United States Department of Health & Human Services

Office of the Chief Information Officer

Office of the Assistant Secretary for Resources and Technology

Department of Health and Human Services (HHS)

Enterprise Performance Life Cycle Framework

OVERVIEW DOCUMENT

January 18, 2010

VERSION HISTORY

This document is the culmination of a collaborative effort by the Enterprise Performance Life Cycle Framework (EPLC) Workgroup. This group is composed of OPDIV and HHS representatives. This document will go through a formal CIO review, approval process and sign off prior to Agency wide distribution for each new release. This document is intended to be a living document with periodic review and updates that are under the control of the OCIO CPIC Office. Versions and descriptions of change will be recorded in the table below.

Version Number	Revision Date	Approved By	Approval Date	Description of Change
1.0		EPLC Workgroup	05/07/2008	Baseline Document
1.1	06/26/2008			Added Enterprise Architecture Context Section 1.5
1.2	10/1/2008			Consistency and clarity edits Edits in response to OPDIV Review
1.3	1/18/2009			Includes updates from OPDIVs and Security Critical Partner change request comments

EXECUTIVE SUMMARY

The Office of Management and Budget (OMB) and the Congress are setting ever higher standards for the management and performance of information technology investments within the Federal government. Those standards require a project management and accountability environment where IT projects achieve consistently successful outcomes that maximize alignment with business objectives and meet key cost, schedule and performance objectives.

A key to successful IT management is a solid project management methodology that incorporates best government and commercial practices through a consistent and repeatable process, and provides a standard structure for planning, managing and overseeing IT projects over their entire life cycle. The HHS Enterprise Performance Life Cycle (EPLC) framework provides that methodology for HHS.

The EPLC framework consists of ten life cycle phases. Within each phase, activities, responsibilities, reviews, and deliverables are defined. Exit criteria are established for each phase and Stage Gate reviews are conducted through the IT Governance process to ensure that the project's management quality, soundness, and technical feasibility remain adequate and the project is ready to move forward to the next phase. The EPLC framework provides a guide to Project Managers, Business Owners, IT Governance Executives, other Stakeholders, and Critical Partners throughout the life of the project.

The EPLC framework is designed to provide the flexibility needed to adequately manage risk while allowing for differences in project size, complexity, scope, duration, etc. Examples of flexibility include the ability (with IT Governance approval) to tailor the framework where particular phases or deliverables may not apply, to aggregate phases and deliverables when appropriate, to provide for conditional stage gate approvals that allow progress to a subsequent phase in a manner that identifies and controls for risk. The EPLC framework also accommodates iterative development methodologies.

Implementation of the EPLC framework should allow HHS to improve the quality of project planning and execution, reducing overall project risk. Reducing risk, in turn, increases HHS' ability to move IT projects that best meet business needs into the production environment more quickly and with established cost constraints. The framework also provides an effective vehicle for adopting and propagating best practices in IT management. Finally, the framework provides a solid foundation for Project Manager training and certification and more effective IT Capital Planning.

The EPLC framework implementation is likely to shift more time and resources to the planning phases for projects and require additional resources from Project Managers, Business Owners, and IT Governance participants for review and approval activities. This increased investment in planning and oversight is expected to be more than offset by reduced resources spent in duplicative efforts and rework of avoidable errors.

Industry and government experience demonstrates that the quality of IT projects is directly proportional to the quality of the management processes used to acquire and operate the IT products those projects produce. Implementing the EPLC framework will help ensure the quality of HHS IT products through improved project management processes.

Table of Contents

Table of Figures

1. INTRODUCTION

1.1. Purpose

The purpose of this document is to provide an overview of the Department of Health and Human Services (HHS) Enterprise Performance Life Cycle (EPLC) framework. This document identifies the ten phases of the EPLC and describes the associated responsibilities, activities, exit criteria, deliverables and reviews associated with each phase.

This overview document is a result of work performed by the HHS EPLC Workgroup, composed of representatives from all Operating Divisions (OPDIVs).

1.2. Scope

The HHS EPLC framework applies to all HHS IT investments and projects, including but not limited to new projects, major enhancements to existing projects, projects associated with steady state investments, high-priority, fast-track IT projects, and new Commercial Off-the-Shelf (COTS) product acquisitions.

A large investment may consist of a single project, or of several logically related projects. For the purposes of this document, an investment will be assumed to consist of a single project. Considerations for managing investments composed of multiple projects are provided in Section 4. The EPLC framework is compatible with the current policy scope. It applies to the Operating Divisions, all Staff Divisions (STAFFDIVs), and the Office of the Inspector General, (hereinafter referred to collectively as “HHS OPDIVs”). The EPLC framework has an initial focus on the life cycle of information technology (IT) projects. Eventually, the scope may be expanded to address non-IT projects.

1.3. Background

Information technology plays a critical role in helping HHS carry out its complex, wide-ranging and evolving mission and objectives. HHS uses IT investments to support more than 300 programs that protect the health of all Americans and provide essential human services. Those programs are administered by OPDIVs which have responsibilities throughout the country. Each year, HHS invests more than $2 billion to ensure that its OPDIVs have the technology to support their programs. HHS IT investments include software and computer systems interconnected through nationwide networks. Many HHS systems are interconnected with partners in the federal, state, local, tribal and private sectors. As a result, HHS has a very complex and difficult task in ensuring that its diverse IT investments are properly aligned within a coherent Enterprise Architecture.

HHS approaches the management of IT projects from an enterprise perspective that facilitates smooth interfaces among HHS IT projects and with HHS partners. These projects and their interfaces must be adequately established through appropriate enterprise architecture. Adhering to recognized IT standards, as well as to Section 508, security and privacy requirements is essential to this goal. By managing and governing its projects from an enterprise perspective, HHS will be in a better position to take advantage of economies of scale, as it purchases computers, related equipment and software on a large scale -- maximizing its bargaining and buying power. Furthermore, this enterprise perspective will enable improved compliance with the Clinger-Cohen Act and other legislative and regulatory requirements that require HHS to manage and govern its IT projects from an enterprise perspective.

In addition to focusing on the planning, development, operation and management of individual IT projects, HHS must also ensure that the overall portfolio of IT projects achieves alignment with HHS strategic goals and maximizes the return on the Department's IT project. The HHS IT Capital Planning and Investment Control (CPIC) Program, in conjunction with the IT Governance process, brings together the various critical partners required to ensure maximum IT portfolio performance.

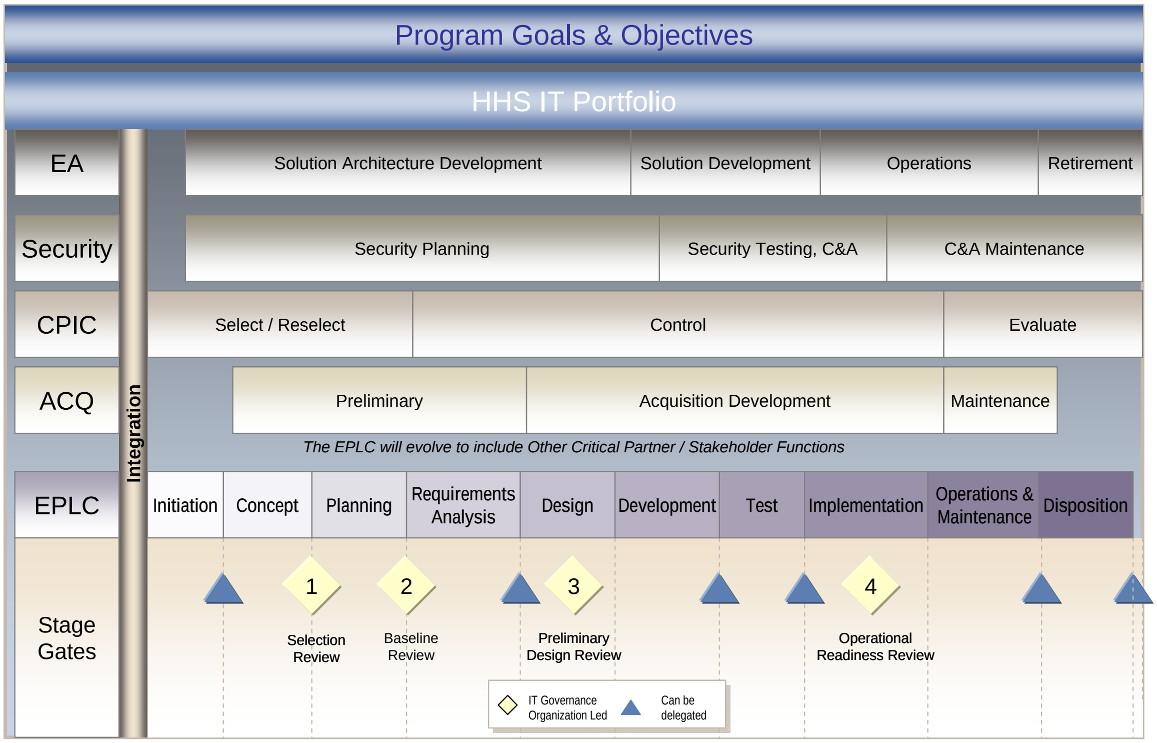
The EPLC framework is part of an ongoing effort by HHS to further strengthen its IT management and governance processes. With this new enterprise-wide approach to project management, there will also be a greater emphasis by the Department on demonstrating measurable results for each of its IT projects and to better justify actions taken as IT projects are being developed.

1.4. Vision

The EPLC framework will help establish a project management and accountability environment where HHS IT projects achieve consistently successful outcomes that maximize alignment with Department-wide and individual OPDIV goals and objectives. Figure 1 illustrates the context of the EPLC.

This overview document is supplemented with support materials, such as practices guides and templates that have been created by the EPLC Workgroup. The EPLC framework will be modified as experience dictates. For example, if a particular deliverable is frequently added as part of the tailoring process, this deliverable will be considered for addition to the EPLC. The reader is also directed to review critical partner web sites (Enterprise Architecture, CPIC, Security, etc.) for additional individual policy guidance.

Figure 1 - Enterprise Performance Life Cycle Context



1.5. Enterprise Architecture Context

The Office of Management and Budget (OMB) has prescribed a frame of reference for linking goals to results. This Performance Improvement Life Cycle (PIL) has three-phases: "Architect", "Invest" and "Implement" (Figure 2). Each life cycle phase is comprised of integrated enterprise processes which combine to transform the agency's top-down strategic goals and bottom-up system needs into a logical series of work products designed to help the agency achieve strategic results. Through this process integration, the Performance Improvement Lifecycle provides the foundation for sound IT management practices, end-to-end governance of IT investments, and the alignment of IT investments with an agency's strategic goals so an agency can achieve its desired mission outcomes and business results.

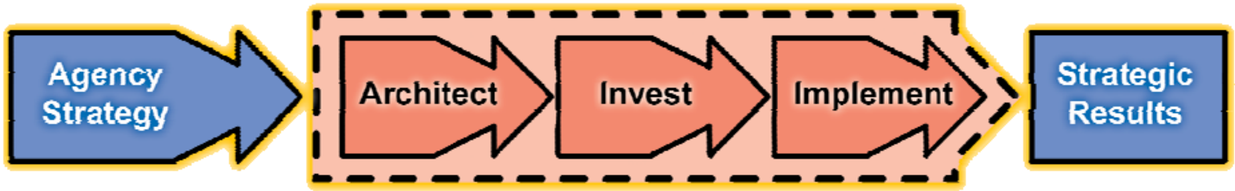


Figure 2: Performance Improvement Life Cycle

Figure 3 below highlights the HHS Performance Improvement Lifecycle which extends this integrated process model to include other key HHS management processes.

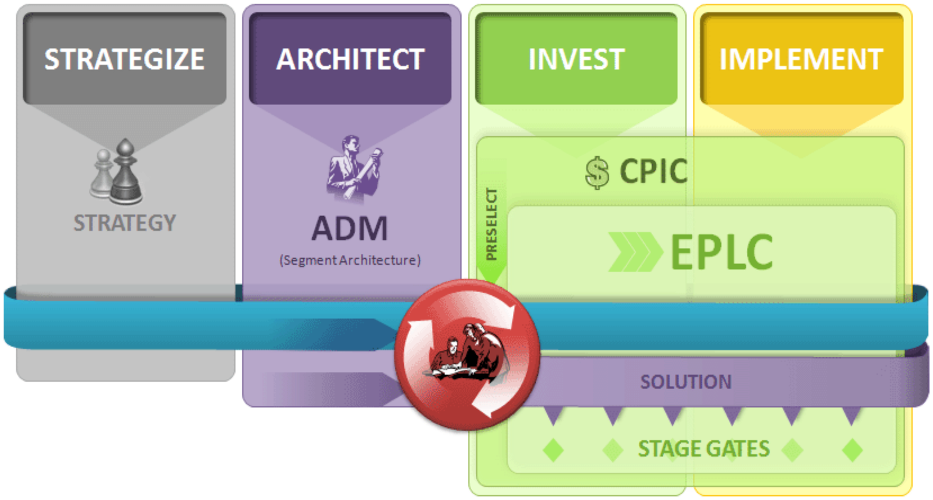


Figure 3: HHS Performance Improvement Life Cycle

The Strategize Phase establishes the strategic HHS business and technology direction. HHS enterprise needs are, in part, derived from external drivers such as legislative mandates or other capabilities to be pursued as a mechanism to improve mission performance. In many cases the need to be satisfied will correspond to a gap between the current state of HHS organizational capabilities and an intended future state.

A primary function of the Architect Phase is the identification and analysis of capability gaps between that current and future state. HHS organizes architecture work primarily through segments of functionality within a common business area. Analysis of segments of business functionality reveals the need for an investment to fill a particular capability gap. Analysis of segments of functionality results in a common framework of compatibility and interoperability within which related projects can be made. The HHS Architecture Development Methodology describes how this analysis of segments is accomplished.

The Invest Phase ensures the alignment of sound business project selections in support of strategic, and sometimes tactical, goals and objectives.

The Implementation phase ensures that projects and investments are executed according to agreed upon project or investment management plans. This phase also measures performance to determine how well the implementation solutions achieve the desired results and mission outcomes.

Leveraging the HHS Performance Improvement Life Cycle and monitoring the effective management of projects throughout the EPLC provides validation and assurances that a project or investment is addressing specified capability gaps and providing the intended performance improvements.

1.6. Key Definitions

The table below contains key definitions used throughout the methodology.

IT Portfolio The combination of all IT assets, resources, and investments owned or planned by an organization in order to achieve its strategic goals, objectives, and mission.

IT Investment An organizational investment employing or producing IT or IT-related assets. Each investment has or will incur costs for the investment, has expected or realized benefits arising from the investment, has a schedule of project activities and deadlines, and has or will incur risks associated with engaging in the investment.

IT Project A project is a temporary planned endeavor funded by an approved information technology investment; thus achieving a specific goal and creating a unique product, service, or result. A project has a defined start and end point with specific objectives that, when attained signify completion.

1.7. Benefits

The following outcomes and benefits are expected to accrue from implementation of the EPLC framework:

- Ability to leverage EPLC-type frameworks long established in the private sector as best practices to yield substantial benefits to HHS.
- Establish a foundation and supporting structure designed to aid in the successful planning, engineering, implementation, maintenance, management, and governance of HHS IT projects.
- Improved project planning and execution by project managers, and faster propagation of best practices in the project management community.
- Improved management response for individual IT projects and the broader IT investment portfolio to budgetary and other strategic changes through deliberate and approved baseline changes that fully consider Enterprise Architecture (EA), security and other impacts.
- Movement of IT projects into the production environment more quickly and with higher quality.
- Better operational support for production systems.
- Better measurement of IT performance (both at the individual project and at the portfolio level).
- More timely identification and resolution of project issues, reducing the risk of cost overruns, schedule delays, scope creep, and other typical pitfalls.
- Improved competitiveness of IT projects in the budget process through improved performance management and linkage of IT investments to program mission.

- Enhancement of the CPIC Select, Control and Evaluate processes for IT investment portfolio management.
- Integration of the IT Investment Management (ITIM) and software development life cycles into one HHS IT enterprise performance life cycle.
- Greater re-use of activities and deliverables by Integrated Project Team members when moving among different projects.

1.8. Impact

The EPLC framework implementation is likely to shift more time and resources to the planning phases for projects and require additional resources from Project Managers, Critical partners and IT Governance organization participants for review and approval activities. This increased investment in planning and oversight is expected to return dividends in reduced program risk and less effort expended in rework or fixing foreseeable problems.

1.9. Goals and Objectives

HHS has established the following goals and objectives for EPLC framework implementation:

Goal 1: Provide a coherent and effective project management methodology to guide IT project management at HHS. The methodology is intended to consistently deliver IT capabilities that provide maximum support to HHS business needs within approved cost and schedule constraints.

Objectives:

- Expand the role of Business Owners throughout the IT project life cycle to ensure that IT projects remain targeted on highest priority business needs and meet necessary schedule and cost constraints.
- Improve project performance by applying repeatable processes and industry-leading practices for project and earned value management.
- Provide guidance to Project Managers regarding the activities and deliverables required for project planning and execution throughout all stages of project management.
- Establish a minimum set of core activities and deliverables for all IT projects.
- Require additional activities and deliverables based on individual project circumstances.
- Provide project templates and tools to help jump-start project activities.
- Provide examples from other projects for reference.
- Standardize IT project management within HHS based on best practices.
- Encourage employment of best practices.
- Identify key processes that each project must follow to meet Federal regulations and other compliance mandates.

Goal 2: Better integrate IT project planning and execution with IT Governance, including more effective multi-disciplinary reviews of IT projects by the Critical Partners.

Objectives:

- Facilitate alignment of IT projects with the HHS Strategic Plan.
- Streamline the IT Governance process.
- Provide a more effective process for integrating multi-disciplinary Critical Partner reviews into the IT Governance process.
- Establish clear, reasonable expectations and practical standards/guidelines.
- Ensure compliance with HHS Enterprise Architecture (EA) and prescribed design standards.

2. THE EPLC FRAMEWORK CONCEPT

The EPLC framework organizes the activities, deliverables and governance reviews of an IT project into ten life cycle phases. The EPLC framework provides a project management methodology that guides the activities of project managers, Business Owners, Critical Partners, IT Governance organization and other stakeholders throughout the life cycle of the project to ensure an enterprise perspective is maintained during planning, execution and governance processes. Although one of the objectives of the EPLC framework is to standardize IT project management within HHS based on best practices, the framework also allows tailoring to accommodate the specific circumstances (e.g., size, duration, complexity, and acquisition strategy) of each project.

Use of the EPLC framework and associated best practices in IT project management is intended to reduce risk within individual IT projects and across the HHS IT project portfolio. HHS will select only sound, viable IT projects with reasonable baselines for funding and inclusion in the IT project portfolio. IT projects will be managed and implemented in a structured manner, using sound project management practices, and ensuring involvement by business stakeholders and technical experts throughout the project's life cycle. IT projects will be evaluated for how well they have achieved their business objectives. IT project performance will be measured against established business outcomes and will be subject to changes as appropriate.

A detailed explanation of the framework and its components is shown below. In summary:

- Project Managers are responsible for proposing any tailoring they believe is appropriate for IT Governance organization approval, then planning for and executing the activities, deliverables and reviews required.

- The Stage Gate Review Lead will coordinate Critical Partner reviews and facilitate resolution of issues that arise during the course of the project.

