R	C	C	C
Network Vulnerability Assessment Resolution Report	I	C	A	I	C	R	C	C	C
Project Schedule (Interim)*	C	C	C	A	C	R	C	SR	C
Risk Register (Interim)*	C	C	C	A	C	R	C	SR	C
Issues List (Interim)*	C	C	C	A	C	R	C	SR	C
Action Items (Interim)*	C	C	C	A	C	R	C	SR	C
Decision Log (Interim)*	C	C	C	A	C	R	C	SR	C
Lesson Learned Log (Interim)*	C	C	C	A	C	R	C	SR	C
Privacy Impact Assessment (Final)*	C	C	A	I	C	R	C	I	I
System Security Plan (Final)*	C	C	A	I	I	R	C	I	I
Information System Risk Assessment (Final)*	C	C	A	I	I	R	C	I	C
Information System Description (Baseline)*	C	A	C	I	C	R	C	C	C
Monitoring Strategy (Updated)*	C	A	C	I	C	R	C	I	C
Security Control Description (Updated)*	C	C	A	I	C	R	C	I	C
Software Assurance Misuse Cases (Final)*	C	C	A	I	C	R	C	I	C
Contingency Plan (Updated)*	C	A	C	I	C	R	C	C	C
Contingency Plan Test (Preliminary / Final)*	C	A	C	I	C	R	C	C	C
Security Control Assessment (Preliminary)*	C	C	A	I	C	R	C	I	C
Section 508 Assessment Package (Interim)*	C	A	C	I	I	R	I	I	I
Data Use Agreement (Interim)*	C	C	A	I	I	R	C	I	I
Implementation Plan (Interim)*	C	A	C	I	SR	R	C	I	C
User Manual (Interim)*	A	C	C	I	C	R	C	C	C
Operations & Maintenance Manual (Interim)*	C	A	C	I	C	R	C	C	C

TEST PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
Performance Test Plan and Results Template (Final)*	C	A	C	I	C	R	C	C	I
Version Description Document (Baseline)*	C	A	C	I	C	R	C	C	C
Test Summary Report (Preliminary)*	C	A	C	I	I	R	C	I	C
Training Artifacts (Preliminary)*	A	C	C	I	C	C	R	C	C

* Needed for Implementation Readiness Review Gate

Phase Gate: Implementation Readiness Review Complete



IMPLEMENTATION PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
<i>Activities</i>									
Train end users	A	C	C	I	C	C	R	C	C
Perform data conversion	C	A	C	I	I	R	C	I	I
Verify system results	A	C	C	I	C	R	C	I	C
Update system maintenance and support documentation as needed	C	A	C	I	C	R	C	C	C
Conduct beta testing	A	C	C	I	C	R	C	C	C
Verify system performance against SLAs	C	A	C	I	C	SR	C	I	I
<i>Deliverables Produced or Updated During This Phase</i>									
Beta Test Evaluation Report	R	A	C	I	I	SR	C	I	C
Privacy Impact Assessment	C	C	A	I	I	R	C	I	I
Information Security Risk Assessment	C	C	A	I	I	R	C	I	C
Data Use/ Data Exchange/ Interconnection Security Agreements	C	C	A	I	C	R	C	I	C
MARS-E Security Controls	I	C	A	I	I	R	C	I	C
IRS Safeguards Procedures Report (SPR)	I	C	A	I	I	R	C	I	C
Site Readiness Reports	A	C	C	I	C	R	C	I	I
System Operations Documentation	I	A	C	I	I	R	C	I	C
System Maintenance, Support and System Transition Plan	I	A	C	I	C	R	C	I	C
Infrastructure, System Source Code and Documentation	I	A	C	I	C	R	C	I	C
Updated Infrastructure, System Source Code and Design Documentation	I	A	C	I	C	R	C	I	C
Infrastructure Services Deployment Report	I	A	C	I	C	R	I	I	I
Plan of Action and Milestones (POA&M)	I	C	A	I	C	R	SR	C	C
Interconnected Systems Agreement (ISA)	I	C	A	I	I	R	C	I	C
Training Plan	A	C	C	I	C	R	SR	C	C
Project Schedule (Final)*	C	C	C	A	C	R	C	SR	C
Risk Register (Final)*	C	C	C	A	C	R	C	SR	C
Issues List (Final)*	C	C	C	A	C	R	C	SR	C

IMPLEMENTATION PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
Action Items (Final)*	C	C	C	A	C	R	C	SR	C
Decision Log (Final)*	C	C	C	A	C	R	C	SR	C
Lesson Learned Log (Final)*	C	C	C	A	C	R	C	SR	C
Information System Description (Final)*	I	A	C	I	C	R	C	C	C
Security Control Assessment (Final)*	I	C	A	I	C	R	C	I	C
Authority To Operate (ATO) Submission (Preliminary / Final)*	I	C	A	I	I	R	C	I	C
Plan of Action & Milestones (Preliminary / Final)*	C	C	A	C	C	R	SR	C	C
CMS CIO-Issued ATO (Preliminary / Final)*	C	C	A	I	I	R	C	I	C
Section 508 Assessment Package (Final)*	C	A	I	I	I	R	I	I	I
Data Use Agreement (Final)*	C	C	A	I	I	R	C	I	I
Implementation Plan (Final)*	C	A	C	C	SR	R	C	I	C
User Manual (Final)*	C	A	C	I	C	R	C	C	C
Operations & Maintenance Manual (Final)*	I	A	C	I	C	R	C	C	C
Test Summary Report (Final)*	A	A	C	I	I	R	C	I	C
Training Artifacts (Final)*	A	SR	C	I	C	C	R	C	C

* Needed for Operational Readiness Review Gate

Phase Gate: Operational Readiness Review Complete



OPERATIONS AND MAINTENANCE PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
<i>Activities</i>									
Perform routine maintenance: bug fixes, minor change requests, and patches within the scope of service level agreements	I	A	C	I	C	R	C	I	C
Manage Application Software Installation(s), Application Life Cycles, Manage Application Health Assessments, Application Portfolio, Support Vendors Manage App Availability, App Performance, Knowledge Assets, Maintenance & License Agreements and all environments' Changes	I	A	C	I	C	R	C	I	C
Continuously monitor and improve upon processes and technology	I	A	C	I	C	R	C	C	C
Establish a strategy for managing O&M releases including identifying and documenting procedures concerning recovery/back out in the event of a failure during implementation of a release	I	A	C	I	C	R	C	C	C
Identify and document procedures concerning restart/recovery in the event of a system failure and for continuity of operations in the event of emergencies	C	A	C	I	C	R	C	I	C
Conduct continuous security monitoring of selected controls on an ongoing basis to ensure that maintenance patches and enhancements have not introduced any vulnerabilities.	I	C	A	I	C	R	C	I	I
Perform annual Operational Analysis adequately to evaluate system performance, user satisfaction with the system, adaptability to changing business needs, and new technologies that might improve the system.	C	A	C	I	C	R	C	C	C
<i>Deliverables Produced or Updated During This Phase</i>									
SLA, System Performance, System QA Reports	C	A	C	I	C	R	C	C	C
System Incident and Corrective Maintenance Reports	I	A	C	I	C	R	C	C	C
Monthly Operation Report	I	A	C	I	C	R	C	C	C
Annual Operational Readiness Report	C	A	C	I	C	R	C	C	C
Warranty Completion Report	C	A	C	I	C	R	C	C	C