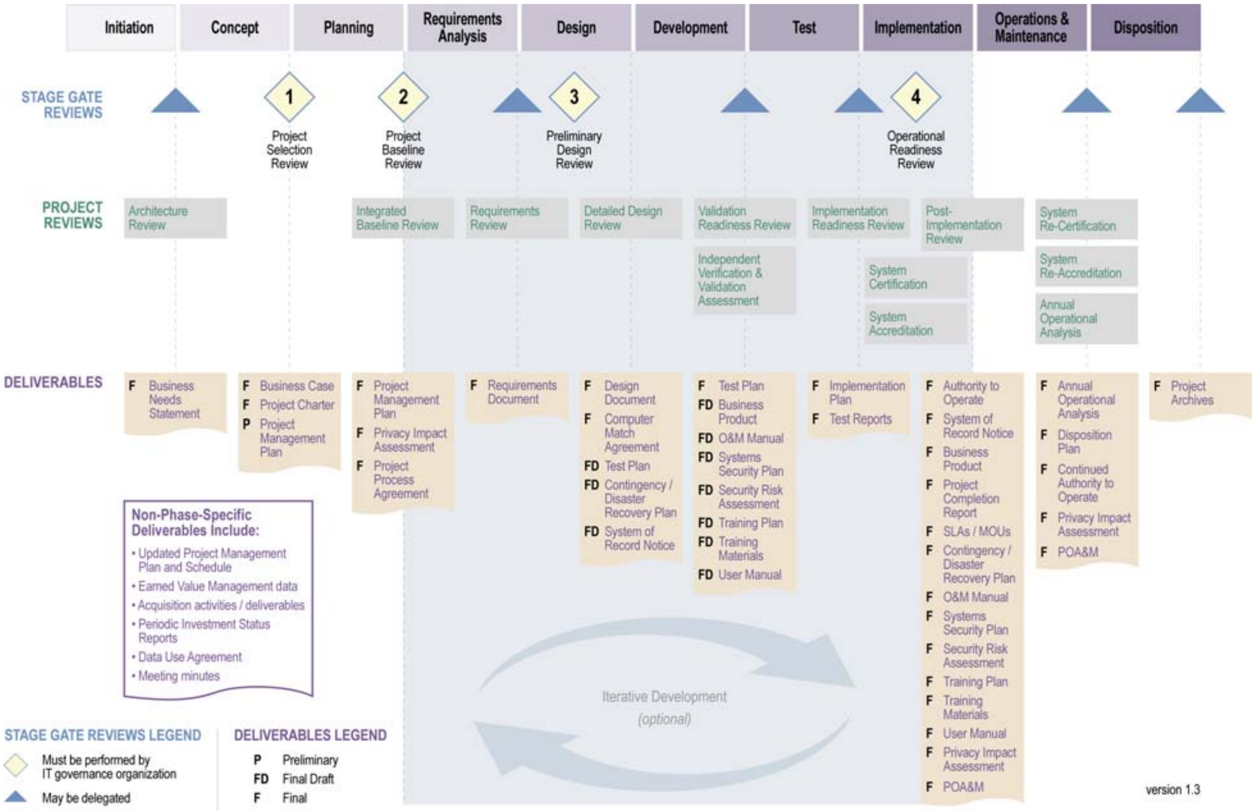
- During Stage Gate Reviews under the direct cognizance of the IT Governance organization, the Critical Partners will review documents for completeness, accuracy and adequacy and make recommendations to the IT Governance organization regarding quality of work performed under the framework, any resolved issues, and projects readiness to advance to the next life cycle phase.

- The IT Governance organization will review the Critical Partner recommendations and decide whether to require additional work to meet exit criteria or to approve advancement to the next Phase. For Stage Gate Reviews that have been delegated to the Project Manager, the Project Manager will apply the same standards and complete the same review documentation as the IT Governance organization.

2.1. EPLC Framework Elements

This subsection defines the basic elements of the EPLC framework: the life cycle phases, stakeholders, phase activities and deliverables, exit criteria, project reviews and stage gates. Figure 4 provides an overview.

Figure 4 - Enterprise Performance Life Cycle


Initiation
Concept
Planning
Requirements Analysis
Design
Development
Test
Implementation
Operations & Maintenance
Disposition
STAGE GATE REVIEWS
1
Project Selection Review
2
Project Baseline Review
3
Preliminary Design Review
4
Operational Readiness Review
PROJECT REVIEWS
Architecture Review
Integrated Baseline Review
Requirements Review
Detailed Design Review
Validation Readiness Review
Independent Verification & Validation Assessment
Implementation Readiness Review
System Certification
System Accreditation
Post-Implementation Review
System Re-Certification
System Re-Accreditation
Annual Operational Analysis
DELIVERABLES
F Business Needs Statement
F Business Case
F Project Charter
P Project Management Plan
F Project Management Plan
F Privacy Impact Assessment
F Project Process Agreement
F Requirements Document
F Design Document
F Computer Match Agreement
FD Test Plan
FD Contingency / Disaster Recovery Plan
FD System of Record Notice
F Test Plan
FD Business Product
FD O&M Manual
FD Systems Security Plan
FD Security Risk Assessment
FD Training Plan
FD Training Materials
FD User Manual
F Implementation Plan
F Test Reports
F Authority to Operate
F System of Record Notice
F Business Product
F Project Completion Report
F SLAs / MOUs
F Contingency / Disaster Recovery Plan
F O&M Manual
F Systems Security Plan
F Security Risk Assessment
F Training Plan
F Training Materials
F User Manual
F Privacy Impact Assessment
F POA&M
F Annual Operational Analysis
F Disposition Plan
F Continued Authority to Operate
F Privacy Impact Assessment
F POA&M
F Project Archives
Non-Phase-Specific Deliverables Include:
• Updated Project Management Plan and Schedule
• Earned Value Management data
• Acquisition activities / deliverables
• Periodic Investment Status Reports
• Data Use Agreement
• Meeting minutes
Iterative Development
(optional)
STAGE GATE REVIEWS LEGEND
Must be performed by IT governance organization
May be delegated
DELIVERABLES LEGEND
P Preliminary
FD Final Draft
F Final
version 1.3

2.1.1. Life Cycle Phases

The EPLC framework consists of ten life cycle phases. Listed below are the phases and a brief description of each.

- **Initiation –** Identifies the business need, develops a Rough Order of Magnitude (ROM) cost and preliminary schedule, and basic business and technical risks. The outcome of the Initiation Phase is the decision to invest in a full business case analysis and preliminary project management plan.

- **Concept –** Identifies the high level business and functional requirements required to develop the full business case analysis and preliminary Project Management Plan for the proposed project. The outcomes of the Concept Phase are selection to the HHS IT project portfolio; approval of initial project cost, schedule and performance baselines; and issuance of a Project Charter.

- **Planning –** Completes development of a full Project Management Plan and if applicable, refinement of project cost, schedule and performance baselines.

Outcomes of the Planning phase are a complete and adequate project planning with sufficient requirements development to validate the planning and project baselines.

- **Requirements Analysis –** Develop detailed functional and non-functional requirements, the Requirements Traceability Matrix (RTM) and award contracts if needed. The outcome of the Requirements Analysis Phase is award of contracts if needed and approval of the requirements.
- **Design –** Develops the Design Document. The outcome of the Design Phase is completion of the Business Product design and successful completion of Preliminary and Detailed Design Reviews with physical Enterprise Architecture diagrams as needed.
- **Development –** Develops code and other deliverables required to build the Business Product and conduct an Independent Verification & Validation Assessment. The outcome of the Development Phase is completion of all coding and associated documentation; user, operator and maintenance documentation, and test planning.
- **Test –** Thorough testing and audit of the Business Product's design, coding and documentation. The outcome of the Test Phase is completed acceptance testing and readiness for training and implementation.
- **Implementation –** Conduct user and operator training, determine readiness to implement, and execute the Implementation Plan, including any phased implementation. The outcome of the Implementation Phase is successful establishment of full production capability and completion of the Post-Implementation Review.
- **Operations and Maintenance –** Operate and maintain the production system and conduct annual operational analyses. The outcome of the Operations and Maintenance Phase is successful operation of the asset against current cost, schedule and performance benchmarks.
- **Disposition –** Retires an asset when operational analysis indicates that it is no longer cost-effective to operate the asset. The outcome of the Disposition Phase is the deliberate and systematic decommissioning of the Business Product with appropriate consideration of data archiving and security, migration of data or functionality to new assets, and incorporation of lessons learned over the project life cycle.

A more detailed description of each phase and the various tasks required to be performed during each phase are provided in Section 3.

2.1.2. Stakeholders

This subsection lists the typical stakeholders for an IT project over its life cycle. Each stakeholder plays an essential role in execution of the EPLC framework and the success of HHS IT projects. The role of each stakeholder varies throughout the life cycle. Stakeholder roles are discussed in more detail later in this document.

IT Governance: Responsible for ensuring that the project is technically sound; follows established IT project management practices; and meets the Business Owner's needs. Components of the IT Governance organization are:

- Information Technology Investment Review Board (ITIRB).
- CIO Council/Technical Review Board.
- Chief Information Officer (CIO).

Similar IT Governance organizations will be established at both the Department and OPDIV levels.

Stage Gate Review Lead: Responsible for coordination of the Critical Partners for Stage Gate Reviews.

Critical Partners: Critical Partners are functional managers in the areas of: Enterprise Architecture, Security, Acquisition Management, Finance, Budget, Human Resources, Section 508, CPIC, and Performance. The Critical Partners are considered subject matter experts and participate in the IT project, in the IT Stage Gate reviews, and governance decisions to ensure compliance with policies in their respective areas. They assist in making timely tradeoff decisions where conflicts arise during the planning and execution of a project. Because organizational structures vary in HHS and the OPDIVs, the expertise for these Critical Partner roles may be fulfilled from a mixture of organizations, as appropriate. The CPIC Critical Partner Role is responsible for reviewing the Project documentation and cost and schedule as key measures of Project Management performance. Because the Performance Critical Partner is responsible for evaluating whether the project meets the business objectives, this review would logically be done by the Business Owner.

Project Management

- **Project Manager (PM)**: The Project Manager is responsible for project performance in relation to approved cost, schedule and performance baselines. The Project Manager maintains information project status, control, performance, risk, corrective action and outlook. This person is accountable to the Business Owner for meeting business requirements and to IT Governance for meeting IT project management requirements.
- **Integrated Project Team (IPT):** The IPT is chaired by the Project Manager with Critical Partner and Business Owner representatives to assist the Project Manager with planning and execution of the project.

Business Owner: The executive in charge of the organization, who serves as the primary customer and advocate for an IT project. The Business Owner is responsible for identifying the business needs and performance measures to be satisfied by an IT project; providing funding for the IT project; establishing and approving changes to cost, schedule and performance goals; and validating that the IT project initially meets business requirements and continues to meet business requirements.

In-House Development and Operations Teams: Technical personnel that execute projects are expected to follow the EPLC framework and be integral partners in the HHS project management process.

Contractors: Much of HHS' IT development and operations are outsourced to contractor support. Contractors must follow the EPLC framework and be integral partners in the HHS project management process.

End Users: Individuals who physically use the final product for data input, reports, etc.

Infrastructure Support Staff: Staff providing common infrastructure equipment and services that both impact on and are impacted by IT project development and operations must be an integral part of the EPLC process.

2.1.3. Phase Activities and Deliverables

Activities to be performed and specific deliverables that are required to document those activities are established for each phase of the life cycle. A complete list of deliverables is in Appendix C. Deliverable templates may be found at: http://www.hhs.gov/ocio/eplc/Enterprise%20Performance%20Lifecycle%20Artifacts/eplc_artifacts.html. Activities are established based on statute, regulation, policy and best practice and are designed to reduce project risk.

EPLC references several Security artifacts. These include the Privacy Impact Assessment System Security Plan, Security Risk Assessment, System of Record Notice, and Security Certification and Accreditation Letters. For a list of all Security artifacts, please refer to Appendix E. Security controls must be established and integrated into EPLC activities, phases, and reviews.

Many activities and deliverables go through iterative cycles during the life cycle, with an initial effort, updates during one or more subsequent phases, and a final deliverable as illustrated in Figure 5. A preliminary Project Management Plan is required to provide sufficient cost and schedule estimates for the IT Governance organization to make an informed decision about selection. A Final Draft is a deliverable that is complete in the opinion of the Project Manager; the Final version will be the same unless changes are required as a result of testing and final coordination. Some deliverables (particularly baselines and project plans) undergo change control in which the IT Governance organization must approve initial documents and any subsequent changes. Each year the Project Manager may provide updated deliverables associated with the project's Operations and Maintenance phase.

Figure 5 - Deliverables by Phase

EPLC Deliverables by Phase	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	Operations and Maintenance	Disposition
Business Needs Statement	F									
Business Case		F								
Project Charter		F								
Project Management Plan		P	F							
Privacy Impact Assessment			F					F	F	
Project Process Agreement			F							
Requirements Document				F						
Design Document					F					
Computer Match Agreement					F					
Test Plan					FD	F				
Contingency/Disaster Recovery Plan					FD			F		
System of Records Notice					FD			F		
Operations & Maintenance Manual						FD		F		
Systems Security Plan						FD		F		
Training Plan						FD		F		
Training Materials						FD		F		
User Manual						FD		F		
Security Risk Assessment						FD		F		
Business Product						FD		F		
Test Reports							F			
Implementation Plan							F			
Authority to Operate								F	F	
Project Completion Report								F		
SLAs/MOUs								F		
Annual Operational Analysis									F	
Plan of Action & Milestones								F	F	
Disposition Plan									F	
Project Archives										F

Legend:	P	Preliminary
	FD	Final Draft
	F	Final

EPLC templates, checklists and practices guides can be found at http://www.hhs.gov/ocio/eplc/Enterprise%20Performance%20Lifecycle%20Artifacts/eplc_artifacts.html

Please refer to Appendix E for Security artifacts.

2.1.4. Exit Criteria

Exit Criteria must be achieved before proceeding to the next phase. On an exception basis, the IT Governance process can permit advancement to the next phase without completion of some exit criteria, but will condition that advancement on specific required actions and due dates to satisfy the exit criteria at the earliest possible date. Before Exit Criteria are reviewed, the Project Manager will verify that the set of deliverables for the Phase is complete and acceptable.

Generic Exit criteria are set to monitor the overall status of the project and any necessary corrective actions taken to bring the project into alignment with original goals. Rebaselining may require updates to documentation and additional IT Governance approval.

2.1.5. Project Reviews

Project reviews are formal reviews led by the Project Manager. Project reviews are conducted at specific points in the life cycle to ensure that events have occurred and decisions have been made before continuing with the project. The Stage Gate Review will ensure that any required project reviews have been successfully conducted in addition to ensuring that required deliverables are complete, accurate and compliant with EPLC.

2.1.6. Stage Gate Reviews

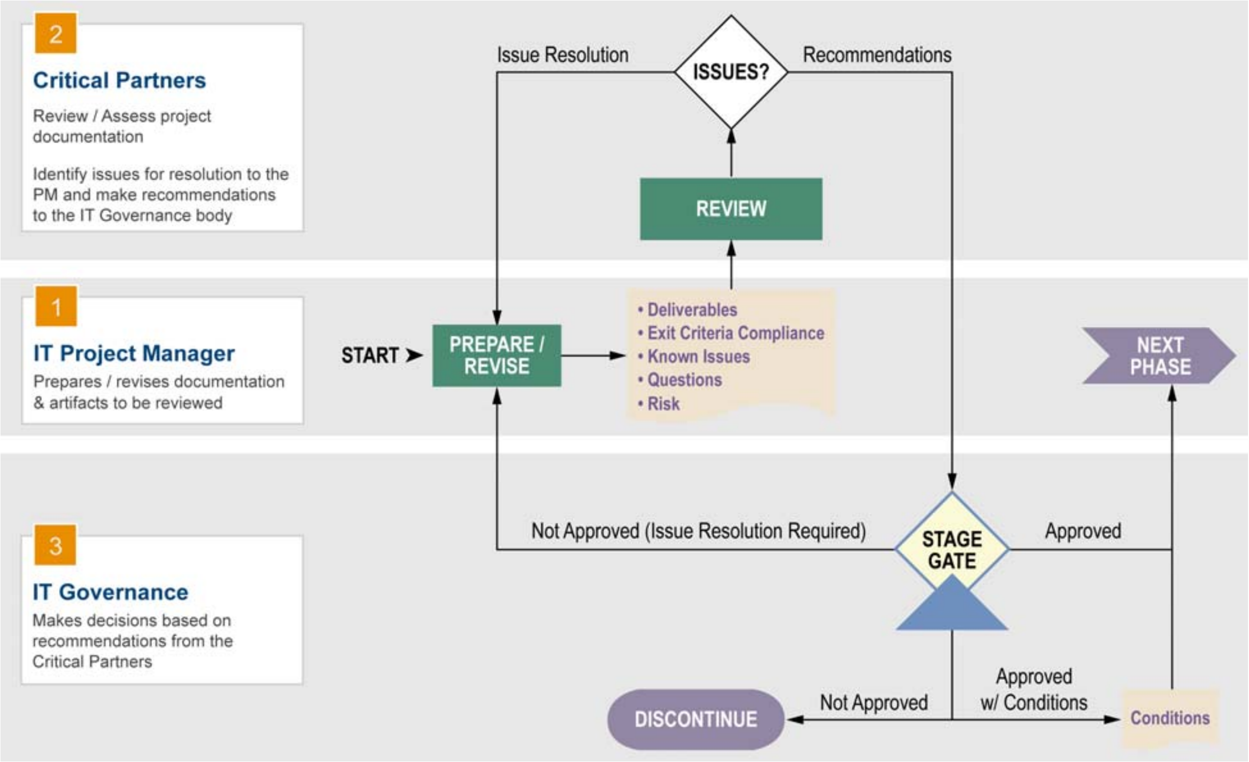
Stage Gate Reviews are required during a phase or at the end of each phase to provide for independent review and approval of key elements of the IT project's development or operation. Stage Gate Reviews consist of an independent confirmation by Critical Partners to the IT Governance organization that Project Managers satisfactorily produced all the required deliverables and adequately met all exit criteria for the phase to permit advancement to the next phase. The Project Manager is also responsible for providing documentation of known issues and plans to mitigate the risks, if any.

The emphasis of Stage Gate Reviews is on:

- The successful accomplishment of the phase objectives.
- The plans for the next life cycle phase.
- The risks associated with moving into the next life cycle phase.

Stage Gate Reviews also address the availability of resources to execute the subsequent life cycle phases. The results of the review by the Critical Partners are provided with recommended action to the IT Governance organization for decision. The Stage Gate Review process is illustrated in Figure 6.

Figure 6 - Stage Gate Review Process


2
Critical Partners
Review / Assess project documentation
Identify issues for resolution to the PM and make recommendations to the IT Governance body
1
IT Project Manager
Prepares / revises documentation & artifacts to be reviewed
3
IT Governance
Makes decisions based on recommendations from the Critical Partners
Issue Resolution
ISSUES?
Recommendations
REVIEW
START
PREPARE / REVISE
• Deliverables
• Exit Criteria Compliance
• Known Issues
• Questions
• Risk
NEXT PHASE
Not Approved (Issue Resolution Required)
STAGE GATE
Approved
Approved w/ Conditions
Not Approved
DISCONTINUE
Conditions

The IT Governance organization may choose to approve the project's continuation to the next phase with or without conditions. Approval with conditions requires the IT Governance organization to establish a process for maintaining oversight of the project to ensure conditions are met. The IT Governance organization may require issue resolution by the Project Manager before approving continuation, and is responsible for discontinuing any project which fails to resolve serious issues.