OPERATIONS AND MAINTENANCE PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
Post Implementation Report	C	A	C	C	C	R	C	C	C
O&M Run-book	I	A	C	I	C	R	C	C	C
Business Case Analysis	A	C	C	I	C	R	C	C	C
Contingency/ Recovery Plan	C	A	C	C	C	R	C	C	C
Project Closeout Report (Preliminary / Final)*	SR	SR	C	A	C	R	C	C	C
Privacy Impact Assessment (Updated)*	C	C	A	I	C	R	C	I	I
System Security Plan (Updated)v	C	C	A	I	I	R	C	I	I
Business Risk Assessment (Updated)*	R	C	A	I	I	R	C	C	I
Information System Risk Assessment (Updated)*	C	A	SR	I	I	R	C	I	C
Information System Description (Updated)*	C	A	C	I	C	R	C	C	C
Security Requirements (Updated)*	C	C	A	I	I	R	C	I	I
Monitoring Strategy (Updated)*	C	A	SR	I	C	R	C	I	C
Security Control Description (Updated)*	C	C	A	I	C	R	C	I	C
Software Assurance Misuse Cases (Updated)*	C	C	A	I	C	R	C	I	C
Contingency Plan (Updated)*	C	A	C	I	C	R	C	C	C
Contingency Plan Test (Updated)*	C	A	C	I	C	R	C	C	C
Security Control Assessment (Updated)*	C	A	A	I	C	R	C	I	C
ATO Submission (Updated)*	C	C	A	I	I	R	C	I	C
Plan of Action & Milestones (Updated)*	C	C	A	I	C	R	R	C	C
CMS CIO-Issued ATO (Updated)*	I	C	A	I	I	R	C	I	C
Security Monitoring Reports (Updated)*	I	C	A	I	C	R	C	I	I
System Disposition Plan (Preliminary / Final)*	C	A	C	I	C	R	C	C	C
Post-Implementation Report (Preliminary / Final)*	A	C	C	C	C	I	R	C	C
Annual Operational Analysis Report (Preliminary / Final)*	C	A	C	I	C	C	R	C	C

* Needed for Post Implementation Review Gate

Phase Gate: Post Implementation Review Complete



RETIRE PHASE	STATE					CONTRACTOR			
	HCFA BUSINESS	HCFA IS	HCFA ENTERPRISE SECURITY	PROGRAM & PROJECT MANAGEMENT	STS (INFRASTRUCTURE)	SI	TAS	SPMO	IV&V
<i>Activities</i>									
Develop back out plan for retirement of a system release or retirement of the entire system.	C	A	C	C	C	R	C	C	C
Perform Legacy Analysis to identify, analyze and address interfaces of the system to be retired with other systems. Also include a complete assets inventory (software, hardware, services, etc.)	C	A	C	C	C	R	C	C	C
Develop program to remove the system to be retired and its data, including performing data conversion, security and impact analysis and other system updates and data migration.	C	A	C	C	C	R	C	C	C
Perform changes to other systems that interface with the system to be retired.	C	A	C	C	C	R	C	C	C
Test the programs used to retire the system and any systems interfaced to the retired system.	R/S	A	C	I	C	R	C	C	C
Translate legacy data as appropriate, and delete any scheduled jobs including backups.	C	A	C	C	-	R	C	C	C
Continuously update System Overview Documentation.	C	A	I	I	-	R	C	I	I
Archive system data, documentation and vestiges.	C	A	I	I	-	R	C	I	I
<i>Deliverables Produced or Updated During This Phase</i>									
System Overview Document	C	A	C	I	C	R	C	C	C
Back out Plan	C	A	C	C	C	R	C	C	C
Operations & Support procedures	C	A	C	I	C	R	C	C	C
System Security Plan (Updated)*	C	C	A	I	I	R	C	I	I
Business Risk Assessment (Updated)*	C	C	A	I	I	R	C	C	I
Information System Risk Assessment (Updated)*	C	C	A	I	I	R	C	I	C
Information System Description (Updated)*	C	A	C	I	C	R	C	I	I
Monitoring Strategy (Updated)*	C	A	SR	I	-	R	C	I	C
System Disposition Plan / Report*	C	A	C	I	-	R	C	C	C

* Needed for Disposition Review Gate

Phase Gate: Disposition Review Complete

APPENDIX B

Key

Deliverable Classification	Length of State Review Period for each Review Cycle	Length of Contractor Update Period after Receiving State Updates
Type A	Seven (7) days	Seven (7) days
Type B	Ten (10) days	Ten (10) days
Type C	Twenty (20) days	Twenty (20) days

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
Deliverable 1	Project Management Plan	Once upon State approval; Update if necessary	The Project Management Plan is the overall plan for project execution, monitoring, and control and should include information describing the project management approach, the internal organizational structure and organizational chart, roles and responsibilities, a summary of the Project's purpose, scope, and objectives, a description of the constraints and/or assumptions on which the Project is based, a list of product deliverables, a summary of the Project's schedule and budget, and the methods for updating, reviewing and disseminating the PMP as well as specific supplemental management plans for critical project areas: a) Overall Project Management Approach b) Scope Management Plan	a) The Project Management Plan and component plans have been reviewed and appropriately updated. b) The Project Management Plan defines how the project will be executed, monitored and controlled and includes high level estimates of the baselines. c) The Project Management Plan is fully scaled and details all the appropriate components that address the needs of the project. This includes the definition of appropriately scaled reviews and deliverables	a) Issues List b) Action Items c) Decision Log d) Lesson Learned Log e) Staff Planning and Monitoring Processes f) Staffing Tracker g) Resource Availability Calendar h) Key Personnel Transition Plan i) Onboarding Checklist j) Onboarding Arrival Packet k) Acceptable Use Policy and Information Protection Plan l) Roll-On Form m) Team Member Transitions Plan n) Roll-Off Form o) Off-Boarding Checklist	Type C