With the exception of four Stage Gate Reviews that must be conducted by the IT Governance organization (as shown in Figure 6 above), the IT Governance organization may delegate conduct of Stage Gate Reviews to the Project Manager or other entity as designated by the OPDIV if appropriate due to such factors as size of a project level of technical risk, complexity, and essentiality to the HHS mission. For example, most complex and long-term projects (e.g., on the scale of UFMS) would likely require Stage Gate Reviews by the IT Governance organization after every phase and multiple periodic reviews during a phase, while many projects with shorter life cycles would require less extensive review that could, in many cases, be delegated to the Project Manager.

Any Stage Gate Review not conducted by the IT Governance organization will be delegated to the Project Manager, who will apply the same standards and will complete the same review documentation as the IT Governance organization would have. If the Project Manager conducting any Stage Gate Review determines that a change in project cost, schedule or performance baselines is required, the Project Manager must elevate the Stage Gate Review to the IT Governance organization.

The Stage Gate Reviews requiring IT Governance organization review are:

- Project Selection Review (at the conclusion of the Concept Phase).
- Project Baseline Review (at the conclusion of the Planning Phase).
- Preliminary Design Review (during the Design Phase).
- Operational Readiness Review (during the Implementation Phase).

More information about these reviews is included in Section 3, in the phases where they occur.

2.2. Approach

This subsection describes the basic approach used in the EPLC framework. All framework activities fall into three categories: create, review and approve.

2.2.1. Project Management Orientation (Create)

The Project Manager is ultimately responsible for planning and conducting phase activities within established project cost, schedule and performance baselines, subject to guidance and direction from the IT Governance organization and the Business Owner.

The primary means for planning, executing and accountability for project activities is the collection of managerial documents defined as the Project Management Plan (PMP). HHS uses the PMP as the principal tool for organizing and managing IT projects throughout the EPLC. The PMP establishes the baselines and benchmark activities that project performance will be reported and tracked against. Project Managers keep the PMP current by updating its subordinate-level plans as required to reflect changes and refinements during the life cycle.

2.2.2. Critical Partners (Review)

Critical Partners have the primary responsibility to review progress of IT projects at specified Stage Gate Reviews to ensure that the project meets the Critical Partners' respective requirements. Critical Partners are responsible for evaluating the completeness, accuracy and adequacy of phase deliverables and for evaluating whether the project meets exit criteria for advancement to the next phase. These stakeholders will provide recommendations and any issues identified to the IT Governance organization and the Business Owner based on their review.

The Stage Gate Review Lead facilitates the review by the several Critical Partners, and ensures that cross-functional issues are either resolved at the staff level or articulated to the IT Governance organization for resolution. The Stage Gate Review Lead also consolidates Critical Partner recommendations for presentation to the IT Governance organization.

2.2.3. IT Governance (Approve)

The IT Governance organization is ultimately responsible for selecting projects for the IT project portfolio, approving Project Baselines and controlling changes to those baselines, monitoring performance against Project Baselines and requiring corrective actions where necessary, conducting Stage Gate Reviews through Critical Partners, and approving Stage Gate completion.

2.3. Impact on HHS IT Project Management

Implementation of the EPLC framework should have the following implications for IT project management within the Department:

- Continued training requirements for IT Governance Executives, Critical Partners, Project Managers, Integrated Project Team members and other stakeholders to understand and effectively apply the EPLC framework.
- A shift in management resources to earlier in the life cycle through greater emphasis on planning and documentation.
- Increased role for Business Owners, Critical Partners, IT Governance Executives and other stakeholders in the IT project management process.
- Better balance between authority and accountability within the IT project management process by ensuring that decisions are made at the lowest level at which accountability can be established. The goal is to delegate both authority and accountability as low within the organization as possible.
- Greater transparency regarding IT project management information and decision making.
- Better resource estimates and consideration of resource limitations in setting project cost, schedule and performance baselines to avoid over-tasking limited resources.

2.4. Ongoing Project Management Deliverables

Certain project management activities are inherently required in every life cycle phase. Those activities are described here rather than repeating them in each phase. Project management activities include:

- Application of knowledge, skills, tools, and techniques to project activities to meet the project requirements.
- Ongoing updates to the Project Management Plan, including the Risk Management and Issues Logs.
- Ongoing Earned Value Management (EVM) and status reporting to measure compliance with baselines and take timely corrective action, as appropriate.
- Ongoing management of scope and change requests.
- Ongoing communications to ensure all stakeholders are apprised appropriately.
- Ensuring that security requirements are considered and met early in the project management process thereby increasing compliance and improving the security of complete projects.

Project management deliverables to be submitted on an established periodic basis include:

- Integrated Baseline Documentation.
- Independent Verification & Validation (IV&V) Reports.

- Contractor Performance Report (CPR) (or acceptable equivalent, if full EVM standards compliance is not required).
- Contract Fund Status Report (CFSR) (or acceptable equivalent, if full EVM standards compliance is not required).
- Updated Project Schedule.
- Periodic Project Status Reports.
- Meeting Minutes.

Independent Verification & Validation (IV&V) is a rigorous independent process that evaluates the correctness and quality of the Business Product to ensure that it is developed in accordance with customer requirements and is well-engineered. IV&V partnerships provide high value to many projects and may be introduced at any Phase of a project as determined by OPDIV project and governance requirements. Depending on project size, risk and other factors, the IT Governance organization may approve tailoring the IV&V requirement to match the project requirement.

2.5. Tailoring

An essential element of the EPLC framework is the ability to tailor framework requirements to the specific circumstances of each project. By doing so, HHS will be able to preserve a consistent and repeatable project management methodology while recognizing in a deliberate manner when certain elements of the framework are not applicable or not cost-effective for a particular project. The EPLC framework does not preclude OPDIVs from requiring more rigor.

2.5.1. Concept

The EPLC framework provides a complete list of activities, deliverables and reviews that are necessary to properly manage and control a large-scale, mission-critical, high-risk system. However, not all HHS projects fall into this category. While all projects require adequate documentation and deliverables to ensure that they are progressing appropriately and to provide management with enough information to make informed decisions concerning the future of the system, lower risk projects do not need as much documentation to maintain appropriate oversight and control. To meet the needs of HHS projects, the EPLC framework will provide criteria to assist Project Managers, Critical Partners, and IT Governance personnel in assessing appropriate tailoring of the EPLC framework.

Tailoring consists of waiving particular life cycle phases, activities, deliverables or reviews. The tailoring strategy will provide the justification for the tailoring as well as identify the specific elements of the framework to be tailored. The tailoring strategy for the project is described in the Project Process Agreement, which is formally approved at the Project Baseline Review. Any subsequent change to the Project Process Agreement must be approved by the IT Governance organization.

2.5.2. Evaluation Factors for Framework Tailoring

There are some fundamental elements that can never be removed from EPLC framework through tailoring. These include:

- Identifying the business need.

- Documenting correct, clear and adequate functional and non-functional requirements.
- Following processes that ensure the system will be able to operate within the as-is and/or target enterprise architecture.
- Adequate Business Product testing.
- Appropriate operations and maintenance documentation.

Otherwise, Project Managers, Critical Partners and the IT Governance organization should include consideration of the following factors in determining the tailoring strategy for a project:

- **Cost:** As cost decreases, framework elements that mitigate cost risk or that are relatively expensive are candidates for tailoring.
- **Risk:** Framework elements that mitigate low-level risks are candidates for tailoring.
- **Schedule:** Framework elements that provide for "corporate knowledge" or continuity over time or during team turnover are candidates for tailoring if the schedule is short enough to lower those risks.
- **Acquisition Strategy:** Contracts awarded for contractor developed or operated projects should require project management methodologies equivalent to the EPLC framework for tasks and deliverables. Tasks and deliverables provided under performance-based contracts are candidates for tailoring if they mitigate risk. Note also that, while COTS projects may be candidates for tailoring of some EPLC Development Phase activities, COTS projects must accomplish most activities in other Phases to ensure proper project selection, Enterprise Architecture compliance, security, implementation, Operations and Maintenance support, etc.
- **Development Methodology:** Choice of development methodology is likely to affect the iterative nature of the framework elements, but is unlikely to offer significant tailoring opportunities solely on the basis of development methodology.

2.6. Fast Track Projects

Mission-critical, urgent projects demand rigorous planning and monitoring. The EPLC is intended to enable HHS to successfully manage risk, thus it is especially important that the EPLC be applied to fast track projects. The Project Process Agreement deliverable for each project defines how the EPLC is to be tailored. Options for tailoring include:

- **Acceleration:** For example, the initiation phase of the EPLC is designed in part to answer the question "are we doing the right thing?" In the case of some projects, such as a legislatively-mandated program, the answer to this question is largely pre-determined. Acceleration does not relieve the project manager of the need to demonstrate that the proposed project will meet the requirements stated in the mandate and do so in the optimal manner.
- **Consolidation:** It is possible to tailor the EPLC framework so that phases are consolidated.

- **Deferral:** At Stage Gate Reviews, the IT Governance organization has the option to approve with conditions. If all exit criteria are not met, the IT Governance organization may accept the risk of moving forward with the condition that those criteria will be met at a later date.

Tailoring may be more appropriate for smaller projects.

2.7. Development Methodologies/Iterative Nature

The EPLC framework applies to all projects, regardless of the development methodology used, and can be applied appropriately to meet the particular needs of the methodology applied. Specifically, the framework can accommodate the iterative nature of many development methodologies (including the "waterfall", Spiral, Rapid Application Development, Incremental, and Rapid Prototyping) primarily through the use of iterative cycles within the overall life cycle phases.

2.8. Multiple Layers

The EPLC framework is intended to operate on many levels simultaneously. Two specific areas where this is true are among the various organizational levels within HHS and among the hierarchy of investments, projects and systems.

2.8.1. Department/OPDIV

The EPLC framework will apply to all levels of HHS and is compatible with current Department CPIC policy. As used in this document, "HHS" refers to both Department-wide and OPDIV levels unless otherwise noted. For those projects that are designated for OPDIV review, Project Managers and the OPDIV governance process will apply the EPLC framework. For those projects meeting threshold criteria for Department-level review, Project Managers and the Department-level governance process will apply the EPLC framework. The OPDIVs will establish IT Governance processes that are consistent with HHS CPIC policy and procedures, including the EPLC framework. The Department will generally focus on ensuring OPDIV processes are compliant rather than conducting direct reviews of OPDIV-level projects as a matter of course. However, the Department reserves the right to conduct project reviews of OPDIV-level projects when necessary to review process compliance or to otherwise fulfill its HHS IT project, investment, and portfolio management responsibilities.

2.8.2. Investment/Project/System

There is significant variation in designation of IT portfolios, investments, and projects. The EPLC framework should be considered a "nested" framework for purposes of this hierarchy. For example, a large investment may consist of several logically related projects. Project Managers are responsible to the Investment Manager for project compliance with the framework, and the Investment Manager is responsible to the IT Governance organization for overall investment compliance with the framework.

2.9. Stage Gate Reviews

Stage Gate Reviews are conducted by the IT Governance organization (in conjunction with project stakeholders) to ensure that projects, as they move through their life cycles, are fully complying with relevant IT project management requirements and other applicable Critical

Partner policies. The reviews also assess project performance against baselines and require corrective action plans or rebaselining as appropriate to the situation. Most importantly, Stage Gate Reviews determine that the project is ready to advance to the next Phase. Stage Gate Reviews are also the most appropriate time for the IT Governance organization, in consultation with affected Business Owners, to change project cost, schedule or performance baselines in response to changing HHS mission priorities.

2.10. EPLC Guidance and Support

Implementation of the EPLC framework will require significant training and guidance for the entire IT project stakeholder community. In addition to training programs, EPLC framework guidance and support will be provided via the following methods.

2.10.1. Web Sites

HHS has established an Internet Web site that contains the information described in the remainder of this subsection. It is located at http://www.hhs.gov/ocio/eplc/index.html.

2.10.2. Practices Guides

Practices Guides are brief documents describing the background, requirements, best practices, and key terminology of industry-leading project management practices and their accompanying project management templates.

2.10.3. Templates

Templates are standardized documents with a preset format. They are used as a starting point for framework deliverables to ensure quality and consistency. Templates are designed to be customized for the use of each project and include instructions and boiler plate text.

2.10.4. Checklists

Checklists are brief documents listing the items to be noted, checked, remembered and delivered when completing the accompanying template.

3. THE EPLC FRAMEWORK

This section presents a more detailed description of the EPLC framework life cycle phases along with the stakeholder responsibilities, activities, deliverables, exit criteria and Stage Gate Reviews required in each phase.

3.1. Initiation Phase

3.1.1. Description

During the Initiation Phase, a Business Owner identifies a business need for which a technological solution is required and a preliminary enterprise architecture review is conducted to determine if there is sufficient justification to proceed into the Concept Phase. The Initiation Phase may be triggered as a result of business process improvement activities, changes in business functions, advances in information technology, or may arise from external sources, such as public law or the general public. When an opportunity to improve business/mission accomplishments or to address a deficiency is identified, the Business Owner and the Project Manager (if already assigned) document these opportunities in the Business Needs Statement. Sufficient high-level functional requirements are required to understand what the project is intended to do and how it supports the business needs.

The Architecture Review examines whether the proposed project potentially duplicates, interferes, contradicts or can leverage another project that already exists, or is proposed, under development, or planned for near-term disposition.

3.1.2. Responsibilities

Business Owner: The Business Owner is the principal authority on matters regarding the expression of business needs, the interpretation of functional requirements language, and the mediation of issues regarding the priority, scope and domain of business requirements. The Business Owner must understand what constitutes a requirement and must take ownership of the initial and final business requirements. The Business Owner champions the proposed project to the IT Governance body to gain approval.

Critical Partners: Critical Partners review and comment on the Business Needs Statement.

- **Enterprise Architecture:** Validate alignment of the Business Need Statement with the Enterprise Architecture. Determine if the preliminary enterprise architecture review reveals any duplication or interferes, contradicts, or can leverage another existing or proposed project, if the project addresses compliance with HHS enterprise architecture goals, and if there is any impact on the Enterprise Architecture or the infrastructure.

- **Security:** Determine if the Business Needs Statement contains any potential information security concerns.

- **Budget:** Determine if the Business Needs Statement ensures that adequate financial resources are available.

- **CPIC:** Verify that the initial scope of the project will adequately address requirements specified in the Business Needs Statement.

- **Performance:** Ensure that Risk Tolerance levels are established.

3.1.3. Activities

Activities during the Initiation Phase are designed to determine whether or not the proposed project aligns with the mission of the organization, supports the achievement of a short term and/or long term goal(s), and justifies development of a full Business Case and preliminary Project Management Plan.

3.1.4. Deliverables

Business Needs Statement (Final)

A Business Needs Statement identifies the business need for a proposed investment or project. It includes a brief description of the proposed project's purpose, goals, and scope. The Business Needs Statement provides sufficient information to justify a decision whether or not the organization should move forward with the development of a full business case.

3.1.5. Exit Criteria

Objective: To determine if this project proposal is worth pursuing. [Is there a good chance that the project will be approved and funded? Does this project proposal warrant investing in the development of a business case and preliminary project management plan?]

Phase Specific Exit Criteria:

- A Business Owner has been identified and confirmed. [Someone who will champion the project, defines the business needs and project requirements, and secures funding].
- Approval of this project is highly probable. The decision is based on the following factors: acceptable risk/return; high-priority business need/mandate; and no more preferable alternative (use/modify existing application, not addressable through business process reengineering or other non-IT solution).
- Project description is sufficient to permit development of an acceptable business case and preliminary project management plan.

3.1.6. Project Review

The Architecture Review is performed to ensure that the Business Needs Statement is sound and is consistent with the Enterprise Architecture.

3.1.7. Stage Gate Review

The Initiation Stage Gate Review considers whether the Business Needs Statement justifies proceeding to the Concept Phase for a full Business Case and preliminary Project Management Plan.

3.2. Concept Phase

3.2.1. Description

The Concept Phase begins when the IT Governance organization approves the Business Needs Statement to enable a new business process or enhance an existing business process through the application of information technology. The purposes of the Concept Phase are to:

- Identify and validate an opportunity to improve business accomplishments of the organization or to correct a deficiency related to a business need.
- Identify significant assumptions and constraints on solutions relative to that need.
- Explore alternative concepts and methods to satisfy the need.

In the Concept Phase, sufficient requirements detail is developed to support the detailed cost and schedule estimates, alternatives analyses, and other elements of the Business Case and preliminary Project Management Plan. The primary outcome of the Concept Phase is the proposal and approval of a high level Rough Order of Magnitude..

3.2.2. Responsibilities

Business Owner: The Business Owner is responsible for ensuring that adequate financial and business process resources are made available to support the project once approved and selecting the Project Manager.

Project Manager: The Project Manager develops the Business Case and preliminary Project Management Plan.

Critical Partners: Critical Partners review and comment on the Business Case and participate in the Project Selection Review.

- **Enterprise Architecture:** Establish that the outcomes or results of executing the project are included in the Target Enterprise Architecture and that they are aligned to the HHS IT Strategic Plan. Ascertain that the Alternatives Analysis considers the use of existing systems and/or GOTS/COTS products. Verify that the business processes are modeled in sufficient detail.
- **Security:** Conclude that all applicable security and privacy standards have been considered in sufficient detail as part of the Business Case. Verify that:
    - the Project has been categorized correctly under FIPS 199 and NIST guidelines;
    - a System Accreditation Memorandum has been correctly initiated;
    - an Electronic Authentication Risk Assessment has been correctly performed in compliance with OMB and NIST guidelines;
    - a Privacy Threshold Analysis has been correctly performed so as to determine if a full PIA will be required to support the Project;
    - the Minimum Baseline Security Requirements (MBLSR) have been selected correctly from the NIST Security Controls Catalog; and
    - the Initial Security Risk Assessment Report has been completed in accordance with NIST guidelines.
- **Acquisition:** Ascertain if a preliminary Acquisition Strategy that is appropriate to the level of the requirements definition is part of the Business Case, and includes performance-based acquisitions. Verify that the overall acquisition strategy includes consideration of internal versus external acquisition, re-use, the use of commercial off-the-shelf technologies, 508 compliance and, if Requests for Information are necessary, how contracting work will be divided, and expected contract types.

- **Budget:** Establish that the Business Case includes a financing and budgeting plan and that there is sufficient requirements detail to support the detailed cost and schedule estimates needed during the Planning and Requirements Analysis Phases.
- **HR:** Determine the probability and/or impact of any anticipated workforce disruptions has been reviewed and make certain the need for staffing classifications such as new Position Descriptions, grade levels, etc., and potential workforce planning such as employee training or A-76 activities have been evaluated.
- **Section 508:** Make sure that plans are in place to incorporate Section 508 requirements in the contract(s).
- **CPIC:** Review the preliminary Project Management Plan and components to ensure that they are adequately developed. Conclude that the required authority and project structural foundation are in place.
- **Performance:** Ensure that the approval of the performance baselines is completed. Determine that appropriate potential performance goals are established as part of the Business Case. Conclude that the required authority and project structural foundation is in place.

IT Governance Organization: The IT Governance organization conducts the Project Selection Review.