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			<ul style="list-style-type: none"> c) Schedule Management Plan d) Communication Management Plan e) Quality Management Plan f) Risk/Issue Management Plan g) Change Management Plan (including Training Plan) h) Configuration Management Plan i) Performance Management Plan j) Staffing Management Plan k) Financial Management Plan <p>The Project Management Plan is created during the PBR Gate of the SDLC and State approval of the project management plan is required as a criteria item for completion of the Project Baseline Review</p>			
Deliverable 2	Key Performance Indicator Management Plan	Once upon State approval; Update if necessary	<p>The KPI Management Plan describes the processes and mechanisms by which Key Performance Indicators will be defined, tracked, and properly reviewed during the duration of the project. At a minimum the KPI Management Plan shall include:</p> <ul style="list-style-type: none"> a) A description of the KPI, and the business value it will bring to the project 	<ul style="list-style-type: none"> a) The Plan properly describes the state-approved KPIs that will be tracked during the project b) The Plan establishes the process by which KPIs will be documented, tracked, and updated over time 	a) Continuous Improvement Plan	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			<ul style="list-style-type: none"> b) Identification of the tools, processes, inputs, and calculations that will be used to generate the KPIs current result c) The process by which KPIs will be reported, tracked, and reviewed to ensure that over time the KPI is in compliance with established limits d) Additional metrics that will be needed for each KPI if is found out of compliance e) The communication plan for reporting KPI results, including escalation plans for KPIs found out of compliance f) The roles and responsibilities for KPI generation, tracking, and reporting 	<ul style="list-style-type: none"> c) The Plan details how each KPI will be calculated d) The Plan has a properly defined KPI communication plan 		
Deliverable 3	Requirements Management Plan	Once upon State approval; Update if necessary	<p>The Requirements Management Plan provides a clear and concise layout of how detailed requirements will be gathered (including sections for functional, technical, security, performance, operational, etc.).</p> <p>The Requirements Management Plan must</p>	<ul style="list-style-type: none"> a) The Requirements Management Plan prescribes the tools and methodologies of capturing, standardizing, classifying, monitoring, reporting, maintaining, and managing requirements. 		Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			outline a robust method to store and track functional, technical and other operational and performance requirements.	b) The Requirements Management Plan shall outline methods for maintaining requirements traceability throughout the development process; methodology and processes adopted during development; types and conduct of test activities, and the change control and configuration management processes.		
Deliverable 4	Business Rules Management Plan	Once upon State approval; Update if necessary	The Business Rules Management Plan will detail the tools, processes, and methods by which business rules are managed, changed, or retired.	a) The Business Rules Management Plan outlines the standards, tools, and methodologies that will be used in managing business rules across the solution life cycle. b) The Business Rules Management Plan outlines the industry-recognized Business Rules Engine (BRE) or Business Rules Management System (BRMS) used to document business rules c) The Business Rules Management Plan outlines the format that will be utilized when developing business rules		Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
				<ul style="list-style-type: none"> d) The Business Rules Management Plan identifies the responsibilities of Business Rules Management, including critical access and segregation of duties considerations e) The Business Rules Management Plan includes explanation regarding compliance with the Minimum Acceptable Risk Standards for Exchanges (MARS-E), and proper alignment with the project Security Plan 		
Deliverable 5	Design Management Plan	Once upon State approval; Update if necessary	The Design Management Plan details the approach to system design. The plan must ensure that the system conforms to the defined standards for system design and systems architecture. The plan also ensures that the Enterprise Architecture (EA) requirements within the State are taken into consideration during the System design. The plan must ensure completeness and level of detail in design specifications. The Design Management Plan will outline considerations of the design on the selection of a Software Development Methodology.	<ul style="list-style-type: none"> a) The Design Management Plan details the approach to system design. b) The Design Management Plan must ensure that the system conforms to the defined standards for system design and systems architecture. c) The Design Management Plan demonstrates conformance to the States Enterprise Architecture (EA). d) The Design Management Plan demonstrates how all 		Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
				<p>requirements will be addressed in design.</p> <p>e) The Design Management Plan must ensure completeness and level of detail in design specifications.</p> <p>f) The Design Management Plan will outline considerations of the design on the selection of a Software Development Methodology.</p>		
Deliverable 6	Test Management Plan	Once upon State approval; Update if necessary	The Test Management Plan outlines the approach that will be employed to test the Solution and to evaluate the results of that testing; outlines general testing roles and responsibilities; and serves as the top-level plan that will be used to govern and direct the detailed testing work. The Test Management Plan should address complexities associated with a multiple release implementation.	<p>a) The Test Management Plan details the planning, execution, and management activities to be executed in order to monitor and control testing, and ensure alignment of corresponding activities with the project goals and objectives.</p> <p>b) The Test Management Plan references a defect resolution process that is inclusive of defect identification, prioritization, creation, tracking, and resolution and retesting activities to</p>	<p>a) Unit Testing template</p> <p>b) Smoke/Sanity Testing template</p> <p>c) Regression Testing template</p> <p>d) Ad-hoc Testing template</p> <p>e) Exploratory Testing template</p> <p>f) Usability Testing template</p> <p>g) GUI Software Testing template</p> <p>h) Accessibility Testing template</p> <p>i) Security Compliance Testing template</p> <p>j) Compatibility Testing template</p> <p>k) Functional Testing template</p> <p>l) Boundary Testing template</p>	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
				<ul style="list-style-type: none"> be followed when a defect is found. c) The Test Management Plan defines the testing environments hours of operations during testing execution. d) The Test Management Plan outlines the expectations for level of detail that shall be required in each test case. 	<ul style="list-style-type: none"> m) Negative Testing template n) Error Handling Testing template o) Alert/Monitoring Testing template p) Capacity Testing template q) Performance Test Plan and Results template 	
Deliverable 7	Implementation and Deployment Plan	Monthly, throughout project lifecycle	The Implementation and Deployment Plan explains the implementation methodology to be used, explaining how operations will transfer from the legacy system to the new System. The Plan will also contain an up-to-date detailed implementation schedule.	<ul style="list-style-type: none"> a) The Implementation and Deployment Plan contains an up-to-date detailed implementation schedule to be followed. b) The Implementation and Deployment Plan describes the major tasks required to be taken, and the objective behind each task. c) The Implementation and Deployment Plan lists the support equipment (hardware), software, data, facilities and materials required for the implementation, if applicable. 	<ul style="list-style-type: none"> a) Release Plan b) Implementation Plan c) Monitoring Strategy d) Version Description Document e) Information System Description f) Release and Deployment Plan g) System Sunset Plan h) Cut-Over Plan i) Roll Back Plan j) Turnover Plan k) Knowledge Transition Plan 	Type A
Deliverable 8	Data Conversion and Synchronization Plan	Monthly, throughout project lifecycle	The Data Conversion and Synchronization Plan describes the strategy, preparation, and specifications for data	<ul style="list-style-type: none"> a) The Data Conversion and Synchronization Plan describes rationale for the conversion and a 	<ul style="list-style-type: none"> a) Extract Control Documents b) Roll Back Plan 	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			conversion activities. This plan describes the overall approach, assumptions, and processes that will be used in the data conversion. It includes an inventory and cross reference of source and target data elements, schema, metadata and all self-describing files; process for data extraction, transformation and loading for each data source; tools needed to execute the conversion; and strategy for data quality assurance and control.	<ul style="list-style-type: none"> b) The Data Conversion and Synchronization Plan outlines the approach that will be used to extract, transform/cleanse and load data from the source to target destinations during the conversion/migration process c) The Data Conversion and Synchronization Plan outlines the schedule of conversion activities to be accomplished in accordance with this Data Conversion Plan 		
Deliverable 9	System Security Plan	The initial System Security Plan shall be completed in Release I then reviewed and updated on an as needed basis, including annually, and when there are major system modifications that could potentially impact the	The System Security Plan documents the system's security level and describes managerial, technical and operational security controls. An Initial copy of the System Security Plan includes an initial Risk Assessment (RA) that contains mission/business process risks and the monitoring strategy, for review and approval by the Technical Change Control Board (TCCB) and Project Steering Committee.	<ul style="list-style-type: none"> a) The System Security Plan works in synchronization with the safeguard procedures to detail the control requirements for the protection of all data received, stored, processed and transmitted in compliance with all Federal Laws and Regulations. b) The System Security Plan includes the current level of existing security 	<ul style="list-style-type: none"> a) Part A System Identification b) Part B Security Controls Workbook c) Part C Privacy Controls Workbook d) Part D SSP Attachments e) Appendix A – IRS Requirements for Safeguarding Federal Tax Information (FTI) f) Appendix B – Security and Privacy Agreements and Compliance Artifacts 	Type C

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
		security and privacy of the information system.		<ul style="list-style-type: none"> c) The System Security Plan outlines the applicable Laws or Regulations. d) The System Security Plan contains a review log that is maintained to record the reviews that have taken place for this system. e) The System Security Plan organizes security controls into groups of families. f) Exit criteria includes CMS signoff 	<ul style="list-style-type: none"> g) Memorandum of Understanding h) Interconnection Security Agreements (ISA) i) Computer Matching Agreement j) Information Exchange Agreement k) Privacy Impact Analysis l) Security Impact Analysis m) Asset Inventory n) Asset Management Plan o) Information System Risk Assessment (ISRA) 	
Deliverable 10	Business Continuity and Disaster Recovery Plan	Monthly, throughout project lifecycle	The Business Continuity and Disaster Recovery Plan describes the strategy and organized course of action that is to be taken if things don't go as planned or if there is a loss of use of the established business product (e.g., system) due to a disaster such as a flood, fire, computer virus, or major failure. The Business Continuity and Disaster Recovery Plan describes the strategy for ensuring recovery of the business product in accordance with stated Recovery Time Objective and Recovery Point Objectives.	<ul style="list-style-type: none"> a) The Business Continuity and Disaster Recovery Plan b) The Business Continuity and Disaster Recovery Plan prescribes responsibilities as they relate to actions that will be taken in response to a disruption. c) The Business Continuity and Disaster Recovery Plan clearly outlines milestones, 	<ul style="list-style-type: none"> a) Business Continuity Plan b) Disaster Recovery c) Disaster Recovery Plan Training d) Configuration Management Plan e) Configuration Management Database f) Asset Management Plan g) Business Continuity Plan Training h) Backup Management Plan 	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
				notification activities, emergency handling of routine procedures, required contacts, formal agreements, lessons learned activities, and procedures to return normal operations in the event of a disaster.	i) Business Impact Analysis	
Deliverable 11	Capacity Plan	Monthly, throughout project lifecycle	<p>The Capacity Plan will address business capacity, service capacity, and IT component capacity management strategies that will be executed through the duration of the project. The Capacity Plan will also outline the management process and tools that will be used to complete capacity management, as well as estimates of future system workloads.</p> <p>The capacity plan will include, but not limited to, infrastructure, database, network, and any other aspects required to meet the performance requirements of the system.</p>	<ul style="list-style-type: none"> a) The Capacity Plan demonstrates a State-approved skill and resource level to effectively execute the Capacity Plan. b) The Capacity Plan defines capacity performance success at the business process level c) The Capacity Plan outlines the practices, objectives, performance factors, monitoring and reporting activities, and communication strategies of the Capacity Plan. d) The Capacity Plan addresses steps and activities needed to address instances of abnormal levels of system use outside of forecasted operating procedures. 	a) System Capacity and Performance Plan	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
Deliverable 12	Data Management Plan	Monthly, throughout project lifecycle	A defined plan for the management of data that provides, at a minimum, a summary of activities for data generation, a summary of the types of data generated by the relevant activities, the plans for preservation of the generated data, and a description of the appropriate level of access for the generated data.	<ul style="list-style-type: none"> a) The Data Management Plan includes a summary of activities that generate data b) The Data Management Plan includes a summary and appropriate categorization of the data types generated by the identified activities. c) The Data Management Plan includes a plan for storage and maintenance of the data generated by the identified activities, in both the short-term and long-term (if relevant). d) The Data Management Plan includes a plan describing whether and how the data generated by the identified activities will be reviewed and made available to the public and how the metadata describing it will be stored. 		Type A
Deliverable 13	Performance and Availability Plan	Monthly, throughout project lifecycle	The Performance and Availability Plan will identify target performance areas and methods of measurement; establish the baseline metrics for the agreed upon goal areas; and assist HCFA in	<ul style="list-style-type: none"> a) The Performance and Availability Plan identifies and prioritizes the performance measurement goals and objectives to 	<ul style="list-style-type: none"> a) Performance Test Plan and Results Template b) Program Availability Management Plan 	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			determining the level of achievement of the performance goals.	<p>align with the information needs of the customer, project, organization, and stakeholders, as applicable.</p> <p>b) The Performance and Availability Plan includes a Traceability of Information Needs to Measurement Objectives by defining the information need, measurement objective, and the performance measure threshold.</p> <p>c) The Performance and Availability Plan describes the methods, processes, tools and techniques that will be used for performance measurement.</p> <p>d) The Performance and Availability Plan outlines the data that will be collected, how it will be collected, and where it will be stored.</p> <p>e) The Performance and Availability Plan includes analysis on the data collected, and a review of the data to identify trends and opportunities for</p>		

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
				<p>improvements and corrective actions.</p> <p>f) The Performance and Availability Plan includes an approach for identifying and addressing deficiencies in performance and availability.</p>		
Deliverable 14	Work Breakdown Structure (WBS)	Monthly, throughout project lifecycle	<p>The Work Breakdown Structure (WBS) is a preliminary step in the preparation of a project work plan and schedule that encompasses all activities from Project Initiation to Project Closure. The WBS must define the project's overall objectives by describing the project tasks and deliverables. The WBS must include:</p> <ul style="list-style-type: none"> a) A consolidated view of the activities, activity descriptions, and activity durations b) Resources assigned to each activity c) A list of deliverables tied to project milestones d) A way to track the project schedule against the planned schedule e) Deliverable approval periods <p>This deliverable is associated with the PBR Gate and must be delivered to the State prior</p>	<ul style="list-style-type: none"> a) The WBS defines 100% of the project scope b) The WBS was created with input provided by all relevant stakeholders c) The WBS is outlined as such that the project activities and tasks are able to be executed, monitored, and controlled. d) The WBS is broken down such that any work package greater than 80 hours must be broken down into component activities. e) The WBS includes a WBS Dictionary, or executable activities being followed to completing the process. 		Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			to the completion of the project baseline review.			
Deliverable 15	Risk Register (update weekly)	Monthly, throughout project lifecycle	The Risk Register contains the findings of the Risk Management Process and serves as the source of record for risk management activities to track the approaches and action plans for dealing with identified risks, which typically involve one of four options: avoidance, mitigation, transference, or acceptance. Once an approach is selected, detailed actions to implement are developed and the risk register serves as a record of those activities that information throughout the SDLC. The initial risk register is created during the ORR Gate and must be approved by the state prior to the completion of the project baseline review.	<ul style="list-style-type: none"> a) The Risk Register will contain Risk Category, Probability, Impact, Risk Score, Risk Ranking, Risk Response, Trigger and Risk Owner. b) The Risk Register should identify how risks are mitigated (change request, work around, deferment) 	a) Risk Management Plan	Type A
Deliverable 16	Baselined Work Plan and Schedule	Monthly, throughout project lifecycle	This is a work plan and schedule that is managed in an appropriate project management tool.	<ul style="list-style-type: none"> a) The schedule has sufficient detail to support the projected durations. b) The master work plan must reflect any changes from the plan submitted within the Contractor's original proposal that were discussed and agreed to during project planning. 		Type A
Deliverable 17	Status Reporting	Weekly and Monthly, throughout project lifecycle	This deliverable must be a recurring deliverable for the entire length of the project. The deliverable must at a minimum include periodic	<ul style="list-style-type: none"> a) The reports contain all of the required elements as agreed upon by HCFA and the Contractor. 		Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			<p>reporting of the following activities:</p> <ul style="list-style-type: none"> a) Status of work completed against the Project Work Plan b) Objectives for the next reporting period c) Client responsibilities for the next reporting period d) Recovery plan for all work activities not tracking to the approved schedule e) Projected completion dates compared to approved baseline key dates f) Escalated risks, issues (including schedule and budget), and Action items g) Disposition of logged issues and risks h) Important decisions i) Actual/projected Project Work Plan dates versus baseline Project Work Plan milestone dates j) One-page graphical summary of the Project Work Plan status of all major tasks and subtasks for each release in a Desktop Project Plan <p>Adjustments to status reporting requirements will be</p>			

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			addressed through the Memorandum of Understanding (MOU) process.			
Deliverable 18	Financial Status Report	Weekly and Monthly, throughout project lifecycle	The Financial Status Report tracks the project costs to the project budget baseline and outlines any budgetary risks.	<ul style="list-style-type: none"> a) Includes estimates to completion, or cost performance index information. b) It will reflect approved changes to project budget. c) Includes reporting on any project work stream that has had activity against it. 		Type A
Deliverable 19	Detailed Requirements Traceability Matrix	Updated monthly throughout project lifecycle	The Detailed Requirements Traceability Matrix describes the life of a requirement, in both a forward and backward direction, ideally through each step of the entire product's life cycle, ensuring scope is met.	<ul style="list-style-type: none"> a) The Requirements Traceability Matrix outlines describes each requirement independently, which Release each requirement was met or updated, and provides traceability to applicable test cases to demonstrate how each requirement was implemented. b) The Requirements Traceability Matrix shows the difference between functional and non-functional requirements. c) The Requirements Traceability Matrix allows rationale to be included when requirements are not fully traceable throughout the lifecycle. 	<ul style="list-style-type: none"> a) Requirements Specification Document including but not limited to: b) Business Rules c) Business Process Flow Diagrams d) Requirements Traceability Matrix Functional/Non-Functional Requirements 	Type C

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
Deliverable 20	Requirements Specification Document	Once per release upon State approval	The Requirements Specification Document provides all requirements expected to be implemented. This document lists the business requirements, business rules, stakeholder requirements, and functional/nonfunctional requirements for the project. It also contains use case scenarios that describe how the requirements will be implemented.	<ul style="list-style-type: none"> a) The Requirements Specification Document outlines business, technical, governance and project management stakeholders inclusive of requirements gathering, review, and approval. b) The Requirements Specification Document includes references to all interdependent deliverables and artifacts throughout the lifecycle, specifically documents that ensure traceability to the implemented Solution. c) The Requirements Specification Document includes business and functional rationale of the included requirements. d) The Requirements Specification Document details the Solution, written in a level of detail easily understood by non-technical personnel. e) The Requirements Specification Document includes Business Process Flow Diagrams 	<ul style="list-style-type: none"> a) Requirements Specification Document including but not limited to: b) Business Rules c) Business Process Flow Diagrams d) Requirements Traceability Matrix Functional/Non-Functional Requirements 	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
				detailing the Business Process that is being introduced or enhanced.		
Deliverable 21	System Architecture Design Document	Once per release upon State approval	<p>The System Architecture Design Document (SADD) describes:</p> <ul style="list-style-type: none"> a) How the functional and nonfunctional requirements recorded in the Requirements Document will be met in the Solution design. b) How the preliminary user-oriented functional design recorded in the High Level Technical Design Concept/Alternatives document will be met in the Solution design. <p>The SADD describes design goals and considerations, provides a high-level overview of the system architecture, and describes the data design associated with the system, as well as the human-machine interface and operational scenarios. The high-level system design is further decomposed into low-level detailed design specifications for each of the system's components, including hardware, internal communications, software, system integrity controls, and</p>	<ul style="list-style-type: none"> a) Functional and non-functional requirements are mapped to supporting technical design. b) Functional design requirements are mapped to technical design specifications. c) A high level system design is provided. 	<ul style="list-style-type: none"> a) Technical Architecture Diagrams b) Systems Design Document c) High Level Technical Design Concept/Alternatives d) FTI Labeling Methodology 	Type C