3.2.3. Activities

The following activities are performed as part of the Concept Phase:

- Establish project sponsorship/ownership.
- Identify and establish the Business Case for the proposed project.
- Document the analysis and planning activities.
- Determine IPT staffing requirements for the project.
- Review and approve advancement to the next phase.

During the Concept Phase, the Project Manager creates a Project Charter to document the organizational roles and responsibilities, including designation of the proposed Integrated Project Team (IPT) to move the project forward. The Business Case should identify why a business capability is necessary and what business benefits can be expected by implementing this project. It is important to state the needs or opportunities in business terms. Avoid identifying a specific product or vendor as the solution. The background information provided should be at a level of detail sufficient to familiarize senior managers with the history, issues and customer service opportunities that can be realized through improvements to business processes with the potential support of IT. This background information must not offer or predetermine any specific automated solution, tool, or product.

The Concept Phase involves the appointment of a Project Manager who carries both the responsibility and accountability for project planning and execution. For smaller efforts, this may only involve assigning a project to a manager within an existing organization that already has an inherent support structure. For new projects entailing a significant impact on the organization, a completely new organizational element may be formed - requiring the hiring and reassignment of technical and business specialists.

The Project Manager will apply the EPLC framework and other processes and procedures for project activities. These include developing a preliminary Project Management Plan (PMP) that addresses project planning, requirements management, project tracking, contractor management, verification and validation, quality assurance, change management, and risk management.

During the Concept Phase, high-level analysis and preliminary risk assessment are performed on the proposed project to establish the business case for proceeding forward in the life cycle. The business process is modeled and possible business and technical alternatives are identified. High-level system requirements, high-level technical design concept/alternatives and cost estimates are prepared. The overall strategy for acquisition is developed, including consideration of internal versus external acquisition, whether Requests for Information are necessary, how work will be divided, and expected contract types.

The Concept Phase ends with a decision by the IT Governance organization of whether or not to approve commitment of the necessary resources to solve the business need.

3.2.4. Deliverables

Business Case with components (Final)

- Business Process Models (BPMs)
- Investment/Project (e.g., FIPS-199 categorization needed for information security)
- High-Level Requirements
- Preliminary Acquisition Strategy

The Business Case is a documented, structured proposal for business improvement that is prepared to facilitate a selection decision for a proposed investment or project by organizational decision makers. The Business Case describes the reasons and justification for the investment or project in terms of business process performance, needs and/or problems, and expected benefits. It identifies the high-level requirements that are to be satisfied, an analysis of proposed alternative solutions (with reasons for rejecting or carrying forward each option), assumptions, constraints, a risk-adjusted cost-benefit analysis, and preliminary acquisition strategy.

Project Charter (Final)

The Project Charter formally authorizes a project, describes the business need for the project and the product to be created by the project. It provides the project manager with the authority to apply up to a certain level of organizational resources to project activities.

Project Management Plan with components (Preliminary)

- Risk Management
- Acquisition Strategy
- Change Management
- Configuration Management
- Project Categorization
- Requirements Management

The Project Management Plan is a dynamic formal approved document that defines how the project is executed, monitored and controlled. It may be summary or detailed and may be composed of one or more subsidiary management plans and other planning documents. The main objective of the PMP is to document assumptions and decisions for how the project is to be managed, to help in communication between all of the concerned parties and to document the scope, costs and time sequencing of the project.

- Communications Plan
- Work Breakdown Structure (WBS) /Project Schedule
- IV&V Planning
- Quality Assurance
- Records Management
- Staffing Management
- Security Approach (a description of how security requirements will be addressed by the plan)

3.2.5. Exit Criteria

Objective: To determine if the project has been clearly defined and has the supporting organizational structure to proceed with full planning.

Phase Specific Exit Criteria:

- The scope of the project has been adequately described in the Business Case and that the high level requirements meet the business need.
- The project organizational structure is scaled to support the project and the project manager and the project team are qualified [Organizational Mappings support project communication needs.]
- The Project Charter adequately authorized the project to proceed based on the agreed upon project scope.
- The Preliminary Project Management Plan adequately defines how the project will be executed, monitored and controlled and includes high level estimates of the baselines.
- The high level analysis demonstrates that the outcomes will be aligned with the Target Enterprise Architecture.
- All applicable security and privacy standards have been considered in sufficient detail as part of the Business Case. FIPS-199 categorization and an initial assessment of system accreditation boundary are established.
- A Designated Approving Authority (DAA) has been identified.

3.2.6. Stage Gate Review

The Project Selection Review (PSR) is a formal inspection of a proposed IT project by the IT Governance organization to determine if it is a sound, viable, and worthy of funding, support and inclusion in the organization's IT Project Portfolio. This Stage Gate Review is one of the four that cannot be delegated by the IT Governance organization.

3.3. Planning Phase

3.3.1. Description

The Planning Phase begins when the project has been formally approved and funded, and the Project Charter is approved. This Phase requires study and analysis culminating in the full Project Management Plan and that may lead to system development activities.

If obtaining contractor support is necessary, perform acquisition activities. The project work is broken down into specific tasks and sub-tasks, including the identification of project deliverables and assignment of allocated resources to each task. Control documents relating to that effort are produced. The degree of project management rigor that is to be applied to the project is determined and milestones are established. Specific plans for management and governance of the project are established and documented to guide ongoing project execution and control. The Planning Phase ends with a formal review during which the adequacy of the Project Management Plan is determined.

In the planning phase, sufficient requirements detail is required to support the development of the project's Project Management Plan and permit outside validation of this deliverable.

3.3.2. Responsibilities

Business Owner: The Business Owner is responsible for authorizing and ensuring that the funding and resources are in place to support the project.

Project Manager: The Project Manager is responsible and accountable for the successful execution of the Planning Phase. The Project Manager is responsible for leading the Integrated Project Team that accomplishes the Phase activities and deliverables.

Integrated Project Team: The Integrated Project Team members (regardless of the organization of permanent assignment) are responsible for accomplishing assigned tasks as directed by the Project Manager.

Critical Partners: Critical Partners assess completeness of Planning Phase activities, robustness of the plans for the next life cycle phase, availability of resources to execute the next phase, and acceptability of the acquisition risk of entering the next phase. For applicable projects, this assessment also includes the readiness to award any major contracting efforts needed to execute the next phase.

- **Enterprise Architecture:** Conclude that compliance with Enterprise Architecture has been maintained.
- **Security:** Ensure that the Risk Management Plan accurately establishes that the security and privacy requirements have been identified and planned for. System Categorization, MBLSR, Initial System Security Plan, Risk Assessment, and preliminary IT Contingency Plans are reviewed and ready for approval by the DAA.
- **Acquisition:** Make certain that acquisition activities to obtain contractor support have been completed in compliance with the Project Management Plan. Confirm that detailed activities and timelines for preparing acquisition documents, selecting vendors, and awarding contracts are developed.
- **Budget:** Determine if there is a realistic budget to accomplish all planned work and that the Total Cost of Ownership has been evaluated.
- **Finance:** Ensure that planning for financial management issues has been properly addressed and that interactions with financial systems are planned in compliance with financial standards and regulations.
- **HR:** Determine if required staff development has been documented and planned.

- **Section 508:** Verify that Applicable Section 508 standards are identified and planned for and that the vulnerability and impact of being non compliant with Section 508 has been included in the overall risk management planning.
- **CPIC:** Determine if the project has been tailored and approvals for any alteration of deliverables and reviews have been obtained and the Project Management Plan components, including the Risk Management Plan) are fully developed.
- **Performance:** Ensure that business owner expected performance benefits are fully defined and that business product deliverables are well-planned.

IT Governance organization: During the Project Baseline Review, the IT Governance organization examines whether scope, cost and schedule that have been established for the project are adequately documented and that the project management strategy is appropriate for moving the project forward in the life cycle.

3.3.3. Activities

The following activities are performed as part of the Planning Phase. The results of these activities are captured in the Project Management Plan.

The Project Management Plan (PMP) is the primary managerial document in the life cycle of a project. The components of this document can be tailored to the particular project's circumstances and typically include new or updated plans based on standard plans for the system for:

- Risk Management
- Acquisition
- Change Management
- Configuration Management
- Project Categorization
- Requirements Management
- Communications
- Work Breakdown Structure/Project Schedule
- Independent Verification & Validation
- Quality Assurance
- Records Management
- Staffing Management
- Security Approach (a description of how security requirements will be addressed by the plan))

The Project Manager (PM) works with the Business Owner to verify the scope of the proposed program, participation of the key organizations, and potential individuals who can participate in the formal reviews of the project. This decision addresses both programmatic and information management-oriented participation as well as technical interests in the project that are known at this time.

The Project Manager plans the subsequent phases to allow development of the project schedule and budget requirements, and to define the expected performance benefits. The Project Manager also prepares a Project Process Agreement that specifies project deliverables and their expected levels of detail, and documents the justification for tailoring EPLC elements, if any. Detailed activities and timelines for preparing acquisition documents, selecting vendors, and awarding contracts are developed.

The Integrated Project Team identifies all alternatives that may address the need and any programmatic or technical risks. The risks associated with further development are also studied. (The results of these assessments are summarized in the Business Case and the Project Management Plan). To ensure that Privacy Act considerations are addressed early in the project life cycle, the Project Manager also prepares a Privacy Impact Assessment.

3.3.4. Deliverables

Project Management Plan (PMP) with components (Final)

- Risk Management
- Acquisition Strategy
- Change Management
- Configuration Management
- Project Categorization
- Requirements Management
- Communications Plan
- Work Breakdown Structure (WBS) /Project Schedule
- IV&V Planning
- Quality Assurance
- Records Management
- Staffing Management Plan
- Security Approach(a description of how security requirements will be addressed by the plan)

The Project Management Plan (PMP) is a dynamic formal approved document that defines how the project is executed, monitored and controlled. It may be summary or detailed and may be composed of one or more subsidiary management plans and other planning documents. The main objective of the PMP is to document assumptions and decisions for how the project is to be managed, to help in communication between all of the concerned parties and to document the scope, costs and time sequencing of the project.

Privacy Impact Assessment (PIA) (Final)

Based on the initial FIPS 199 categorization and the identification of the need or potential to collect Privacy Act data/information, the assessment required by the Privacy Act and/or E-Government Act of 2002 to conduct assessments on projects before developing or procuring information technology that collects, maintains, or disseminates personal information in identifiable form. A PIA is an agency review of how collected information is handled by and protected in a manner consistent with Federal standards for privacy and information security. The PIA determines what kind of information in identifiable form is contained within a system, what is done with that information, and how that information is protected. Though the PIA specifically refers to "privacy", a PIA also typically covers confidentiality, access to data, and use of data.

Project Process Agreement (PPA) (Final)

- Deliverable & Stage Gate Waivers
- Authorization to Proceed

The Project Process Agreement (PPA) is used to authorize and document the justifications for using, not using, or combining specific Stage Gate Reviews and the selection of specific deliverables applicable to the investment/project, including the expected level of detail to be provided.

3.3.5. Exit Criteria

Objective: To determine if the project has finalized project planning and defined initial baselines and requirements to permit outside validation.

Phase Specific Exit Criteria:

- The full scope of the project has been adequately described in the Business Case and the high level requirements meet the business need.
- 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.
- All Deliverables have been defined.
- The Acquisition Strategy has been approved by the Contracting Officer and there is obligated money for contract awards. All applicable contract clauses have been considered.
- The risk limits of the Business Owner have been defined and risks of highest impact have been sufficiently addressed with either mitigation or contingency plans.

3.3.6. Project Review

The Integrated Baseline Review (IBR) is an internal inspection led by the Integrated Project Team to verify that the project baseline is in place, together with a realistic budget to accomplish all planned work. The IBR includes an evaluation of the Performance Measurement Baseline for realism and inherent risks. When contractor resources are involved, the IBR provides a forum through which the government's team gains a sense of ownership and understanding of the contractor's management process and assurance that earned value management has been appropriately established for the project.

3.3.7. Stage Gate Review

The Project Baseline Review (PBR) is a formal inspection of the entire project and performance measurement baseline initially developed for the IT project. This review is one of the four Stage Gate Reviews that cannot be delegated by the IT Governance organization. The PBR is conducted to obtain management approval that the scope, cost and schedule that have been established for the project are adequately documented and that the project management strategy is appropriate for moving the project forward in the life cycle. Upon successful completion of this review, the Project Management Plan is officially baselined.

The PBR includes review of the budget, risk, and user requirements for the project. Emphasis should be on the total cost of ownership and not just development or acquisition costs.

3.4. Requirements Analysis Phase

3.4.1. Description

During the Requirements Analysis Phase, the business (project in-scope) requirements that were documented during the Concept Phase in an earlier phase are validated and further analyzed and decomposed into functional and non-functional requirements that define the Business Product in more detail with regard to inputs, processes, outputs, and interfaces. If appropriate, a logical depiction of the data entities, relationships and attributes of the system/application is also created. During the Requirements Analysis Phase, the initial strategy for testing and implementation should be considered. In addition, the work planned for future phases is redefined, if necessary, based on information acquired during the Requirements Analysis Phase. The Requirements Analysis Phase ends with a review to determine readiness to proceed to the Design Phase.

Detailed application requirements (both functional and non-functional) are required to permit detailed project management planning, execution and control. If detailed requirements and subsequent planning identify a breach of the project-level cost, schedule or performance baselines established at the end of the planning phase, a formal change to the Project Baselines should be requested.

3.4.2. Responsibilities

Business Owner: The Business Owner participates in the Requirements activities and may approve the final requirements.

End Users: The End Users participate in the development of detail of functional requirement and provide input into non-functional requirements.

Project Manager: The Project Manager is responsible and accountable for the successful planning and execution of the Requirements Analysis Phase. The Project Manager is responsible for leading the Integrated Project Team that accomplishes the Phase tasks and deliverables.

Integrated Project Team: The Integrated Project Team members (regardless of the organization of permanent assignment) are responsible for accomplishing assigned tasks as directed by the Project Manager.

Contracting Officer: The Contracting Officer is responsible and accountable for preparing solicitation documents under the guidance of the Project Manager.

Critical Partners: The Critical Partners provide oversight, advice and counsel to the Project Manager to ensure that the Requirements Document addresses relevant standards. Additionally, Critical Partners provide information, judgments, and recommendations during the Requirements Review.

- **Enterprise Architecture**: Find out if requirements provide a suitable basis for subsequent design activities and all service components have been appropriately identified. Determine if technologies and other requirements are consistent with the Enterprise Architecture. Identify relevant technical and/or service standards that will apply to or constrain solution design and development activities. Determine if the Requirements document contains a traceability matrix that is complete and plans are complete to track technical changes. Establish that the Business Process Models and Logical Data Models are documented at the proper level.

- **Security:** Ensure that an assessment of the required information security and privacy controls has been completed and determine if requirements reflect alignment with established information security standards including the FIPS-199 Categorization and that the Accreditation Boundary is established with all dependencies and relationships. Ensure the assessment of required security controls (per NIST guidelines) has been completed.
- **Acquisition**: Review acquisition strategy to ensure it includes necessary requirements analysis, alternatives analysis, and procurement and contract award plans. Ensure that there is sufficient information to make management decisions and evaluate vendor proposals.
- **Budget:** Ascertain if requirements are in accord with project-level cost baselines established at the end of the Planning Phase or a formal change to the Project Baselines has been requested.
- **Finance:** Determine if financial management requirements are in accordance with requirements established at the end of the Planning Phase or a formal change to the Project Baselines has been requested.
- **HR:** By reviewing an update of the Project Management Plan, ascertain if staffing and organizational requirements have been fully documented.
- **Section 508:** Make certain that the requirements for applicable Section 508 standards have been identified.
- **CPIC:** Confirm the requirements document contains a traceability matrix, business process model and logical data model.
- **Performance:** Determine if the requirements are in accordance with project-level performance baselines established at the end of the Planning Phase or a formal change to the Project Baselines has been requested.

3.4.3. Activities

The tasks described below are performed during the Requirements Analysis Phase:

- Requirements elicitation is done during sessions with the end users.
- Business needs are consolidated and affirmed. The functional requirements and the data requirements are then consolidated. The functional requirements are connected to the data requirements.
- The Requirements Document (RD) is a record of the above requirements. This can be established as a matrix and tracked for satisfaction of every module of the system as development progresses.

- Documentation from prior phases may need to be revised or updated.
- The following activities are performed as part of the Requirements Analysis Phase. The results of these activities are captured in the Acquisition Strategy, which also requires additional items not covered by this list:
  - Requirements Analysis
  - Analysis of Alternatives
  - Procurement of Government Human Resources and Services
  - Acquisition Strategy
  - Acquisition of Contractor Services if required
  - Solicitation of Services
  - Technical Evaluation Report
  - Source Selection Recommendation
  - Contract Award
  - Adjustment of Funds
  - Contract Performance
- The Acquisition Strategy should provide adequate information to enable the following actions:
  - Making management decisions concerning procurement of government human resources and services Memorandum of Understanding (MOU) and Service Level Agreement (SLAs) and contractor services procurement, including ensuring the availability of funding.
  - Performing a technical analysis and evaluation of vendor proposals.
  - Vendors' bid preparation.
  - The Source Selection Official to base a selection.

The Acquisition Strategy becomes critical after the Requirements Document has been approved. Several acquisitions may be needed to procure an entire system and are a continuous part of the life cycle. The Acquisition Strategy is continuously updated with the active involvement of the Investment Manager and Contracting Officer.

3.4.4. Deliverables

Requirements Document with components (Final)

- Functional & Non-Functional Requirements
- Requirements Traceability Matrix (RTM)
- Business Process Model

The Requirements Document describes both the project and product requirements. It outlines the technical, functional, performance and other requirements necessary to deliver the end business product.

(BPM) Expansion

- Logical Data Model

3.4.5. Exit Criteria

Objective: To determine if the project requirements have been defined sufficiently to be translated into the Business Product.

Phase Specific Exit Criteria:

- The initial Test Plan is defined.
- Requirements have been grouped and sufficiently detailed so that they can be tested once the product is developed.
- Process and Data Models are defined adequately for product design.

Generic Exit Criteria:

- Variances from baselines have been identified and mitigated. [Cost and schedule variances and scope changes are identified, significant variances are explained, and Corrective Action Plans (CAPs) or rebaseline requests are in place as appropriate.]
- Project Baselines have been reviewed and revised as appropriate. [Should this project continue as-is, be modified, or be terminated based on current knowledge?]
- The Project Management Plan and component plans have been reviewed and appropriately updated. [This includes Risk Management, Acquisition Strategy, Change Management, Configuration Management, Project Categorization, Requirements Management, Communication Plan, WBS/Schedule, IV&V Planning, Quality Assurance, Records Management, Staffing Management Plan and Security Approach.]

3.4.6. Project Review

The Requirements Review is conducted to verify that the requirements are complete, accurate, consistent and problem-free; to evaluate the responsiveness of the requirements to the business requirements; to ensure that the requirements are a suitable basis for subsequent design activities; to ensure traceability within the requirements and between the design documents; and to affirm final agreement regarding the content of the Requirements Document. Upon successful completion of this review, the Requirements Document is baselined.

3.4.7. Stage Gate Review

The Requirements Analysis Stage Gate Review considers whether the project should proceed to the Design Phase.