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			external interfaces. The high-level system design serves as primary input to the Preliminary Design Review. The low-level detailed design serves as input to the Detailed Design Review.			
Deliverable 22	Interface Control Document(s)	Once per release upon State approval	<p>The Interface Control Document (ICD) describes the relationship between the two interconnected systems. This ICD specifies the interface requirements to be met by the participating systems and at minimum, describe the interface definitions and design (including XML/SOAP/flat file/other specifications for file formats),. It describes the design specifications for the interface, defines the message structure and protocols that govern the interchange of data, and identifies the communication paths along which the data are expected to flow. For each interface, the following information will be provided:</p> <ul style="list-style-type: none"> a) A general description of the interface; b) Assumptions where appropriate; c) A description of the data exchange format and protocol for exchange; and d) Estimated size and frequency of data exchange 	<ul style="list-style-type: none"> a) All ICDs defined as required have been created. b) The ICD describes the interface, including purpose, format, message structure, and protocols. c) The ICDs indicate the size and frequency of the data exchange. d) Memorandum of Understanding or System Interface Agreements have been established to document the interface expectations. e) The ICD has been tested via simulation. 	<ul style="list-style-type: none"> a) TEDS Interface/Integration Management Plan b) Memorandum of Understanding c) Interconnection Security Agreement d) Interface Control Test Plan 	Type C

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
Deliverable 23	Database Design Document	Once per release upon State approval	The Database Design Document describes the design of a database and the software units used to access or manipulate the data.	<ul style="list-style-type: none"> a) The Database Design Document outlines the DBMS to be used for the Solution b) The Database Design Document outlines tasks and responsibilities for database administration and reporting, including performance monitoring, efficiency, backup and recovery. c) The document indicates key design decisions. d) The document includes a detailed database design, including data formats, data software objects, data structures, and database management system files. e) The document describes how the preliminary data design documented in the Logical Data Model are transformed into more technical system design specifications from which the system will be built. 	<ul style="list-style-type: none"> a) Logical Data Model b) Physical Data Model c) Entity Relationship Diagram (ERD) for the logical data model d) Data Flow Diagrams 	Type C

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
Deliverable 24	Data Dictionary	Once per release upon State approval	The Data Dictionary comprehensively outlines the data element name, type, length, source, validation rules, maintenance (create, read, update, delete (CRUD) capability), data stores, outputs, aliases, and description. The Data Dictionary shall provide a data classification of all data collected and transferred by the Solution.	<ul style="list-style-type: none"> a) The Data Dictionary characterizes data formatting requirements and validation rules b) The Data Dictionary describes the data classification of database elements (entity, attributes etc.) 		Type C
Deliverable 25	SOA Models	Once per release upon State approval	SOA Models will outline a services portfolio by identifying services, defining a service hierarchy, and classifying the services based on this hierarchy. This will involve defining the coarse-granularity and fine-granularity of services. This document must identify and prioritize the key services and the mechanisms to create the service layers using industry standards.	<ul style="list-style-type: none"> a) The SOA Models identify the Services Portfolio Management requirements, which must include the requirements for how often services should be reviewed, how often they should be updated, and how they should be published b) The SOA Models identify the Quality of Service requirements for each service, which will involve defining scalability, availability, and response time (latency) of services in order to ensure that they are within the promised range c) The SOA Models identify interface requirements, which will involve both internal and external 	<ul style="list-style-type: none"> a) Service Oriented Architecture (SOA) Model including but not limited to: b) Definition of service hierarchy c) Prioritization of key services d) Mechanisms to create service layers e) Technical Architecture Diagrams f) Quality of Service Requirements g) Interface Requirements h) Security Requirements i) Performance Requirements j) Operational Requirements 	Type C

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
				<p>Partners and ensuring that the new System is sufficiently scalable and flexible to support the number of interfaces that will be required.</p> <p>Interface requirements must also include defining what communications should be asynchronous, and what communications should be synchronous</p> <p>d) The SOA Models identify security requirements, which may include encryption, authentication, data protection, and constraints on performing certain operations</p> <p>e) The SOA Models identify performance requirements, which may include the expected response time for application tasks, failover support for applications, and hours of availability</p> <p>f) The SOA Models identify operational requirements, which may include server</p>		

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
				needs, scalability requirements, hosting requirements, monitoring, load balancing, failover, fault recovery, accounting and metering		
Deliverable 26	Functional Design Document (Including Use Cases)	Once per release upon State approval	The Functional Design Document expands upon the requirements document to describe how the functional requirements will be implemented. This document goes to a granular level and describes such things as the tables to be updated, fields to be added, screens to be created or changed, business rules to be changed, and additional interfaces.	<ul style="list-style-type: none"> a) Accounts for all functional requirements b) Demonstrates how functional requirements will be addressed within the design c) Use cases that describe how the requirements will impact the system, included both positive and negative use cases. d) Business Process Flow Diagrams detailing the Business Process that is being introduced or enhanced. 	a) Systems Design Document	Type C
Deliverable 27	Technical Design Document	Once per release upon State approval	A Technical Design Document reflects the details required for System development/configuration and operation. This document must be developed based on outputs from the technical design sessions conducted with all Stakeholders and/or functional design, interface control documents. The Technical Design Document	<ul style="list-style-type: none"> a) Contains detailed description of system architecture. b) Includes entity relationship diagrams and data flow diagrams c) References the data dictionary (i.e., all data elements are 	<ul style="list-style-type: none"> a) Technical Architecture Diagrams b) Systems Design Document c) Business Rules d) Document Print/Letter/Notices/Electronic Output Management Plan 	Type C

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			<p>must include the following components:</p> <ul style="list-style-type: none"> b) Detailed description of System architecture c) Entity Relationship Diagrams, Create, Retrieve, Update, Delete details for database elements for the component being elaborated in the design d) Data Flow Diagrams e) Processing controls f) Processes to manage System installation and configuration g) Data backup procedures h) Availability and resilience controls such as load balancing, failover capabilities, and fault tolerance. <p>The Technical Design Document must include, at a minimum, the interface definitions and design (including XML/SOAP specifications for file formats), the new System design based on reviewing existing class diagrams, sequence diagrams, updated object models that represent the internal workings and designs of the containing subsystems that will expose the services, and the component</p>	<ul style="list-style-type: none"> d) Specified processing controls e) Specifies installation, configuration, and backup procedures f) Includes security controls g) Addresses availability and resilience controls such as load balancing, failover, and fault tolerance h) References ICDs i) Requirements and Design components mapped appropriately in configuration management database 	<ul style="list-style-type: none"> e) Configuration Management Plan f) Backup Management Plan g) Availability and Performance Plan h) Interface Control Documents 	

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			specification (details of the component that will implement the service) and service assignment to each layer defined in the System architecture.			
Deliverable 28	Service Level Agreements (SLAs)/Memorandum of Understandings (MOUs)	Once per release upon State approval	A Service Level Agreement(s) (SLA) is a contractual agreement between an internal or external service provider and their customer specifying performance guarantees with associated penalties should the service not be performed as contracted. A Memorandum(s) of Understanding (MOU) is a legal document that outlines the terms and details of an agreement between parties, including of each party's requirements and responsibilities.	<ul style="list-style-type: none"> a) The SLA/MOU outlines the agreed upon period of performance and any performance guarantees with associated complications falling within the period as well as reporting mechanisms/frequency and review process. b) The SLA/MOU includes a process to be followed in the event that an agreement change is to be made c) The SLA/MOU escalation process is included and detailed in nature 	<ul style="list-style-type: none"> a) Service Level Management Plan b) Service Level Agreements c) Memorandum of Understanding 	Type B
Deliverable 29	Automated Code Review Results	Once per release upon State approval	This deliverable will display the results from an automated tool's code review. These results will be used by developers to address issues in the coding. This will also be helpful in determining the overall quality of the code being produced.	<ul style="list-style-type: none"> a) Results are comprehensive of code. b) Results provide evidence to indicate product quality. c) Results indicate level of compliance with coding standards. 	<ul style="list-style-type: none"> a) Coding Standards and Quality Review Plan 	Type A
Deliverable 30	System Configuration Document	Once per release upon State approval	A System Configuration Document captures all the configuration information of the systems. This document	<ul style="list-style-type: none"> a) Documents all system configuration elements (software, hardware, OS, 	<ul style="list-style-type: none"> a) Configuration Management Plan b) Asset Management Plan 	Type C