3.5. Design Phase

3.5.1. Description

The Design Phase seeks to develop detailed specifications that emphasize the physical solution to the end user's information technology needs. The system requirements and logical description of the entities, relationships, and attributes of the data that were documented during the Requirements Analysis Phase are further refined and allocated into system and database design specifications that are organized in a way suitable for implementation within the constraints of a physical environment (e.g., computer, database, facilities).

A formal review of the high-level architectural design is conducted prior to detailed design of the Business Product to achieve confidence that the design satisfies the system requirements, is in conformance with the enterprise architecture and prescribed design standards, to raise and resolve any critical technical and/or project-related issues, and to identify and mitigate project, technical, security, and/or business risks affecting continued detailed design and subsequent life cycle activities. During the Design Phase, the initial strategy for any necessary training is also begun. Estimates of project expenses are updated to reflect actual costs and estimates for future phases. In addition, the work planned for future phases is redefined, if necessary, based on information acquired during the Design Phase.

For COTS products, some tasks and activities may have been performed by the vendor and vendor documentation may be appropriate to meet some documentation requirements. This is acceptable as long as each required activity is performed and each required deliverable is available.

3.5.2. Responsibilities

Business Owner: The Business Owner may participate in the Preliminary Design Review.

Project Manager: The Project Manager is responsible and accountable for the successful execution of the Design Phase. The Project Manager is responsible for leading the team that accomplishes the phase activities and deliverables.

Integrated Project Team: The Integrated Project Team members (regardless of the organization of permanent assignment) are responsible for accomplishing assigned tasks as directed by the Project Manager.

Contracting Officer: The Contracting Officer is responsible and accountable for preparing solicitation documents under the guidance of the Project Manager.

Critical Partners: The Critical Partners participate in a Design Review to ensure compliance with policies in their respective areas and to make any necessary tradeoff decisions if conflicting goals have arisen during the Design.

- **Enterprise Architecture:** Conduct a formal review of the high-level architectural design to achieve confidence that the design satisfies the system requirements, is in conformance with the Enterprise Architecture and prescribed design standards.
- **Security:** Establish that Information security documents (C&A, Privacy Impact Assessment, System of Record Notice, and Computer Match Agreement) are reviewed for completeness and accuracy and that Contingency/Disaster Recovery Plan includes complete procedures, arrangements and responsibilities. Verify that project information security risks are identified and mitigation plans are made and documented.
- **Acquisition:** Verify that contracts are being fulfilled according to award or approved changes.
- **Budget:** Guarantee that the budget is sufficient to meet the needs of the project. Determine if project business risks are identified and mitigation plans are made.
- **Finance:** Guarantee that estimates of project expenses have been updated to reflect actual costs and estimates for future phases. Determine if project business risks are identified and mitigation plans are made.

- **HR:** Confirm that issues related to staffing, workforce, or other HR areas have been addressed.
- **Section 508:** Establish that any new or further requirements that have been discovered that are necessary to accommodate individuals with disabilities have been added to the Requirements Document and the Design documents. Confirm that there are test cases which incorporate Section 508 standards.
- **CPIC:** Make sure that the Design is fully documented.
- **Performance:** Determine if project technical risks are identified and mitigation plans are made. Verify that performance goals are agreed upon.

IT Governance Organization: The IT Governance organization conducts the Preliminary Design Review to achieve agreement and confidence that the design satisfies the functional and non-functional requirements and is in conformance with the enterprise architecture.

3.5.3. Activities

The following tasks are performed during the Design Phase.

The Design Document is developed by the Project Manager and Integrated Project Team, identifying the steps used in the design of the Business Product. The prerequisites for this phase are the Business Case, Project Management Plan, and Requirements Document. The Project Manager and Integrated Project Team identify/specify the desired environments (design, development, test, and operations). The business organization, roles and procedures for designing this system/application are articulated. The Design Document is a deliverable of the Design Phase. Documents from the previous phases are revised as necessary during the Design Phase.

In the system design, first the general system characteristics are defined. The data storage and access for the database layer are designed. The user interface at the desktop layer is designed. The business rules layer or the application logic is designed. The interfaces from application to application and application to database also are designed and documented.

Based on the Privacy Impact Assessment, developed during the Planning Phase, a System of Record Notice (SORN) is prepared, if required, to inform the public of any information collection by the Business Product about citizens. A Computer Match Agreement (CMA) is also prepared, if needed, to establish the conditions, safeguards, and procedures under which HHS agrees to disclose data where there is a computerized comparison of two or more automated System of Records (SORs).

A Contingency/Disaster Recovery Plan is developed containing emergency response procedures; backup arrangements, procedures and responsibilities; and post-disaster recovery procedures and responsibilities. It is included in this phase because many of these factors will affect the design of the system. During the Design Phase, a final draft Test Plan is also prepared. The Test Plan describes the test cases and test environment specifications, and includes a Requirements Traceability Matrix that maps requirements to the specific tests to be conducted in the Test Phase. This final draft Test Plan will be used in the Development Phase to test components as they are built and integrated.

The end user community is included in Design Phase actions as needed. New or further requirements might be discovered that are necessary to accommodate individuals with disabilities. If so, these requirements are added to the RD and the design documents.

3.5.4. Deliverables

Design Document with components (Architectural & detailed elements) (Final)

- Physical Data Model (database design)
- Release Strategy
- Data Conversion
- Interface Control
- Section 508 Compliance
- Capacity /Implementation Planning
- Updated RTM

The Design Document describes the technical solution that satisfies the requirements for the Business Product (e.g., system). Either directly or by reference to other documents, the Design Document provides a high-level overview of the entire solution architecture and data design, including external interfaces, as well as lower-level detailed design specifications for internal components of the Business Product that are to be developed.

Computer Match Agreement (CMA) (Final)

A Computer Match Agreement CMA is a written accord that establishes the conditions, safeguards, and procedures under which a Federal organization agrees to disclose data where there is a computerized comparison of two or more automated System of Records (SORs). In conjunction with a CMA, an Inter/Intra-agency Agreement (IA) is also prepared when the SOR(s) involved in the comparison are the responsibility of another Federal agency.

Test Plan (Final Draft)

- **Test Case Specification**

The Test Plan defines the types of tests (e.g. unit, function, integration, system, information security, performance (load and stress), regression, user acceptance, and/or independent verification and validation) to be carried out. The document describes the acceptance criteria for those tests, roles and responsibilities of individuals involved in the testing process, traceability matrix, resources required (hardware and software environments), and other elements relevant to test planning and execution. This plan details the manner of testing (test cases, simulation, etc) of the integrated Business Product system. It must include as part of the main document or as a separate document detailed Test Case Specifications that describe the purpose and manner of each specific test, the required inputs and expected results for the test, step-by-step procedures for executing the test, and the pass/fail criteria for determining acceptance.

Contingency/Disaster Recovery Plan (Final Draft)

The Contingency/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 plan describes the strategy for ensuring recovery of the business product in accordance with stated recovery time and recovery point objectives.

System of Record Notice (SORN) (Final Draft)

The Privacy Act defines a System of Record (SOR) as a group of any records under the control of a Federal agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Additionally, the Privacy Act requires that the Federal government inform the public of any collection of information about its citizens from which data are retrieved by a unique identifier as described above. The System of Record Notice (SORN) fulfills this requirement to inform the public via the publication of a system notice in the Federal Register. This notice describes the SOR and gives the public an opportunity to comment. Without the written consent of the subject individual, the Privacy Act prohibits the release of protected information maintained in a SOR unless one of the 12 defined disclosure exceptions is applicable.

3.5.5. Exit Criteria

Objective: To determine if the design process will create a Business Product that meets the requirements within a specified project budget and schedule.

Phase Specific Exit Criteria:

- No significant outstanding concerns among stakeholders regarding design adequacy or feasibility.
- Design is adequately documented to allow effective and efficient development.
- Contingency/Disaster Recovery plans are adequately documented to provide clear procedures and responsibilities
- Security Documents are as complete and accurate as possible.

Generic Exit Criteria:

- Variances from baselines have been identified and mitigated. [Cost and schedule variances and scope changes are identified, significant variances are explained, and Corrective Action Plans (CAPs) or rebaseline requests are in place as appropriate.]
- Project Baselines have been reviewed and revised as appropriate. [Should this project continue as-is, be modified, or be terminated based on current knowledge?]
- The Project Management Plan and component plans have been reviewed and appropriately updated. [This includes Risk Management, Acquisition Strategy, Change Management, Configuration Management, Project Categorization, Requirements Management, Communication Plan, WBS/Schedule, IV&V Planning, Quality Assurance, Records Management, Staffing Management Plan and Security Approach.]

3.5.6. Project Review

The Detailed Design Review (DDR) is conducted subsequent to a PDR to achieve confidence that the individual design components (units/modules) of an automated system/application, and how they interface with one another, have been completely defined and documented in sufficient detail such that the design of the Business Product is complete, fully integrated, and ready to move to the Development Phase. Upon successful completion of this review, the Design Document and other adjunct documents are baselined.

The DDR should identify and resolve open issues regarding any of the following:

- The system-wide or subsystem-wide design decisions.
- The architectural design of a Business Product system or subsystem.
- The Business Product design decisions.
- The architectural design of a Business Product item.
- The detailed design of a Business Product item or portion thereof (such as a database).

3.5.7. Stage Gate Review

The Preliminary Design Review (PDR) is a formal inspection of the high-level architectural design of an automated system, its software and external interfaces, which is conducted to achieve agreement and confidence that the design satisfies the functional and non-functional requirements and is in conformance with the enterprise architecture. Overall project status, proposed technical solutions, evolving software products, associated documentation, and capacity estimates are reviewed to determine completeness and consistency with design standards, to raise and resolve any technical and/or project-related issues, and to identify and mitigate project, technical, information security, and/or business risks affecting continued detailed design and subsequent development, testing, implementation, and operations & maintenance activities. This review is one of the four Stage Gate Reviews that cannot be delegated by the IT Governance organization.

3.6. Development Phase

3.6.1. Description

During the Development Phase, the system developer takes the detailed design information documented in the previous phase and transforms it into machine-executable form, and ensures that all of the individual components of the Business Product function correctly and interface properly with other components within the system/application. As necessary and appropriate, system hardware, networking and telecommunications equipment, and COTS/GOTS software is acquired and configured. New custom-software programs are developed, database(s) are built, and software components (COTS, GOTS, and custom-developed software and databases) are integrated. Test data and test case specifications are finalized. Unit and integration testing is performed by the developer with test results appropriately documented. Data conversion and training plans are finalized and user procedures are baselined, while operations, office and maintenance procedures are also initially developed. The Development Phase ends with a Stage Gate Review to determine readiness to proceed to the Test Phase.

3.6.2. Responsibilities

Project Manager: The Project Manager is responsible and accountable for the successful execution of the Development Phase. The Project Manager is responsible for leading the Integrated Project Team that accomplishes the Development Phase activities and deliverables.

Integrated Project Team: The Integrated Project Team members (regardless of the organization of permanent assignment) are responsible for accomplishing assigned tasks as directed by the Project Manager.

Development Team: Technical personnel that execute projects are expected to follow the EPLC framework and be integral partners in the HHS project management process.

Critical Partners: The Critical Partners provide oversight, advice and counsel to the Project Manager on the conduct and requirements of the Development Phase.

- **Enterprise Architecture:** Determine if approved change requests are compliant with the Enterprise Architecture Technical Reference Model and do not negatively impact any dependencies on other systems.
- **Security**: Make sure that all development plans address safety, information security, and privacy concerns. Validate that the test plan includes explicit testing of information security controls and functional capabilities. Confirm that the Systems Security Plan and the Security Risk Assessment address all required topics and that an IV&V Assessment has been conducted.
- **Acquisition**: Conclude that contracts are being fulfilled according to award or approved changes and required assets (e.g., system hardware, COTS/GOTS software) have been acquired according to regulations.
- **Budget:** Verify that the budget is sufficient to meet the needs of the project and project business risks are identified and mitigation plans are made.
- **Finance:** Verify that actual expenses are in accordance with the budget plan.
- **HR:** Ensure that issues related to staffing, workforce, or other HR areas have been addressed.
- **Section 508**: Establish that requirements identified for Section 508 compliance are incorporated into the system.
- **CPIC:** Ensure that EVM is being reported accurately and is within acceptable limits or CAP is in place for remediation.
- **Performance:** Make sure the Business Product covering the requirements is ready for integration and formal testing. Confirm that Test Plans are complete.

3.6.3. Activities

The Development Phase includes several activities that are the responsibility of the developer. The developer places the outputs under configuration control and performs change control. The developer also documents and resolves problems and non-conformances found in the Business Product and tasks.

The developer selects, tailors, and uses those standards, methods, tools, and computer programming languages that are documented, appropriate, and established by the organization for performing the activities in the Development Phase.

Plans for conducting the activities of the Development Phase are developed, documented and executed. The plans include specific standards, methods, tools, actions, and responsibility associated with the development and qualification of all requirements including safety and information security. Separate plans may be developed.

Verify that the Business Product covering the documented and baselined requirements in is a sufficient state of readiness for integration and formal testing by an assigned test group (i.e. other than development personnel).

During the Development Phase, the final Test Plan is prepared. In addition, final drafts of the following project deliverables are developed:

- Business Product
- Operations and Maintenance (O&M) Manual, describing the Business Product, operating environment, production processing requirements, ongoing maintenance activities, and problem tracking and change management procedures.
- Systems Security Plan, addressing system managerial, technical, and operational information security controls
- Security Risk Assessment, documenting the analysis of information security functional requirements, threat impacts, and system protection requirements.
- Training Plan, describing overall goals and learning objectives; activities to develop, conduct, control, and evaluate training; and staff resource requirements.
- Training Materials, comprising all artifacts used to train system end users, such as instructor and student guides, audio and visual aids, computer-based and other media.
- User Manual, explaining how a business user operates the system.

3.6.4. Deliverables

Test Plan (Final)

- Test Case Specification

The Test Plan defines the types of tests (e.g. unit, function, integration, system, information security, performance (load and stress), regression, user acceptance, and/or independent verification and validation) to be carried out. The document describes the acceptance criteria for those tests, roles and responsibilities of individuals involved in the testing process, traceability matrix, resources required (hardware and software environments), and other elements relevant to test planning and execution. This plan details the manner of testing (test cases, simulation, etc) of the integrated software/hardware system. It must include as part of the main document or as a separate document detailed Test Case Specifications that describe the purpose and manner of each specific test, the required inputs and expected results for the test, step-by-step procedures for executing the test, and the pass/fail criteria for determining acceptance.

Operation & Maintenance

The Operations & Maintenance Manual clearly describes the

Manual (Final Draft)

- Help Desk Support

Business Product that will be operating in the production environment and provides the operations and support staff with the information necessary to effectively handle routine production processing, ongoing maintenance, and identified problems, issues, and/or change requests.

Systems Security Plan (SSP) (Final Draft)

The SSP describes managerial, technical and operational security controls (defined by the National Institute of Standards and Technology) that are designed and implemented within the system.

Training Plan (Final Draft)

The Training Plan describes the overall goals, learning objectives, and activities that are to be performed to develop, conduct, control, and evaluate instructions that are to be provided to end users, operators, administrators, and support staff who will use, operate, and/or otherwise support the solution.

Training Materials (Final Draft)

Training Materials include the documentation associated with the deployment of the Business Product. This includes instructor and student guides, audio-visual aids, and computer-based or other media used to disseminate information about the final product to the target audience that is in need of the instruction.

Security Risk Assessment (SRA) (Final Draft)

A Security Risk Assessment will document the analysis of the information security functional requirements and will identify the protection requirements for the system using a formal risk assessment process. The risk assessment includes the identification of threats to and vulnerabilities in the information system; the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on agency assets or operations and the identification and analysis of information security controls for the information system.

User Manual (Final Draft)

The User Manual clearly explains how a business user is to use the established Business Product from a business function perspective.

Business Product (Final Draft)

- Version Description Document

The Business Product is the primary result from the development effort that satisfies the established requirements. In software development efforts, it includes the original source code and machine-compiled, executable computer instructions and data repository (ies). It also includes an identification and description of all configuration items that comprise a specific build or release of the Business Product.

3.6.5. Exit Criteria

Objective: To determine if the code and/or other deliverables needed to build the Business Product have been completed within cost, schedule, and scope guidelines.

Phase Specific Exit Criteria:

- Business Product satisfies the requirements established and refined during the Requirements and Design Phases.
- Test Plan ensures that all test cases will be adequately evaluated and executed, and system tested to ensure requirements are met.
- Information Security plans and risk assessments are complete and in compliance with regulatory requirements.

Generic Exit Criteria:

- Variances from baselines have been identified and mitigated. [Cost and schedule variances and scope changes are identified, significant variances are explained, and Corrective Action Plans (CAPs) or rebaseline requests are in place as appropriate.]
- Project Baselines have been reviewed and revised as appropriate. [Should this project continue as-is, be modified, or be terminated based on current knowledge?]
- The Project Management Plan and component plans have been reviewed and appropriately updated. [This includes Risk Management, Acquisition Strategy, Change Management, Configuration Management, Project Categorization, Requirements Management, Communication Plan, WBS/Schedule, IV&V Planning, Quality Assurance, Records Management, Staffing Management Plan and Security Approach.]

3.6.6. Project Reviews

Two project reviews will be conducted during the Development Phase.

The first is the Validation Readiness Review (VRR). The VRR is conducted to provide assurance that the Business Product that is about to enter validation (system) testing has completed thorough unit/module/software integration testing during the development of the Business Product and is ready for turnover to the formal, controlled test environment where validation testing will be conducted. The scope of the VRR is to inspect the test products and test results obtained during development testing for completeness and accuracy, and to verify that test planning, test cases, scenarios, and scripts provide adequate coverage of documented system requirements. In addition, a review of the test environment, test setup, and test data is performed to ensure they are adequately prepared for validation testing.

The second review is the Independent Verification & Validation Assessment. An IV&V Assessment is conducted by an independent third party to identify potential improvements that may not be apparent to those working directly on a project, or identify problems before they occur and thus avoid loss and minimize the cost of any necessary corrective action. IV&V Assessment also provides management with an independent perspective on the full scope of project activities, from planning through implementation.

3.6.7. Stage Gate Review

The Development Stage Gate Review evaluates whether the project should proceed to the Test Phase.

3.7. Test Phase

3.7.1. Description

The primary purpose of the Test Phase is to determine whether the Business Product developed or acquired and preliminarily tested during the Development Phase is ready for implementation. During the Test Phase, formally controlled and focused testing is performed to uncover errors and bugs in the Business Product that need to be resolved. There are a number of specific validation tests that are performed during the Test Phase (e.g., requirements validation, system integration, interface, regression, information security, performance, stress, usability, and user acceptance). Additional tests may be conducted to validate documentation, training, contingency plans, disaster recovery, and installation depending upon the specific circumstances of the project. The Test Phase ends with a review to determine readiness to proceed to the Implementation Phase.

3.7.2. Responsibilities

Business Owner: The primary customer who is responsible for ensuring that business needs and performance measures are satisfied by reviewing test results.

Project Manager: The Project Manager is responsible and accountable for the successful execution of the Test Phase. The Project Manager is responsible for leading the Integrated Project Team that accomplishes the Test Phase activities and deliverables.

Integrated Project Team: The integrated project team members (regardless of the organization of permanent assignment) are responsible for accomplishing assigned testing tasks as directed by the Project Manager.

Test and Evaluation Team: The Test and Evaluation Team is responsible for Business Product testing and documentation of test results.

End Users: Selected end users may be required to participate in testing, including user acceptance testing.

Critical Partners: The Critical Partners review test procedures and outcomes in their areas.

- **Security:** Check that the validation tests confirm the information security of the Business Product. When required, validate penetration tests and vulnerability scans are executed, documented, and any failed components are documented, and either mitigated and/or accepted as residual risk by the appropriate authority.. Ensure that all high impact risks are documented and mitigated prior to entering the implementation phase.
- **Acquisition:** Determine if changes are reviewed to determine if any contract modifications are necessary.
- **Finance:** Conclude that Changes are reviewed to determine the financial impact.
- **Section 508:** Verify that test plan results for Section 508 testing are satisfactory.
- **CPIC:** Determine if the Implementation Plan has a reasonable schedule.
- **Performance:** Determine if Measurement indicators support the performance measures agreed upon and validation tests confirm the performance measures. Ensure that system functionality is performing as stated and is able to achieve performance goals.

3.7.3. Activities

The following tasks are completed during the Test Phase:

- The Project Manager, in conjunction with the Business Owner and CIO, is responsible for establishing the test team and creating the Test Files/Data.
- The test and evaluation team is responsible for creating/loading the test database(s) and executing the system test(s). All results are documented in the Test Reports. Any failed components are migrated back to the Development Phase for rework, and the passed components migrated ahead for information security testing.
- The test and evaluation team create or load the test database(s) and execute information security test(s). All tests are documented, similar to those above. Failed components are migrated back to the Development Phase for rework, and passed components will be migrated ahead for acceptance testing.
- The test and evaluation team create/load the test database(s) and execute the acceptance test(s). All tests are documented similar to those above. Failed components are migrated back to the Development Phase for rework, and passed components migrate ahead for implementation.
- During this phase, the documentation from all previous phases is finalized to align it with the delivered system. The Project Manager coordinates these update activities.
- Determine whether or not the tested product is ready for production.

During the Test Phase, the project team also develops the final version of the Implementation Plan that describes how the business product will be installed, deployed, and transitioned to the operational environment.

3.7.4. Deliverables

Implementation Plan (Final) The Implementation Plan describes how the business product will be installed, deployed, and transitioned into the operational environment.

Test Reports (Final) Test Reports are completed at the end of each test to verify expected results. A summary report should be created at the end of the testing phases to document the overall test results. These reports summarize the testing activities that were performed and describe any variances between the expected test results and the actual test results and includes identification of unexpected problems and/or defects that were encountered.

3.7.5. Exit Criteria

Objective: To determine if the test processes have been executed according to plan and whether the tests verify that the implementation of the Business Product will be successful.

Phase Specific Exit Criteria:

- Test plan ensures that test cases will be executed to make certain that requirements are met.
- Testing of the Business Product supported the decision to move to the Implementation Phase.
- Implementation Plan provided detailed information on the move of the Business Product into production.

Generic Exit Criteria:

- Variances from baselines have been identified and mitigated. [Cost and schedule variances and scope changes are identified, significant variances are explained, and Corrective Action Plans (CAPs) or rebaseline requests are in place as appropriate.]
- Project Baselines have been reviewed and revised as appropriate. [Should this project continue as-is, be modified, or be terminated based on current knowledge?]
- The Project Management Plan and component plans have been reviewed and appropriately updated. [This includes Risk Management, Acquisition Strategy, Change Management, Configuration Management, Project Categorization, Requirements Management, Communication Plan, WBS/Schedule, IV&V Planning, Quality Assurance, Records Management, Staffing Management Plan and Security Approach.]

3.7.6. Project Review

The Implementation Readiness Review (IRR) is conducted at the end of the Test Phase. The IRR is conducted to ensure that the Business Product that has been developed is ready for implementation activities, such that the required system hardware, networking and telecommunications equipment; COTS, GOTS, and/or custom-developed software; and database(s) can be installed and configured in the production environment(s).

3.7.7. Stage Gate Review

The Test Stage Gate Review evaluates whether the project should proceed to the Implementation Phase.

3.8. Implementation Phase

3.8.1. Description

During the Implementation Phase, the Business Product is moved from development status to production status. The process of implementation is dependent on the characteristics of the project and the Business Product, and thus may be synonymous with installation, deployment, rollout, or go-live. If necessary, data conversion, phased implementation, and training for using, operating, and maintaining the system are accomplished during the Implementation Phase. The final system must be certified and accredited before use in the production environment during the Implementation Phase. The Implementation Phase ends with a formal decision to release the final Business Product into the Operations and Maintenance Phase.

3.8.2. Responsibilities

Business Owner: This is the executive in charge of the organization, who serves as the primary customer and advocate for an IT project. The business owner is responsible for certifying that the performance of the new it project moved into the production environment meets business requirements.

End Users: End users begin utilizing the new IT projects on a daily basis. They may also funnel improvement requests to the IPT for future releases.

Project Manager: The Project Manager is responsible and accountable for the successful execution of the Implementation Phase. The Project Manager is responsible for leading the Integrated Project Team that accomplishes the Implementation Phase activities and deliverables.

Integrated Project Team: The Integrated Project Team members (regardless of the organization of permanent assignment) are responsible for accomplishing assigned tasks as directed by the Project Manager.

Critical Partners: The Critical Partners provide oversight, advice and counsel to the Project Manager on the conduct and requirements of the Implementation Phase. Additionally, they provide information, judgments, and recommendations to the Business Owner and IT Governance organization during project reviews and in support of Project Baselines.

- **Enterprise Architecture:** Confirm that approved change requests are compliant with the Enterprise Architecture.
- **Security:** Determine if Plan of Actions and Milestones (POA&M), the Authority to Operate, including the System Certification and Accreditation, is complete and System of Record Notice is published.
- **Acquisition:** Guarantee that the contracts are being fulfilled according to award or approved changes and completed contracts are closed appropriately.
- **Budget:** Ascertain if change requests are reviewed to determine if a new financial analysis is required.
- **Finance:** Ascertain if actual expenses are in accordance with the budget plan.
- **HR**: Find if issues related to staffing, workforce, or other HR areas have been addressed.
- **Section 508:** Establish that implementation has maintained the integrity of Section 508 compliance.
- **CPIC:** Confirm that the project is still within the original scope and that current Implementation Plan is reasonable.
- **Performance:** Confirm that the completed Business Product is operating as expected and is positioned to meet performance targets.

IT Governance Organization: The IT Governance organization conducts the Operational Readiness Review.

3.8.3. Activities

The following activities are performed as part of the Implementation Phase.

All affected end users and organizations affected are notified of the implementation. Additionally, it is good policy to make internal organizations not directly affected by the implementation aware of the schedule so that allowances can be made for a disruption in the normal activities of that section. The notification should include:

- The schedule of the implementation

- A brief synopsis of the benefits of the new system
- The difference between the old and new system
- Guidelines for the end user affected by the implementation during this phase
- The process to obtain system support, including contact names and phone numbers

Typically, implementation includes converting existing data for use in the new system. The tasks for this effort are two-fold: data input and data verification. When replacing a manual system, hard copy data is entered into the automated system. Some sort of verification that the data is being entered correctly should be conducted throughout this process. This is also the case in data transfer, where data fields in the old system may have been entered inconsistently and therefore affect the integrity of the new database. Verification of the old data becomes imperative to a useful computer system.

One of the ways verification of both system operation and data integrity can be accomplished is through parallel operations. Parallel operations consist of running the old process or system and the new system simultaneously until the new system is certified. In this way if the new system fails in any way, the operation can proceed on the old system while the bugs are worked out.

To ensure that the system is fully operational, install the system in a production environment.

During this phase, the documentation from all previous phases is finalized to align it with the delivered system. The Project Manager coordinates these update activities.

Prior to the Operational Readiness Review, the Authority to Operate must be obtained and a System of Record Notice published.

Final versions of the following documents are prepared during the Implementation Phase, and are required before the project proceeds to the Operations and Maintenance Phase:

- Business Product
- Project Completion Report
- Service Level Agreements (SLAs) and Memoranda of Understanding (MOU)
- Contingency/Disaster Recovery Plan
- Operations and Maintenance (O&M) Manual
- Systems Security Plan
- Security Risk Assessment
- Training Plan
- Training Materials
- User Manual

3.8.4. Deliverables

Authority to Operate (ATO) with components (Final)

- Security Certification & Accreditation Letters
- Section 508 Product Certifications/Exceptions

An Authority to Operate (ATO) is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of a Business Product and explicitly accepts the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of information security controls. Though not security-specific, formal documentation of Section 508 Certification or Exception is also required before a Business Product can be released into operation.

System of Record Notice (SORN) (Final)

The Privacy Act defines a System of Record (SOR) as a group of any records under the control of a Federal agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Additionally, the Privacy Act requires that the Federal government inform the public of any collection of information about its citizens from which data are retrieved by a unique identifier as described above. The System of Record Notice (SORN) fulfills this requirement to inform the public via the publication of a system notice in the Federal Register. This notice describes the SOR and gives the public an opportunity to comment. Without the written consent of the subject individual, the Privacy Act prohibits the release of protected information maintained in a SOR unless one of the 12 defined disclosure exceptions is applicable.

Service Level Agreement(s) (SLAs) and/or Memorandum(s) of Understanding (MOU)

A Service Level Agreement(s) (SLAs) is a contractual agreement between a 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 each parties requirements, responsibilities and period of performance.

Operation & Maintenance Manual (Final)

- **Help Desk Support**

The Operations & Maintenance Manual clearly describes the Business Product that will be operating in the production environment and provides the operations and support staff with the information necessary to effectively handle routine production processing, ongoing maintenance, and identified problems, issues, and/or change requests.

Systems Security Plan (SSP) (Final)

The SSP describes managerial, technical and operational security controls (defined by the National Institute of Standards and Technology) that are designed and implemented within the system.

Training Plan (Final)

The Training Plan describes the overall goals, learning objectives, and activities that are to be performed to develop, conduct, control, and evaluate instructions that are to be provided to end users, operators, administrators, and support staff who will use, operate, and/or otherwise support the solution.

Training Materials (Final)

Training Materials include the documentation associated with the deployment of the Business Product. This includes instructor and student guides, audio-visual aids, and computer-based or other media used to disseminate information about the final product to the target audience that is in need of the instruction.

Security Risk Assessment (SRA) (Final)

A Security Risk Assessment will document the analysis of the information security functional requirements and will identify the protection requirements for the system using a formal risk assessment process. The risk assessment includes the identification of threats to and vulnerabilities in the information system; the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on agency assets or operations and the identification and analysis of information security controls for the information system.

User Manual (Final)

The User Manual clearly explains how a business user is to use the established Business Product from a business function perspective.

Business Product (Final)

- Version Description Document

The Business Product is the primary result from the development effort that satisfies the established requirements. In software development efforts, it includes the original source code and machine-compiled, executable computer instructions and data repository(ies). It also includes an identification and description of all configuration items that comprise a specific build or release of the Business Product.

Project Completion Report (Final)

- Closeout Certification
- Lessons Learned

The Project Completion Report describes any differences between proposed and actual accomplishments, documents lessons learned, provides a status of funds, and provides an explanation of any open-ended action items, along with a certification of conditional or final closeout of the development project.

Contingency/Disaster Recovery Plan (Final)

The Contingency/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 plan describes the strategy for ensuring recovery of the business product in accordance with stated recovery time and recovery point objectives.

Plan of Action and Milestones (POA&M)

A management process that outlines weaknesses and delineates the tasks necessary to mitigate them. The HHS Information Security Program POA&M process will be used to facilitate the remediation of information security program- and system-level weaknesses, and will provide a means for:

- Planning and monitoring corrective actions;
- Defining roles and responsibilities for weakness resolution;
- Assisting in identifying the information security funding requirements necessary to mitigate weaknesses;
- Tracking and prioritizing resources; and
- Informing decision makers.

Privacy Impact Assessment

A PIA is an agency review of how collected information is handled by and protected in a manner consistent with Federal standards for privacy and information security. The PIA determines what kind of information in identifiable form is contained within a system, what is done with that information, and how that information is protected. Though the PIA specifically refers to "privacy", a PIA also typically covers confidentiality, access to data, and use of data.

3.8.5. Exit Criteria

Objective: To verify the operational readiness of the Business Product for release into the production environment

Phase Specific Exit Criteria:

- Business Product ready for production service and notification of the new solution is provided to all end users and staff who are affected.
- No significant outstanding concerns among stakeholders regarding implementation.
- All certification and accreditation documents are complete and accurate, and conform to NIST requirements and HHS standards. This ensures that the certification and accreditation letters are signed and that all POA&M items are up to date.

Generic Exit Criteria:

- Variances from baselines have been identified and mitigated. [Cost and schedule variances and scope changes are identified, significant variances are explained, and Corrective Action Plans (CAPs) or rebaseline requests are in place as appropriate.]
- Project Baselines have been reviewed and revised as appropriate. [Should this project continue as-is, be modified, or be terminated based on current knowledge?]
- The Project Management Plan and component plans have been reviewed and appropriately updated. [This includes Risk Management, Acquisition Strategy, Change Management, Configuration Management, Project Categorization, Requirements

Management, Communication Plan, WBS/Schedule, IV&V Planning, Quality Assurance, Records Management, Staffing Management Plan and Security Approach.]

3.8.6. Project Reviews

Three project reviews are required during the Implementation Phase.

The first is System Certification. System Certification is the comprehensive evaluation of the management, operational, and technical information security controls implemented for an information system to ensure compliance with information security requirements. The certification evaluation includes review of the Information Security Risk Assessment (IS RA), System Security Plan (SSP), other system life cycle documentation, and any findings from past assessments, reviews and/or audits, as well as technical testing and analysis. The technical certification assessment, called the Security Test and Evaluation (ST&E) process, is the execution of test procedures and techniques by an independent third party designed to evaluate the effectiveness of information security controls in a particular environment, and to identify any vulnerabilities in the information system. The results of the certification assessment, together with a review of any other independent audits, reviews or assessments are documented and appropriate corrective action is taken to strengthen internal controls. The SSP and/or IS RA are then updated based upon improvements and changes made to the system, and then the system is certified (approved) prior to subsequent System Accreditation (i.e., authorization to process) by the organization's Designated Approval Authority.

The second review is the System Accreditation. System Accreditation is the official management decision to authorize operation of an information system. To make an informed decision, the organization's Designated Approval Authority (DAA) must have sufficient knowledge and understanding of the current status of the information security programs and information security controls in place to protect the system and information processed, stored, or transmitted by the system. This is a business-driven, risk-based decision founded upon current, credible, comprehensive documentation and test results provided in the System Certification package prepared as a result of predecessor System Certification activities. The organization's DAA must explicitly accept or reject any identified residual risks to the organization's operations and assets remaining after the implementation of the prescribed set of information security controls as documented in the SSP and/or IS RA. Ultimately, the DAA must strike a firm balance between authorizing the operation of information systems necessary to support completion of the business mission, while ensuring that an adequate level of information security is in place. The objective is to strive to implement the most effective information security controls, in consideration of technical, budgetary, time, and resource limitations, while continuing to support business mission requirements.

The third review is the Post-Implementation Review (PIR). After a period of sustained operation (after at least one full processing and reporting cycle has been completed and all end users have been trained and are comfortable with the operation), a PIR is conducted on the completed Business Product that was released into the production environment to determine if it is operating as expected. The purpose of the review is to ascertain the degree of success from the project (in particular, the extent to which it met its objectives, delivered planned levels of benefit, and addressed the specific requirements as originally defined), to examine the efficacy of all elements of the working business solution to see if further improvements can be made to optimize the benefit delivered, and to learn lessons from the project that can be used to improve future project work and solutions.

3.8.7. Stage Gate Review

The Operational Readiness Review (ORR) is a formal inspection conducted to determine if the final Business Product that has been developed or acquired, tested, and implemented is ready for release into the production environment for sustained operations and maintenance support. The IT Governance organization cannot delegate this review.

3.9. Operations and Maintenance Phase

3.9.1. Description

During the Operations & Maintenance (O&M) Phase, the certified and accredited Business Product operates in full-scale production environment for sustained use and operations/maintenance support. Changes and problems with the Business Product may continually be identified and resolved to ensure that the Business Product solution meets ongoing functional and non-functional needs. POA&M's are resolved during this phase. Periodically the Business Product will also need to be re-certified and re-accredited for continued operation in the production environment. When the time comes that the Business Product will no longer be needed or will be replaced, then a plan for final disposition of the Business Product must be prepared and approved prior to moving into the Disposition Phase.

3.9.2. Responsibilities

Project Manager: The Project Manager develops, documents, and executes plans and procedures for conducting activities and tasks of the Operations and Maintenance Phase. To provide for an avenue of problem reporting and customer satisfaction, the Project Manager should create and discuss communications instructions with the Business Product's customers. Project Managers should keep Help Desk personnel informed of all changes to the Business Product, especially those requiring new instructions to end users. The Project Manager should finalize and close-out all POA&Ms and develop a new POA&M that is documented and tracked.

Technical Support: Personnel who provide technical support to the Business Product. This support may involve granting and terminating access rights to the program as authorized by the Project Manager or authorized designee, setup of workstations or terminals to access the system, and maintenance of the operating system for both server and workstation. Technical support personnel may be involved with issuing user IDs or login names and passwords. In a client-server environment, technical support may perform systems scheduled backups and operating system maintenance during downtime.

Vendor Support: The technical support and maintenance on some programs are provided through vendor support. A contract is established outlining the contracted systems administration, operators, and maintenance personnel duties and responsibilities. One responsibility which should be included in the contract is that all changes to the system will be thoroughly documented.

Help Desk: Help Desk personnel provide the day-to-day end users help for the Business Product. Help desk personnel should be kept informed of all changes or modifications to the Business Product. Help Desk personnel are contacted by the end users when questions or problems occur with the daily operations of the system. Help Desk personnel need to maintain a level of proficiency with the Business Product.

Operations or Operators (turn on/off systems, start tasks, backup etc): For many mainframe systems, an operator provides technical support for a program. The operator performs scheduled backup, performs maintenance during downtime and is responsible to ensure the system is online and available for end users. Operators may be involved with issuing user IDs or login names and passwords for the system.

Customers/End Users: The customer needs to be able to share with the project manager the need for improvements or the existence of problems. Some end users live with a situation or problem because they feel they must. Customers may feel that change will be slow or disruptive. Some feel the need to create work-arounds. A customer has the responsibility to report problems, make recommendations for changes to a system, and contribute to Operational Analyses.

Program Analysts or Programmer: Interprets user requirements, designs and writes the code for specialized programs. User changes, improvements, enhancements may be discussed in Joint Application Design sessions. Analyzes programs for errors, debugs the program and tests program design.

Change Control Board: A board of individuals may be convened to approve recommendations for changes and improvements to the Business Product. This group may be chartered. The charter should outline what should be brought before the group for consideration and approval. The board may issue a Change Directive.

Users Group or Team: A group of computer users who share knowledge they have gained concerning a program or system. They usually meet to exchange information, share programs and can provide expert knowledge for a system under consideration for change.

Contract Manager: The Contract Manager has many responsibilities when a contract has been awarded for maintenance of a program. The Contract Manager should have a certificate of training for completion of a Contracting Officer's Technical Representative (COTR) course. The Contract Manager's main role is to make sure that the interests of the Contracting Office are protected and that no modifications are made to the contract without permission from the Contracting Office.