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			often contains: Network configuration by interface, disk partition layout, installed software, with any significant configuration information, hardware and peripherals inventory, physical location of system, authentication information, network integration information (e.g., Network Time Protocol (NTP) configuration, Domain Name System (DNS) resolver configuration), list of authorized super users, list of authorized pseudo users, list of individual(s) responsible for system, with contact information (preferably via multiple communication channels), OS version information, installation idiosyncrasies and patches installed. With good system configuration documentation, a system can be rebuilt from scratch, as well as it can handle other disaster recovery tasks.	<ul style="list-style-type: none"> network configuration, authentication) b) Information can be validated to be accurate and current (e.g., release and patch levels reflect current installation) c) Reflects all approved configuration changes (managed through Technical Change Control Board) 		
Deliverable 31	Unit, System, Regression, and Integration Test Scripts	Once per release upon State approval	This deliverable documents the configuration decisions made in developing the Solution, and includes traceability of configuration decisions to requirements and design. It includes information such as network configuration by interface; disk partition layout; installed software, with any significant configuration information – hardware and peripherals inventory; physical location information; authentication information	<ul style="list-style-type: none"> a) Tests are traceable to requirements. b) Tests have been reviewed for relevance to the respective requirement. c) Tests have been defined for unit, system, regression and integration testing that provide complete coverage 		Type C

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			(method used, configurations for method, etc.); network integration information (e.g., NTP configuration, DNS resolver configuration); list of authorized superusers; list of individual(s) responsible for system, with contact information (preferably via multiple communication channels); OS version information and installation idiosyncrasies; patches installed. This documentation is critical to support staff in operations and maintenance, and also supports disaster recovery tasks as well as OS patch maintenance.	to all testable requirements d) Section 508 testing package		
Deliverable 32	Unit, System, Regression, and Integration Testing Test Results	Once per release upon State approval	Test scripts provide instructions (written using a scripting/programming language) to be performed on a system under test to verify that the system performs as expected. Unit tests occur on individual functions; system integration tests validate performance of multiple sub-systems within the Solution.	<ul style="list-style-type: none"> a) Test activities and results are documented by module. b) Defects and retest results are documented. c) Test results demonstrate completion of all required tests and testing against all requirements. 	<ul style="list-style-type: none"> a) Test Reports and summary reports for unit, system, Regression, integration testing for all areas being tested b) Section 508 Assessment Package results c) Test Summary Report 	Type A
Deliverable 33	System Readiness Certification for UAT	Once per release upon State approval	This deliverable documents completion of testing and associated results for testing completed by the system integrator. Results should indicate success rate, defects, retest results, and completion percentage of tests vs. requirements.	<ul style="list-style-type: none"> a) Open defects have been determined by State to be low impact and low risk. b) All functional and non-functional requirements have been delivered unless change requests have 	<ul style="list-style-type: none"> a) Test Reports b) Section 508 Assessment Package results c) Test Summary Report 	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
				<ul style="list-style-type: none"> c) Modules and components demonstrated stable performance during SIT and performance and capacity testing. d) Release notes have been developed to document functionality included in release. 		
Deliverable 34	Formal Acceptance Testing Report (successful completion of UAT) -Performance Test Results -System Runbook and Troubleshooting Guide -System and Operational Readiness Checklist -Data Conversion Report	Once per release upon State approval	The Formal Acceptance Testing report documents completion of UAT and final steps prior to implementation into production. This report includes documentation to support use and maintenance of the Solution, as well as evidence that readiness activities – including transition requirements – have been completed.	<ul style="list-style-type: none"> a) UAT results are documented, and demonstrate no defects beyond low impact or low risk. b) Troubleshooting guide has been validated by user and support staff for accuracy and relevance of topics. c) Data conversion has been completed successfully; any exceptions have been determined by HCFA to be low impact or low risk. d) All checklist activities for operational readiness have been completed. e) Release notes have been developed to document functionality included in release. 		Type A
Deliverable 35	Contingency/Recovery Plan	All CPs will be reviewed and	The Contingency/Recovery Plan establishes procedures	<ul style="list-style-type: none"> a) The Contingency/Recovery 	a) Disaster Recovery Plan	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
		exercised annually.	<p>to recover a system following a disruption. The Contingency/Recovery Plan. The Plan identifies the activities, resources, and procedures needed to carry out operations during prolonged interruptions to normal operations. The Plan also assigns responsibilities to designated personnel and provides guidance for recovering the system.</p> <p>CP Test Plan should be tested to identify and rectify deficiencies and planning shortfalls, NOT to ascertain the technical competence of personnel with recovery responsibilities.</p> <p>The Business Owner, System Developer/Maintainer, Contingency Plan Coordinator, and SSO shall establish criteria and pre-developed test plan for validating/test CPs on an annual schedule, once every 365 days.</p> <p>CP Test After Action Report will be used for plan updates addressing any identified shortcomings.</p>	<p>ry Plan defines the triggers that would initiate the contingency and recovery operations</p> <p>b) The Contingency/Recovery Plan outlines the individuals with the responsibility/authority to make the decision to initiate the Contingency/Recovery Plan</p> <p>c) The Contingency/Recovery Plan clearly outlines the steps and activities to be taken in the event of a trigger.</p> <p>d) The Contingency/Recovery Plan outlines a dry run simulation of the contingency activities.</p> <p>e) The Contingency/Recovery Plan outlines the communication protocols and flows in the event the Contingency/Recovery Plan is evoked.</p> <p>f) The Contingency/Recovery Plan should include an approach to test the contingency plans.</p>	<p>b) Disaster Recovery Plan Test</p> <p>c) Business Continuity Plan</p> <p>d) Asset Management Plan</p> <p>e) Configuration Management Plan</p> <p>f) Business Continuity Test Plan</p> <p>g) Configuration Management Database</p> <p>h) Build Books for STS</p>	

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
				g) Contingency/Recovery Test After Action Report must be clearly defined.		
Deliverable 36	Beta Test Plan	Once per release upon State approval	A Beta Test Plan is a test plan that is used to describe the methodologies, processes, and testing that is expected to take place on a beta release (non-production release of full functionality).	<ul style="list-style-type: none"> a) The plan outlines methodologies and processes to be used. b) The plan outlines specific testing activities to be performed, including expected outcomes. c) The plan outlines the individuals who will be involved in beta testing and the process for documenting identified issues. 		Type A
Deliverable 37	Network Vulnerability Assessment Resolution Report	Once per release upon State approval	The Network Vulnerability Assessment Resolution Report outlines results of a network vulnerability assessment, the significance of findings, and the completed and planned actions to resolve identified vulnerabilities.	<ul style="list-style-type: none"> a) The Network Vulnerability Assessment Resolution Report includes a status on all open items identified in the assessment. b) The Network Vulnerability Assessment Resolution Report defines the anticipated approach and timeline for resolving open issues based on criticality and severity. c) The Network Vulnerability Assessment 	a) Software Assurance Misuse Cases	Type B

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
				Resolution Report indicates progress in resolving issues that were identified in previous assessments.		
Deliverable 38	Beta Test Evaluation Report	Once per release upon State approval	A Beta Test Evaluation Report is a report that details the results of a Beta test release. The report will: <ul style="list-style-type: none"> a) Compare actual results to expected results b) Identify major defects found with mitigation plans c) Capture feedback and pain points reported by the users testing the system 	<ul style="list-style-type: none"> a) The beta test report details the test environment (number of testers, types of machines used) that was used to execute the beta test b) The beta test details the key functionality that was tested c) The beta test compares actual test results with expected testing results d) Any new risks, issues, and defects found during testing have been properly identified, documented, and prioritized 		Type A
Deliverable 39	Privacy Impact Assessment	Reviewed annually or upon significant system change	Required of federally owned systems. The Privacy Impact Assessment (PIA) is designed to help states quickly identify and subsequently document the specific types of sensitive information that it will collect, process, and store. The Privacy Impact Assessment (PIAs) identifies systems that contain personally identifiable information (PII) and satisfies system compliance with all relevant privacy laws, regulations, and guidance.	<ul style="list-style-type: none"> a) The PIA approved by the HCFA Chief Privacy Officer b) The PIA is sufficient enough to be used to obtain an Authority to Operate (ATO) subject to review/approval by CMS 		Type B