Data Administrator: Performs tasks which ensure that accurate and valid data are entered into the Business Product. Sometimes this person creates the information systems database, maintains the database's information security and develops plans for disaster recovery. The data administrator may be called upon to create queries and reports for a variety of user requests. The data administrator's responsibilities include maintaining the database's data dictionary. The data dictionary provides a description of each field in the database, the field characteristics and what data is maintained with the field.

Telecommunications Analyst and Network System Analyst: Plans, installs, configures, upgrades, and maintains networks as needed. If the project requires it, they ensure that external communications and connectivity are available.

Information Systems Security Officer (ISSO): The ISSO has a requirement to review system change requests, review and in some cases coordinate the Change Impact Assessments, participate in the Change Control Board process, and conduct and report changes that may be made that affect the information security posture of the system.

Critical Partners: The Critical Partners provide oversight, advice and counsel to the Project Manager during the Operations and Maintenance Phase.

- **Enterprise Architecture:** Confirm that the business product is being operated in accord with Enterprise Architecture guidelines.
- **Security**: Determine if the Authority to Operate, System Certification and Accreditation and Privacy Impact Assessments are reviewed and updated at the appropriate times for continued operation. Ensure that Information Security documents are updated as necessary in response to continuous testing and monitoring. Confirm that system backups, physical security, contingency planning, and continuous security monitoring and testing are operated in accord with established information security controls.
- **Acquisition:** Guarantee that contracts are being fulfilled according to award or approved changes.
- **Budget:** Determine if modification requests include appropriate justification and cost benefit analysis.
- **Finance:** Ascertain if actual expenses are in accordance with the budget plan.
- **HR:** Verify that issues related to staffing, workforce, or other HR areas have been addressed.
- **Section 508**: Ascertain that ongoing change requests incorporate requirements for Section 508.
- **CPIC**: Ensure that Operational Analysis is within acceptable limits.
- **Performance:** Confirm service level objectives are being met and that performance measurements and system logs are being maintained. Determine that modifications needed to resolve errors or performance problems are made in accord with change control procedures. Ensure that annual Operational Analysis is performed to evaluate system performance and user satisfaction to verify that risk and performance goals are under control.

3.9.3. Activities

Operations support is an integral part of the day-to-day operation of a system. In small systems, all or part of each task may be done by the same person. But in large systems, each function may be done by separate individuals or even separate areas. The O&M Manual was completed in the Implementation Phase. This document defines tasks, activities, and responsible parties and needs to be updated as changes occur. Systems operations activities and tasks need to be scheduled, on a recurring basis, to ensure that the production environment is fully functional and is performing as specified. The following is a checklist of systems operations key tasks and activities:

- Ensure that systems and networks are performing at agreed upon levels and are available during the defined hours of operation.

- Implement non-emergency requests during scheduled outages, as prescribed in the O&M Manual.
- Ensure all processes, manual and automated, are documented in the operating procedures. These processes should comply with the system documentation.
- Acquisition and storage of supplies, e.g., paper, toner, tapes, removable disks.
- Perform and test backups (day-to-day protection, contingency, and recovery).
- Perform the physical information security functions including ensuring adequate uninterruptible power supply and ensuring that personnel have proper clearances and proper access privileges, etc.
- Ensure contingency planning for disaster recovery is current, tested, and funded.
- Ensure end users are trained on current processes and new processes. Provide periodic refresher training and ensure funding.
- Ensure that service level objectives are kept accurate and are monitored.
- Maintain performance measurements, statistics, and system logs. Examples of performance measures include volume and frequency of data to be processed in each mode, order and type of operations.
- Monitor information security controls and performance statistics, report the results, and escalate problems when they occur. On an ongoing basis validate that reporting for security incidents are detected and that they are resolved in compliance with HHS policies and procedures.

Data/software administration is needed to ensure that input data and output data and databases are correct and continually checked for accuracy and completeness. This includes ensuring that any regularly scheduled jobs are submitted and completed correctly. Software and databases should be maintained at (or near) the current maintenance level. The backup and recovery processes for databases are normally different than the day-to-day data/software administration volume backups. The backup and recovery process of the databases should be performed as a data/software administration task. A checklist of data/software administration tasks and activities includes the following:

- Performing production control and quality control functions (job submission, checking and corrections).
- Interfacing with other functional areas for day-to-day checking/corrections.
- Installing, configuring, upgrading and maintaining database(s). This includes updating processes, data flows, and objects (usually shown in diagrams).
- Developing and performing data/database backup and recovery routines for data integrity and recoverability.
- Ensuring all processes are documented properly in the Operations and Maintenance Manual.
- Developing and maintaining a performance and tuning plan for online process and databases.

- Performing configuration, information security and design reviews/audits to ensure software, system, parameter, and configuration are correct.
- Perform patching of software for the system.
- Manage and control configuration and changes to the system.

One fact of life with any system is that change is inevitable. End Users need an avenue to suggest changes and identify problems. A User Satisfaction Review which can include a Customer Satisfaction Survey can be designed and distributed to obtain feedback on operational systems to help determine if the systems are accurate and reliable**.** Systems administrators and operators need to be able to make recommendations for upgrades to hardware, architecture and streamlining processes. For small in-house systems, modification requests can be handled by an in-house process. For large integrated systems, modification requests may be addressed in the Requirements Document and may take the form of a change package and may require justification and cost benefits analysis for approval by a review board. The Requirements Document for the project may call for a modification cut-off and rollout of the system as a first version and all subsequent changes addressed as a new or enhanced version of the system. A request for modifications to a system may also generate a new project and require a new project initiation plan.

Daily operations of the system/software may necessitate that maintenance personnel identify potential modifications needed to ensure that the system continues to operate as intended and produces quality data. Daily maintenance activities for the system must take place to ensure that any previously undetected errors are fixed. Maintenance personnel may determine that modifications to the system and databases are needed to resolve errors or performance problems. Also, modifications may be needed to provide new capabilities or to take advantage of hardware upgrades or new releases of system software and application software used to operate the system. New capabilities may take the form of routine maintenance or may constitute enhancements to the system or database as a response to user requests for new/improved capabilities. New capability needs may begin a new problem modification process described above.

Completed POA&M items should be closed and outstanding POA&M items should be updated to reflect progress made towards addressing them.. Throughout the phase, continuous information security monitoring of selected controls must be conducted. In addition, periodic reviews of controls, periodic re-evaluation of information categorization and re-certifications and revision of risk assessments and information security plans, and re-certification and re-authorizations to process (re-accreditation) are conducted as required. Because systems undergo periodic maintenance, enhancements and improvement, mini life cycles may be required throughout this stage. Continuous vigilance should be given to virus and intruder detection. The Project Manager must be sure that information security operating procedures are kept updated accordingly.

Review and update system documentation including the operations from the previous phases. In particular, the Operations Manual, Business Case Analysis, and Contingency/Disaster Recovery Plan (including results of tests during this phase) need to be updated as required and finalized during the O&M Phase. Reporting of information security incidents related to the system is also conducted during this phase.

An Authority to Operate may be granted for a period of time equal to or less than three years, but a full C&A to assure that risks are assessed and the approving authority explicitly identifies risks to HHS operations, assets and individuals, must be done before a new Authority to Operate can be granted. Please refer to appropriate NIST and HHS policies for annual and ongoing security reviews requirements.

Business Product changes may also create new privacy risks. For such changes, OMB requires that Privacy Impact Assessments (PIAs) are performed and updated as necessary to reflect new or changed information collection authorities, business processes, or other factors affecting the collection and handling of information in identifiable form

Inevitably, changes in requirements and technology will necessitate the replacement of IT systems. To facilitate that transition, a Disposition Plan is prepared to describe how the retirement of the system will be conducted and how records management will be addressed for both the system documentation and the Business Product.

3.9.4. Deliverables

Annual Operational Analysis (AOA) (Final)

The Annual Operational Analysis (AOA) combines elements from the CPIC evaluation and results from monitoring the performance of the Business Product during normal operations against original user requirements and any newly implemented requirements or changes. This document assists in the analysis of alternatives for deciding on new functional enhancements and/or modifications to the business product, or the need to dispose of or replace the business product altogether.

Disposition Plan (Final)

- Records Management

The Disposition Plan addresses how the various components of an operating Business Product (e.g., system) are to be handled at the completion of operations to ensure proper disposition of all the Business Product components and to avoid disruption of the individuals and/or any other Business Products impacted by the disposition. Includes the planning for the deliberate and systematic decommissioning of the asset with appropriate consideration of records management.

Plan of Action and Milestones (POA&M)

A management process that outlines weaknesses and delineates the tasks necessary to mitigate them. The HHS Information Security Program POA&M process will be used to facilitate the remediation of information security program- and system-level weaknesses, and will provide a means for:

- Planning and monitoring corrective actions;
- Defining roles and responsibilities for weakness resolution;
- Assisting in identifying the information security funding requirements necessary to mitigate weaknesses;
- Tracking and prioritizing resources; and
- Informing decision makers.

Privacy Impact Assessment	A PIA is an agency review of how collected information is handled by and protected in a manner consistent with Federal standards for privacy and information security. The PIA determines what kind of information in identifiable form is contained within a system, what is done with that information, and how that information is protected. Though the PIA specifically refers to "privacy", a PIA also typically covers confidentiality, access to data, and use of data.

3.9.5. Exit Criteria

Objective: To verify that the Business Product is managed and supported in a robust production environment and to determine whether the Business Product is still cost-effective to operate or if it should be retired.

Phase Specific Exit Criteria:

- Annual review of the operation provides a framework for deciding what enhancements or modifications are needed or whether the business product should be replaced or disposed of.
- Business Product documentation and the training programs should include input from stakeholders.

Generic Exit Criteria:

- Variances from baselines have been identified and mitigated. [Cost and schedule variances and scope changes are identified, significant variances are explained, and Corrective Action Plans (CAPs) or rebaseline requests are in place as appropriate.]
- Investment baselines have been reviewed and revised as appropriate. [Should this investment continue as-is, be modified, or be terminated based on current knowledge?]
- The Project Management Plan and component plans have been reviewed and appropriately updated. [This includes Risk Management, Acquisition Strategy, Change Management, Configuration Management, Project Categorization, Requirements Management, Communication Plan, WBS/Schedule, IV&V Planning, Quality Assurance, Records Management, Staff Development Plan and Security Approach.]

3.9.6. Project Reviews

Three periodic project reviews and one special review are conducted in the Operations and Maintenance Phase.

The first review is the annual System Re-Certification. System Re-Certification is the comprehensive re-evaluation of the management, operational, and technical information security controls implemented for an information system that is performed during the Operations & Maintenance Phase to ensure that the system is continuing to operate at an acceptable risk level. Over the life of the system, many changes occur that may reduce the effectiveness of internal information security controls. Information Security controls typically become outdated and less effective as threats and vulnerabilities evolve. The objective of the System Re-Certification is to ensure that system certification is an on-going process, and that information security is managed throughout the life of the system.

The second review is the periodic System Re-Accreditation. System Re-Accreditation is the official management decision to authorize continued operation of an information system after acceptable System Re-Certification and any necessary adjustments have been completed.

The third review is the annual Operational Analysis. The Operational Analysis is performed to evaluate system performance, user satisfaction with the system, adaptability to changing business needs, and new technologies that might improve the system. This review is diagnostic in nature and can lead to development or maintenance activities. Any major system modifications needed after the system has been implemented follow the EPLC framework life cycle process from planning through implementation. The Operational Analysis ultimately determines whether the IT Project should continue, or be modified or terminated.

A Disposition Plan should be developed and reviewed by the project team should the Operational Analysis conclude that the project should be terminated. The Disposition Plan should include a detailed plan with checklist, dependencies, and timing of activities for both contract closeout and administrative closeout.

3.9.7. Stage Gate Review

The Operations & Maintenance Stage Gate Review evaluates whether the project should proceed to the Disposition Phase.

3.10. Disposition Phase

3.10.1. Description

During the Disposition Phase, the operation of a Business Product is formally ended in accordance with organization needs and pertinent laws and regulations. The Business Product is retired or disposed of based on the formal Disposition Plan approved during the Operations & Maintenance Phase. The disposition activities ensure the orderly termination of the Business Product and preserve vital information about the system so that some or all of the information may be reactivated in the future if necessary. Particular emphasis is given to proper preservation of the data processed by the Business Product, so that the data is effectively migrated to another Business Product or archived in accordance with applicable records management regulations and policies for potential future access.

3.10.2. Responsibilities

Business Owner: The primary customer and advocate for an IT project. The Business Owner is responsible for identifying the business needs and certifying that the current Business Product no longer meets business requirements and may be orderly shutdown according to the disposition plan developed.

Project Manager: Authors the Disposition Plan and ensures that all aspects of the Disposition Plan are followed. The Disposition Plan should outline all roles and responsibilities for all actions related to the close down and archive of the system.

Technical Support or Vendor Support: The Disposition Plan may call for the Technical Support Personnel to send system related hardware to a warehouse or may reassign equipment to a new or replacement Business Product. Technical Support Personnel or Operators may perform the cutoff of end users' access per instructions from the Security Manager. Technical Support personnel may assist with the archive of the Information Systems data.

Data Administrator: The Disposition Plan may direct that only certain Business Product data be archived. The Data Administrator would identify the data and assist technical personnel with the actual archive process. The Data Administrator may be involved with identifying data which due to its sensitive nature must be destroyed. They would also be involved with identifying and migrating data to a new or replacement Business Product.

End User Services (Training & Help Desk): End User Services includes training, telecommunications, and Help Desk personnel. The training component coordinates and schedules the development and delivery of all training and facilitates the development of systems training methods and materials. In this phase, End User Services may assist with the retraining of end users to facilitate the transfer to a new or replacement Business Product.

Operations: (turn off systems, start tasks, backup, etc.) Operations interfaces with the computer facility that hosts the Business Product being terminated. This group also schedules, executes, and verifies production job streams; distributes specified outputs; handles other production control activities; and maintains and monitors centralized mainframe database management system software and runtime environments. It also acquires, maintains, customizes and tunes operating system software, assesses the affect of new or changed systems upon the operational environments, manages system software capacities, and advises on or arranges accommodation of new Business Product. In this phase, the Operators would assist Technical Support, Security Manager and Data Administrators with the actual archive process.

Security Managers: The Security Managers need to make sure that all access authority has been eliminated for the end users. Any end users that only use the Business Product should be removed from the system while others that use other Business Product as well as this one may still need access to the overall system, but not the Business Product being shutdown. If there is another Business Product that is taking the place of this Business Product, the Security Managers should coordinate with the new Security Managers.

Critical Partners: The Critical Partners handle transition reviews in their areas.

- **Enterprise Architecture:** Make certain that the system is marked as decommissioned in the Enterprise Architecture and that any dependencies or relationships to the expired system are redirected or similarly expired if no replacement capability exists. Perform impact analysis to determine what changes need to be made to the architecture as a result of the disposition. This includes impact to any dependent systems.
- **Security:** Guarantee that access authorities are removed, that data is properly migrated, and that all hardware and data storage devices have been sanitized to ensure no sensitive data is compromised.
- **Acquisition:** Verify that completed contracts are closed appropriately.
- **Budget:** Ascertain that the financial implications of the transition are reviewed for budget impacts.
- **Finance:** Make certain that final payments to contractors are made; project financial information/status is updated accordingly.
- **HR:** Verify that workforce information is updated, and staff re-assignments are executed.

- **CPIC:** Establish that Lessons Learned have been prepared so that other HHS projects can benefit from them. Ensure that all documentation is complete and archived.

3.10.3. Activities

The tasks and activities required are dependent on the nature of the project. The retirement activities are performed at the end of the project life cycle.

The Disposition Plan must be developed and implemented. The Disposition Plan identifies:

- How the retirement of the Business Product/data will be conducted and when.
- The Business Product retirement date.
- Business Product components to be preserved.
- Data to be preserved.
- Retirement of remaining equipment.
- Archiving of life cycle products.

Project Archives include the system data, software, and documentation designated for archiving in the Disposition Plan. The data from the old system are migrated into the new system or archived.

Similar to the data that is archived or transferred, the software components will need to be transferred to the new system, or if that is not feasible, dispose of appropriately.

The documentation that resulted from the development of the Business Product needs to be archived, where it can be referenced, if needed, at a later date.

Follow the plan in the Disposition Plan for the orderly breakdown of the Business Product, its components and the data within.

If the equipment can be used elsewhere in the organization, it should be recycled. If it is obsolete, notify the property management office to excess all hardware components.

3.10.4. Deliverables

Project Archives (Final)	Project Archives preserve vital information, including both documentation of project execution and the data from the production Business Product.

3.10.5. Exit Criteria

Objective: To have an orderly shutdown of the Business Product operation.

Phase Specific Exit Criteria:

- Data archiving, information security, and data and systems migrations are complete.
- If appropriate, has the migration of data and the function to a new system been well-planned.
- Final phase-end review has been conducted.

3.10.6. Stage Gate Review

A Disposition Review is conducted to ensure that Business Product has been completely and appropriately disposed, thereby ending the life cycle of the IT project.

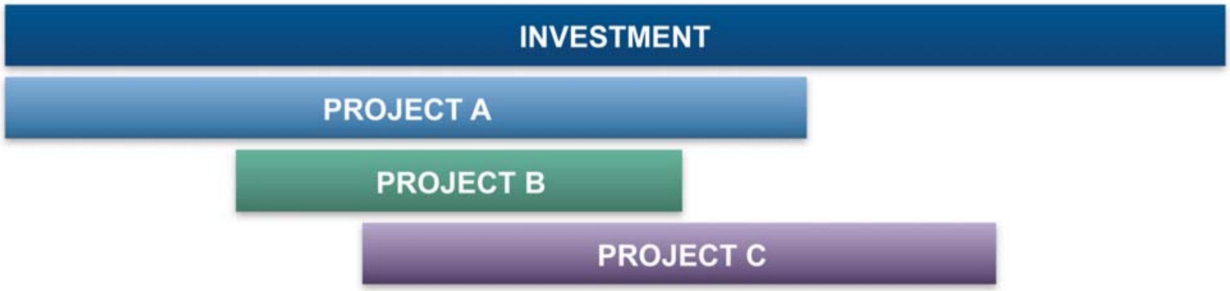
This phase-end review shall be conducted again within six months after retirement of the Business Product. The Disposition Review Report also documents the lessons learned from the shutdown and archiving of the terminated Business Product.

4. INVESTMENTS COMPOSED OF MULTIPLE PROJECTS

Section 3 of this document assumed that an investment consisted of a single project. In that case, the Project Manager could be the Investment Manager and the Project/Investment Manager is directly responsible to the Business Owner and the IT Governance organization for the performance of the project/ investment. The IT Governance organization acts as the independent oversight authority over the project/ investment.

It is sometimes necessary to divide a single large investment into multiple related projects, as depicted in Figure 7.

Figure 7 - IT Investments and IT Projects



When that is necessary, Project Managers will be assigned to the individual projects and they will be responsible to the Investment Manager for all aspects of the EPLC for that project.   As described in HHS Performance Baseline Management Policy (PBM), an IT investment may consist of a single IT project or may be made up of multiple IT projects.