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			The PIA document ensures that privacy protections are incorporated into every stage of an IT system's life cycle, and measures the effectiveness of these protections.			
Deliverable 40	Information Security Risk Assessment	As defined by CMS	<p>Required of federally owned systems. The IS RA contains a list of threats and vulnerabilities, an evaluation of current security controls, their resulting risk levels, and any recommended safeguards to reduce risk exposure. The IS RA also supports risk management through the evaluation of risk impact upon the enterprise security model. It will be used for system certification and accreditation (C&A).</p> <p>CMS requires each Business Owner to develop or update an IS RA in response to each of the following events:</p> <ul style="list-style-type: none"> a) New system; b) Major business process or technology/system modification(s); c) Every third year of an operational system; d) Increase in security risks/exposure; e) Increase of overall system security level; and/or, f) Serious security violation(s) as 	<ul style="list-style-type: none"> a) The IS RA contains a list of threats and vulnerabilities to the system b) The IS RA provides the results of an evaluation of current security controls and their resulting risk levels c) The IS RA includes any recommended safeguards in an attempt to reduce risk exposure. d) The IS RA approved by the HCFA Chief Privacy Officer e) The IS RA is sufficient enough to be used to obtain an ATO subject to review/approval by CMS and required for Authority to Connect (ATC) 	<ul style="list-style-type: none"> a) Information System Risk Assessment b) Information Security Risk Assessment 	Type B

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			described in the CMS g) Information Security Incident h) Handling and Breach Analysis/Notification Procedure			
Deliverable 41	Data Use/Data Exchange/Interconnection Security Agreements	Once per release upon State approval	Information that is required to develop agreements between parties for the use of personal identifiable data, and to ensure secure data exchange. This includes information that the IRS Office of Safeguards expects from an agency regarding their procedures for safeguarding Federal Tax Information (FTI), in any instance where that agency intends to receive, store, process, or transmit FTI.	<ul style="list-style-type: none"> a) The document clearly delineates the roles and responsibilities between parties that are exchanging data b) The document sufficiently addresses the mechanisms for data exchange c) The document sufficiently addresses security controls in place by each party of the agreement, and how those controls will be used together to ensure a secure exchange of data d) The document has been signed by resources who have the proper authority to enter the organization into such agreement 		Type B
Deliverable 42	MARS-E Security Controls	System Security Plan should be reviewed and updated on an as needed basis,	The MARS-E Security Controls Document provides guidance to CMS and its contractors as to the minimum level of required security controls that must be implemented to protect CMS'	<ul style="list-style-type: none"> a) The MARS-E Security Controls Document is compliant with the Minimum Acceptable Risks for Exchanges document 	<ul style="list-style-type: none"> a) SSP Workbook (Security Control Description) b) Business Risk Assessment (Security 	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
		including annually, and when there are major system modifications that could potentially impact the security and privacy of the information system.	information and information systems.	<ul style="list-style-type: none"> b) Assessment of MARS-E compliance shall be done using NIST Publication SP 800-53A "Guide for Assessing the Security Controls in Federal Information Systems and Organizations" standards c) The document can be used to secure an ATO d) The document is signed by the HCFA Chief Security Officer 	<ul style="list-style-type: none"> Awareness) Training Plan c) (Security Awareness) Training Result d) Computer Matching Agreement (CMA) 	
Deliverable 43	IRS Safeguards Procedures Report	The authorization shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the security authorization. All information regarding the authorization shall be provided to the Office of Safeguards as part of the	<p>Supports HCFA in attaining IRS certification for the Solution. Agencies executing data exchange agreements involving access to FTI and subject to safeguarding requirements must have an approved SSR prior to having access to FTI. Section 7 of Publication 1075 outlines SSR Reporting Requirements — 6103(p) (4) (E):</p> <ul style="list-style-type: none"> a) The agency should submit the report for approval at least 90 days prior to the agency receiving FTI. b) The agency must update and submit the SSR annually to encompass any changes that impact the protection of FTI. 	<ul style="list-style-type: none"> a) The document is completed in time enough to provide the IRS the 90-day period needed before accessing FTI b) The document is completed using the IRS SSR prescribed template c) The document is approved by the HCFA CFO prior to submission to the IRS subject to review/approval by CMS/IRS and required for ATC 		Type B

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
		Safeguard Activity Report.	c) The SSR submission and all associated attachments must be sent annually to identify changes to safeguarding procedures.			
Deliverable 44	Site Readiness Reports	Once per release upon State approval	The Site Readiness Reports are based on the results of the site assessments and will address all remote sites in the State. Each Site Readiness Report will detail issues at each particular site and make recommendations on how each issue will be remedied before the rollout of the new System.	<ul style="list-style-type: none"> a) The Site Readiness Report addresses all of the readiness criteria b) The Site Readiness Report identifies deficiencies, remediation, and a recommendation on whether or when to proceed with implementation. 		Type A
Deliverable 45	System Operations Documentation	Once per release upon State approval	<p>The System Operations Documentation describes all required Systems operational activities and must encompass System functionality from a remote user's perspective, a State business user's perspective, and from an information technology and System operations perspective. These manuals must include:</p> <ul style="list-style-type: none"> a) A description of how to use the System based on user roles and responsibilities b) A list of prebuilt reports and their descriptions c) A description of all screens and how they are interrelated, and all help and 	<ul style="list-style-type: none"> a) The document addresses all areas of system operation, as prescribed in the description b) The document has been approved by the appropriate HCFA resources 	<ul style="list-style-type: none"> a) User Manuals b) Release Notes 	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			<ul style="list-style-type: none"> navigation functions and how to use them d) A complete list of error messages, their descriptions, and how to resolve the errors e) A list of all included System documentation and its use f) How to troubleshoot common System problems g) A description of the key data tables, elements, and their contents h) How to perform System maintenance functions like data backup and recovery, run batch processes (if applicable), perform data cleanup, and administer user accounts and permissions i) How to troubleshoot common System problems j) A listing of all logs and how to interpret them k) Key System capacity and security management considerations l) Contact information for receiving support 			

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			<ul style="list-style-type: none"> m) Where to find disaster recovery and business continuity information related to the System n) A listing of System interfaces and how to troubleshoot communications problems o) File descriptions p) System and System environment configuration baseline 			
Deliverable 46	System Maintenance, Support and System Transition Plan	Once per release upon State approval	The System Maintenance, Support and System Transition Plan must outline the transition of system Operations and Maintenance from the Vendor to the State's hosting model. The Plan should note all procedural, staffing, and resource requirements.	<ul style="list-style-type: none"> a) The System Maintenance, Support and System Transition Plan will indicate the amount of dedicated resources providing O&M support, and how sufficient resources will be provided while in support of development activities for future releases. b) The System Maintenance, Support and System Transition Plan will identify all procedures and activities to be transitioned to O&M. 	<ul style="list-style-type: none"> a) O&M Manual b) Service Transition Plan 	Type A
Deliverable 47	Infrastructure, System Source Code and Documentation	Once per release upon State approval	This is the delivery to the State of written custom code, solutions, and documentation that a Contractor has bought	<ul style="list-style-type: none"> a) The Solution has successfully made it through the formalized Gate 	<ul style="list-style-type: none"> a) Business Product b) Configuration Management Plan 	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			or developed. Once the state has approved the Solution by way of successful testing and Gate Reviews, the Solution becomes State property.	Review process and testing and accepted by the state as an approved Solution	c) Configuration Management Database d) Data Dictionary	
Deliverable 48	Updated System Source Code and Design Documentation	Once per release upon State approval	This is updated code, Solution, or documentation that the Contractor has updated from a prior release. Once the state has approved the changes to the Solution by way of successful testing and Gate Reviews, the Solution becomes State property.	a) The Solution has successfully made it through the formalized Gate Review process and testing and accepted by the state as an approved Solution		Type A
Deliverable 49	Infrastructure Services Deployment Report	Once per release upon State approval	The Infrastructure Services Deployment report must address the implementation of the following infrastructure services related to the System: a) Remote Access Infrastructure b) Patch and Remote Security Management Infrastructure c) Service Desk Enhancements d) Code Migration Infrastructure e) Software Configuration Management Infrastructure f) Change and Release Management g) Data Retention and Archiving Infrastructure h) Performance Reporting Infrastructure	a) The report includes the prescribed sections as described in the description	a) Infrastructure Services Deployment	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
Deliverable 50	Plan of Action and Milestones (POA&M)	Review ad update Monthly and submit to CMS quarterly	The Plan of Action and Milestones (POA&M) is a management process that outlines weaknesses and delineates the tasks, timeline and completion criteria necessary to mitigate them.	<ul style="list-style-type: none"> a) The POA&M contains findings from internal and external audits, as well as issues that surfaced as part of the certification process b) All POA&Ms need to have a Corrective Action Plan which includes a root cause analysis, mitigation alternatives and risks associated with each, and strategies for preventing recurrence 	<ul style="list-style-type: none"> a) POA&M Management Plan 	Type A
Deliverable 51	Interconnected Systems Agreement (ISA)	ISAs need not be reissued unless a significant system change has occurred or three years have elapsed since issuance.	Interconnection Security Agreement (ISA) is to establish procedures for mutual cooperation and coordination between the Centers for Medicare & Medicaid Services (CMS) and the State. An ISA is required whenever the security policies of the interconnected systems are not identical and the systems are not administered by the same Authorizing Official. The ISA documents the security protections that must operate on interconnected systems to ensure that transmission between systems permits only acceptable transactions. An ISA includes descriptive, technical, procedural, and planning information. It also formalizes the security understanding between the	<ul style="list-style-type: none"> a) The ISA addresses the development, management, operation, and security of a connection between CMS and the State. b) The ISA contains a description of the information and data that will be made available, exchanged, or passed one-way only by the interconnection of the two systems/networks. c) The ISA describes and documents the information handled by the system and the overall system security level as 	<ul style="list-style-type: none"> a) Security Control Assessment Report b) ATO Submission c) CMS CTO-issued ATO 	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			authorities responsible for the electronic connection between the systems. An ISA must be reissued whenever a significant change occurs to any of the interconnected systems.	<p>LOW, MODERATE or HIGH</p> <p>d) The ISA contains a topological drawing that illustrates the interconnectivity between both systems, including all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Subject to review/approval by CMS and required for ATC</p>		
Deliverable 52	SLA, System Performance, System QA Reports	Weekly and Monthly, based on type of SLA	These reports measure the systems adherence to the prescribed SLAs, tracks current system performance, and system quality.	<p>a) The report provides metrics to show the systems performance in reference to prescribed SLAs</p> <p>b) The report provides metrics to show the overall performance of the system</p> <p>c) The report includes metrics that demonstrates open defects, priority of defects, and the rate at which defects are being resolved</p>		Type A
Deliverable 53	System Incident and Corrective Maintenance Reports	Monthly	The System Incident and Corrective Maintenance Report will outline corrective maintenance requests identified throughout the duration of the Warranty period. Each maintenance	<p>a) The System Incident and Corrective Maintenance Report will include anticipated resolution times for all open corrective</p>		Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			request will have a description, resolution status, and course of action for remedying all open maintenance requests.	<ul style="list-style-type: none"> a) maintenance requests as well as root cause and number of impacted cases and/or members. b) The System Incident and Corrective Maintenance Report will link defects to the release for warranty tracking purposes. c) The System Incident and Corrective Maintenance Report includes ageing, criticality and severity, and an analysis approach to defect reporting. 		
Deliverable 54	Operations Report	Daily (Calendar Days) and Monthly	<p>The Daily and Monthly Operation Reports shall include:</p> <ul style="list-style-type: none"> a) Interface events/issues b) System event/issues c) Software event/issues d) Errors and Anomalies e) Transactions Sent and Received (Daily, Total Amount) f) Transaction Types g) Staffing/Operational Activities and Issues h) Number of notices/letters received and sent (including any/all reconciliation efforts) 	<ul style="list-style-type: none"> a) The reports contain all of the required elements as agreed upon by HCFA and the Contractor. 	<ul style="list-style-type: none"> a) Security Monitoring Reports 	Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			<ul style="list-style-type: none"> i) Cumulative statistics and complete breakdown of all letters and notices by type j) Performance against SLA k) Average response times (for SLA validation) 			
Deliverable 55	AOA Report	Annual	<p>The AOA Report evaluates investment operational results against investment objectives. The AOA Report should include the following sections:</p> <ul style="list-style-type: none"> a) Overview b) Cost Benefit Analysis c) Schedule Analysis d) Performance Analysis e) Risk Analysis f) Improvement g) Recommendations and Approvals 	<ul style="list-style-type: none"> a) The document provides an overview of the current operation of the system and how it fits within the organization's investment objectives. b) The document includes all sections as prescribed in the document description c) The document has the necessary signatures 		Type A
Deliverable 56	Warranty Completion Report	Monthly until completion of warranty	Report validates that the hardware, customized IMS, and supporting software are performing in a stable manner. Report summarizes the current state of production including open issues, transition status and production environment performance statistics.	<ul style="list-style-type: none"> a) The report is produced while the Solution is still within the warranty period b) This report is sufficient enough to communicate needed fixes covered under the warranty 	<ul style="list-style-type: none"> a) Project Completion Report b) Project Closeout Report c) Disposition Plan 	Type A
Deliverable 57	Post Implementation Report	Once per release upon State approval	This Post Implementation Report results from monitoring the performance of the system/application during normal operations against	<ul style="list-style-type: none"> a) The Post Implementation Report contains steps to gather and take action on 		Type A

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			original user requirements and any newly implemented requirements or changes.	<ul style="list-style-type: none"> lessons learned on activities executed in all Solution releases. b) The Post Implementation Report contains a User/Customer Assessment based on feedback received c) The Post Implementation Report contains a Performance Assessment d) The Post Implementation Report contains justification as to if the existing system should continue in operation as is, be enhanced, or terminated. If the system is to be enhanced or terminated, summarize the actions to be taken this fiscal year. 		
Deliverable 58	O&M Runbook	Monthly	The O&M Runbook contains information and strategies designed to guide operational stakeholders in the normal use and maintenance of the Solution. The manual should be designed in a manner that facilitates actions and responses to anything that may arise during normal product operations and maintenance including but not limited to incident, problem,	<ul style="list-style-type: none"> a) The O&M Runbook incorporates testing, training, and reinforcement exercises that are planned and implemented. b) The clarity and effectiveness of the O&M Runbook has been validated through sample 	<ul style="list-style-type: none"> a) Technology Change Management Plan b) Configuration Management Plan and Database c) Assets Management Plan d) Event Management Plan e) Incident Management Plan 	Type C

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
			request, asset, event, and IT change management activities. The O&M Runbook guides those who maintain, support and/or use the system in a day-to-day operations environment.	<ul style="list-style-type: none"> testing by representative users. c) The O&M Runbook defines the target audience for specifies sections of the Runbook. d) The O&M Runbook defines the necessary skills required to perform said activities. 	<ul style="list-style-type: none"> f) Problem Management Plan g) Request Management Plan 	
Deliverable 59	System Go-Live Report	Once per release upon State approval	The System Go-Live Report is a record of how the implementation went. The focus is on deviations from what was considered default or what was planned. This information is critical for a successful transition to maintenance. It is also useful for project closure and for archival for future projects.	<ul style="list-style-type: none"> a) Describes at a high level the major problems encountered during data conversion activities and corrective actions that were applied to solve them b) Describes at a high level the major problems encountered while establishing the Production Environment and corrective actions that were applied to solve them c) Describe at a high level the major problems encountered during the move of the application to the production environment and corrective actions that were applied to solve them 		Type B

Deliverable #	Name	Frequency	Description	Exit Criteria	Artifacts	Review Cycle
Deliverable 60	Operational Readiness Plan and Report	Once per release upon State approval	<p>The Operational Readiness Plan and Report details and reports how the system/application is put into Production without verification that it meets performance requirements and that the operation and maintenance procedures ensure prompt system recovery without loss of data.</p> <p>The Operational readiness plan provides a checklist and an approach for carrying out readiness assessments activities.</p> <p>The Operational readiness activities include a review of the integrity of system data (data cleansing) and readiness for data conversion.</p> <p>The Operational readiness plan provides a mechanism to identify areas of deficiencies with sufficient detail to allow the business unit to prepare an action plan in response to the deficiency.</p> <p>The Operational readiness plan defines a communication plan which identifies points of contact for the relevant implementation stakeholders.</p>	<ul style="list-style-type: none"> a) The Operational Support Plan been completed and signed off. b) The Plan should ensure that the transition and knowledge transfer has successfully been completed and/or a O&M Contractor is in place c) The technical policies and processes are successfully operated in production d) User IDs for all roles are setup 	<ul style="list-style-type: none"> a) Operational Readiness Plan and Report b) System of Record Notice c) Operational Readiness Checklist 	Type A