Per HHS PBM policy, when an IT Investment consists of more than one IT project, the IT Investment Manager develops a customized investment-level management plan, patterned after the EPLC framework to define the life cycle cost, schedule, and scope baselines, and phases of investment-level activities and reviews that are appropriate to the overall investment and to integrate the cost, schedule, and scope baselines and different life cycle phases and deployments of the different projects that comprise the IT Investment.   For IT Investments consisting of multiple IT projects, the IT Investment manager develops an IT Investment performance measurement baseline that reflects the interdependencies and integration of the constituent IT projects, particularly with respect to cost, schedule, scope and risk.

Although investments may have IT projects that are in different life cycle phases at any one time (e.g., one project may be in development as another enters planning), the Investment Manager should consider each IT project as a unique effort and have the Project Manager of each project develop a specific project-level management plan that defines life cycle cost, schedule and performance baselines, phases and Stage Gate Reviews that are appropriate to the specific IT Project. Investment Managers should use tailoring techniques to establish the specific phases and artifacts that are needed for their IT project.

When the IT investment consists of multiple projects, full life-cycle cost and schedule information are captured at the IT project level and rolled up to the parent IT

Investment level to express an investment-level view that integrates the status of the subordinate IT projects.

The IT Governance organization must approve the project-level baselines (cost, schedule and performance), and the EPLC life cycle phases, activities, deliverables and Stage Gate Reviews appropriate to adequate oversight of the overall investment, taking into consideration the project-level activities that are planned.

APPENDIX A: ACRONYMS AND DEFINITIONS INDEX

The table below is a cross referenced list of acronym definitions used in the EPLC Overview Document.

Acronym	Term	See Glossary	See Deliverables
AOA	Annual Operational Analysis		**x**
ATO	Authority to Operate		**x**
BNS	Business Needs Statement		**x**
C&A	Certification & Accreditation	**x**	
CIO	Chief Information Officer	**x**	
CMA	Computer Match Agreement		**x**
CO	Contracting Officer	**x**	
COTS	Commercial Off-the-Shelf	**x**	
CPIC	Capital Planning and Investment Control	**x**	
DUA	Data Use Agreement		**x**
EA	Enterprise Architecture	**x**	
EPLC	Enterprise Performance Life Cycle	**x**	
EVM	Earned Value Management	**x**	
GOTS	Government Off-the-Shelf	**x**	
IM	Investment Manager	**x**	
IPT	Integrated Project Team	**x**	
IT	Information Technology	**x**	
ITIRB	Information Technology Investment Review Board	**x**	
IV&V	Independent Verification & Validation	**x**	
MOU	Memorandum of Understanding		**x**
NDA	Non-Disclosure Agreement		**x**
PBM	Performance Baseline Management	**x**	
PIA	Privacy Impact Assessment		**x**
PM	Project Manager	**x**	
PMP	Project Management Plan		**x**
POA&M	Plan of Action and Milestones		**x**
PPA	Project Process Agreement		**x**
ROM	Rough Order of Magnitude	**x**	
RTM	Requirements Traceability Matrix		**x**
SLA	Service Level Agreement(s)		**x**

Acronym	Term	See Glossary	See Deliverables
SOR	System of Record	**x**	
SORN	System of Record Notice		**x**

APPENDIX B: GLOSSARY

The table below is a glossary of terms used in the EPLC Overview Document.

Application
The use of information resources (information and information technology) to satisfy a specific set of user requirements (OMB A-130, App. III). In particular, an application is usually considered to be the software component of a system. An application runs on, and may or may not be part of, a general support system. The terms “application” and “information system” are sometimes used interchangeably although the latter has a broader definition to include general support systems.

Baseline
Baselines are the standard against which actual work is measured. Baselines are used in the annual report to Congress required by Federal Acquisition Streamlining Act Title V on variances of 10 percent or more from cost and schedule goals and any deviation from performance (scope) goals. Baseline cost and schedule goals should be realistic projections of total cost, total time to complete the project, and interim cost and schedule goals. Performance (scope) goals should be realistic assessments of what the investment or project is intended to accomplish, expressed in quantitative terms, if possible.

Business Owner
The executive in charge of the organization, who serves as the primary customer and advocate for an IT project. The Business Owner is responsible for identifying the business needs and performance measures to be satisfied by an IT project; providing funding for the IT project; establishing and approving changes to cost, schedule and performance goals; and validating that the IT project initially meets business requirements and continues to meet business requirements.

Capital Planning and Investment Control (CPIC)
The CPIC process is an integrated, structured methodology to managing IT investments, which ensures that IT investments align with HHS’ mission and support business needs while minimizing risks and maximizing returns throughout the investment’s life cycle. CPIC uses a systematic selection, control, and continual evaluation process to ensure that an investment supports HHS’ mission and business needs.

Certification & Accreditation (C&A)
C&A is composed of those activities and processes required to maintain security of information systems, periodically review the information security controls, and maintain the certification and authorization of the information system to operate. This process includes activities involved in the information security planning and security testing certification and authorization processes. The C&A phase of the information security process is where the system staff (outlined in the information security documentation) performs the day-to-day functions required to maintain an appropriate level of information security to protect the system. This phase is ongoing while the system is in operation.

Chief Information Officer (CIO)

The Office of the Chief Information Officer advises the Secretary and the Assistant Secretary for Resources and Technology (ASRT) on matters pertaining to the use of information and related technologies to accomplish Departmental goals and program objectives. The mission of the Office is to establish and provide: Assistance and guidance on the use of technology-supported business process reengineering; investment analysis; performance measurement; strategic development and application of information systems and infrastructure; policies to provide improved management of information resources and technology; and better, more efficient service to our clients and employees.

CIO Council

The HHS CIO Council, a cross-OPDIV review committee comprised of the OPDIV CIOs and chaired by the HHS CIO, is responsible for reviewing the technical and managerial soundness of IT investments and providing technical recommendations to the ITIRB.

Commercial Off-the-Shelf (COTS)

COTS refer to a product available in the commercial market place. COTS products are sold to the general public in the course of normal commercial business operations at prices based on established catalog or market prices (Federal Acquisition Regulations). COTS products are delivered with pre-established functionality, although some degree of customization is possible.

Contracting Officer (CO)

The Contracting Officer has the authority to enter into, administer, and/or terminate contracts and make related determinations and findings. The term includes certain authorized representatives of the contracting officer acting within limits of their authority as delegated by the contracting officer. The contracting officer and/or his representative are accountable for preparing solicitation documents with technical support from the Project Manager and acting on behalf of the Head of the Contracting Activity.

Control Phase:

This phase of the CPIC process ensures that IT initiatives are developed and implemented in a disciplined, well-managed, and consistent fashion; that project objectives are being met; that the costs and benefits were accurately estimated; and that spending is in line with the planned budget. This promotes the delivery of quality products and results in initiatives that are completed within scope, on time, and within budget.

Critical Partner

The Critical Partners are functional managers in Enterprise Architecture, Security, Acquisition Management, Finance, Budget and Human Resources that participate in IT project reviews and governance decisions to ensure compliance with policies in their respective areas and to make timely tradeoff decisions where conflicts arise during the planning and execution of a project.

Earned Value Management (EVM)

Earned Value Management integrates the scope of work with schedule and cost elements for optimum planning and control. The qualities and operating characteristics of earned value management systems are described in American National Standards Institute (ANSI) /Electronic Industries Alliance (EIA) Standard-748-1998, Earned Value Management Systems.

Enterprise Architecture (EA)

Enterprise Architecture is a strategic information asset base which defines business mission needs, the information content necessary to operate the business, the information technologies necessary to support business operations, and the transitional processes necessary for implementing new technologies in response to changing business mission needs. Enterprise architecture includes baseline architecture, target architecture and a sequencing plan.

Enterprise Performance Life Cycle (EPLC)

The EPLC is a framework to enhance IT Governance through rigorous application of sound investment and project management principles and industry best practices. The EPLC provides the context for the HHS IT Governance process and describes interdependencies between its project management, investment management, and capital planning components. The EPLC is comprised of 10 phases – from initiation through disposition – and identifies the activities, roles and responsibilities, Stage Gate Reviews, and exit criteria for each phase. The EPLC framework complies with federal regulations and policies, industry best practices, and HHS policies and standards.

Evaluate Phase:

This phase of the CPIC process involves comparing actual to expected results once an IT investment has been implemented; evaluating "mature" systems on their continued effectiveness in supporting mission requirements, and evaluating the cost of continued support or potential retirement and replacement.

Functional Requirements

Functional requirements specify Business Product features and what the Business Product must do. They are directly derived from the objectives defined in the Project Management Plan. A functional requirement is a tangible service, or function, that the Business Product must provide and is a non-technical requirement. See also Non-functional Requirements.

Government Off-the-Shelf (GOTS)

GOTS refers to a product developed by or for a government agency and that can be used by another government agency with the product's pre-established functionality and little or no customization.

Independent Verification & Validation (IV&V)

IV&V is a process employing rigorous methodologies for evaluating the correctness and quality of the product, conducted by personnel not directly engaged in the development of the product. IV&V is a way to ensure that the Business Product is developed in accordance with customer requirements, and that the product is well-engineered. *Validation* is concerned with checking that the product meets the user needs; *Verification* is concerned with checking that the product is well engineered. This is sometimes expressed as "Are we building the right product (or system)?" and "Are we building the product (or system) right?" Therefore, IV&V typically performs in-depth technical analyses of the products and the processes of system development. IV&V advises the customers when signs of problems begin to emerge so that the customer can make plans to deal with the situations.

Information Technology (IT)

Information technology, as defined by the Clinger-Cohen Act of 1996, sections 5002, 5141, and 5142, means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this definition, equipment is “used” by an agency whether the agency uses the equipment directly or it is used by a contractor under a contract with the agency that (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Information Technology Investment Review Board (ITIRB)

The ITIRB is a cross-functional executive review committee responsible for overseeing the management of the HHS IT portfolio, approving and prioritizing IT investments to best achieve HHS strategic goals and objectives, and leveraging opportunities for collaboration across HHS OPDIVs on IT investments that support common lines of business. The HHS ITIRB shall ensure that the HHS IT investment portfolio is of the highest quality and meets the business needs of the Department in the most effective and efficient manner.

IT Investment

An organizational investment employing or producing IT or IT-related assets. Each investment has or will incur costs for the investment, has expected or realized benefits arising from the investment, has a schedule of project activities and deadlines, and has or will incur risks associated with engaging in the investment.

IT Portfolio

The combination of all IT assets, resources, and investments owned or planned by an organization in order to achieve its strategic goals, objectives, and mission.

IT Project

A project is a temporary planned endeavor funded by an approved information technology investment; thus achieving a specific goal and creating a unique product, service, or result. A project has a defined start and end point with specific objectives that, when attained signify completion.

Integrated Project Team (IPT)

The IPT is established by the manager of each IT project with technical and critical partner expertise appropriate to the size, complexity and operational requirements of the project An IPT typically shall consist of representatives from the business office, including any applicable subject matter experts, technical IT staff, budget, acquisition, security, and Enterprise Architecture.

Investment Manager (IM)

The Investment Manager is responsible for planning and executing the investment to achieve approved baselines. The IM may or may not be a subject matter expert in the business area supported by the investment.

IT Governance Organization

The IT Governance organization at HHS and at each OPDIV is responsible for ensuring that projects are technically sound, follow established IT project management practices, and meets the Business Owner’s needs. Components of the IT Governance organization are the ITIRB, the CIO Council (Technical Review Board at the OPDIV level), the Chief Information Officer, and CPIC Manager.

Non-functional Requirements

Non-functional requirements specify the criteria that are used to judge the operation of a Business Product, rather than specific behaviors (in contrast to functional requirements, which describe behavior or functions). Typical non-functional requirements are reliability, scalability, accessibility, performance, availability, and cost. Other terms for non-functional requirements are “constraints”, “quality attributes”, and “quality of service requirements". Non-functional requirements also specify the laws, regulations, and standards with which the Business Product must comply.

Performance Baseline Management (BPM)

Performance Baseline Management (PBM) is the primary HHS CPIC methodology for measuring, reporting, and evaluating the performance of all HHS Major and Tactical IT Investments, and of all HHS Supporting IT Investments with budget year costs equal to or greater than $1M.

Project

A project is a temporary planned endeavor funded by an approved investment; thus achieving a specific goal and creating a unique product, service, or result. A project has a defined start and end point with specific objectives that, when attained signify completion.

Project Manager (PM)

The Project Manager is responsible for project performance in relation to approved cost, schedule and performance baselines. The Project Manager maintains information project status, control, performance, risk, corrective action and outlook. This person is accountable to the Business Owner for meeting business requirements and to IT Governance for meeting IT project management requirements. The Project Manager shall develop the business case in conjunction with the Business Owner to clearly define and capture business need requirements, conduct project planning to adequately define and execute the tasks required to meet approved cost, schedule and performance baselines and conform to HHS policies that apply to IT projects. Project Managers shall be responsible for timely reporting of significant variances from approved baselines and providing corrective action plans or rebaselining proposals as appropriate.

Records Management

Records Management consists of the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved in records creation, maintenance and use, and disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations (44 U.S.C. 2901).

Requirements

Requirements specify what should be produced. They are descriptions of either how the Business Product should behave (functional requirements), or of how the Business Product must comply with laws, regulations, and standards (non-functional requirements).

Risk

An uncertain event that may affect the performance objectives (i.e., cost, schedule, scope or quality) of a project, usually negatively.

Risk Management

An approach for addressing the risks associated with project. Risk management includes identification, analysis, prioritization, and control of risks. Especially critical are those techniques that help define preventative measures to reduce the probability of these factors from occurring and identify countermeasures to successfully deal with these constraints if they develop.

Rough Order of Magnitude (ROM) Cost and schedule estimates based on high-level requirements, and an overall prediction of work to be done to satisfy those requirements. Typically, ROM estimates are based on approximate cost models or expert analysis, and presented as a range.

Section 508 Section 508 refers to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), which requires Federal agencies to develop, procure, maintain, or use electronic and information technology that is accessible to Federal employees and members of the public with disabilities.

Select Phase This phase of the CPIC process ensures that IT investments are chosen that best support the Agency's mission and align with HHS' approach to enterprise architecture.

Solution A comprehensive architectural response to a business problem. Solutions address all layers of the Enterprise Architecture - strategy, business, data, applications and technology/information security.

Stage Gate Phase-driven go/no-go decision points where EPLC activities are reviewed to ensure that appropriate OMB and HHS requirements are observed. A system cannot proceed without a "go" decision or a conditional approval granted by the appropriate senior manager for the specific control gate.

System of Record (SOR) The Privacy Act defines a SOR as a group of any records under the control of a Federal agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Additionally, the Privacy Act requires that the Federal government inform the public of any collection of information about its citizens from which data are retrieved by a unique identifier as described above

1

APPENDIX C: DELIVERABLES DESCRIPTIONS

The table below is a list of deliverable and component descriptions within each outlined phase.

Deliverable	Deliverable Description
Initiation	
Business Needs Statement (Final)	A Business Needs Statement identifies the business need for a proposed investment or project. It includes a brief description of the proposed project's purpose, goals, and scope. The Business Needs Statement provides sufficient information to justify a decision whether or not the organization should move forward with the development of a full business case.
Concept	
Business Case with components (Final) • Business Process Models (BPMs) • Investment/Project Categorization (e.g., FIPS-199 categorization needed for information security) Concept High-Level Requirements • Preliminary Acquisition Strategy	The Business Case is a documented, structured proposal for business improvement that is prepared to facilitate a selection decision for a proposed investment or project by organizational decision makers. The Business Case describes the reasons and justification for the investment or project in terms of business process performance, needs and/or problems, and expected benefits. It identifies the high-level requirements that are to be satisfied, an analysis of proposed alternative solutions (with reasons for rejecting or carrying forward each option), assumptions, constraints, a risk-adjusted cost-benefit analysis, and preliminary acquisition strategy.
Project Charter (Final)	The Project Charter formally authorizes a project, describes the business need for the project and the product to be created by the project. It provides the project manager with the authority to apply up to a certain level of organizational resources to project activities.
Project Management Plan (PMP) with components (Preliminary) • Risk Management • Acquisition Strategy • Change Management • Configuration Management • Project Categorization • Requirements Management • Communications Plan • Work Breakdown Structure (WBS) /Project Schedule • IV&V Planning • Quality Assurance • Records Management • Staffing Management Plan • Security Approach (a description of how security requirements will be addressed by the plan)	The Project Management Plan (PMP) is a dynamic formally approved document that defines how the project is executed, monitored and controlled. It may be summary or detailed and may be composed of one or more subsidiary management plans and other planning documents. The main objective of the PMP is to document assumptions and decisions for how the project is to be managed, to help in communication between all of the concerned parties and to document the scope, costs and time sequencing of the project.

Deliverable	Deliverable Description
Planning	
Project Management Plan (PMP) with components (Final) • Risk Management • Acquisition Strategy • Change Management • Configuration Management • Project Categorization • Requirements Management • Communications Plan • Work Breakdown Structure (WBS) /Project Schedule • IV&V Planning • Quality Assurance • Records Management • Staffing Management Plan • Security Approach (a description of how security requirements will be addressed by the plan)	The Project Management Plan (PMP) is a dynamic formal approved document that defines how the project is executed, monitored and controlled. It may be summary or detailed and may be composed of one or more subsidiary management plans and other planning documents. The main objective of the PMP is to document assumptions and decisions for how the project is to be managed, to help in communication between all of the concerned parties and to document the scope, costs and time sequencing of the project.
Privacy Impact Assessment (PIA) (Final)	Based on the initial FIPS 199 categorization and the identification of the need or potential to collect Privacy Act data/information, the assessment required by the Privacy Act and/or E-Government Act of 2002 to conduct assessments on projects before developing or procuring information technology that collects, maintains, or disseminates personal information in identifiable form. A PIA is an agency review of how collected information is handled by and protected in a manner consistent with Federal standards for privacy and information security. The PIA determines what kind of information in identifiable form is contained within a system, what is done with that information, and how that information is protected. Though the PIA specifically refers to "privacy", a PIA also typically covers confidentiality, access to data, and use of data.
Project Process Agreement (PPA) (Final) • Deliverable & Stage Gate Waivers • Authorization to Proceed	The Project Process Agreement (PPA) is used to authorize and document the justifications for using, not using, or combining specific Stage Gate Reviews and the selection of specific deliverables applicable to the investment/project, including the expected level of detail to be provided.
Requirements Analysis	
Requirements Document with components (Final) • Functional & Non-Functional Requirements • Requirements Traceability Matrix (RTM) • Business Process Model (BPM)	The Requirements Document describes both the project and product requirements. It outlines the technical, functional, performance and other requirements necessary to deliver the end business product.

Deliverable	Deliverable Description
Expansion • Logical Data Model	
Design	
Design Document with components (Architectural & detailed elements) (Final) • Physical Data Model (database design) • Release Strategy • Data Conversion • Interface Control • Section 508 Compliance • Capacity /Implementation Planning • Updated RTM	The Design Document describes the technical solution that satisfies the requirements for the Business Product (e.g., system). Either directly or by reference to other documents, the Design Document provides a high-level overview of the entire solution architecture and data design, including external interfaces, as well as lower-level detailed design specifications for internal components of the Business Product that are to be developed.
Computer Match Agreement (CMA) (Final)	A Computer Match Agreement CMA is a written accord that establishes the conditions, safeguards, and procedures under which a Federal organization agrees to disclose data where there is a computerized comparison of two or more automated System of Records (SORs). In conjunction with a CMA, an Inter/Intra-agency Agreement (IA) is also prepared when the SOR(s) involved in the comparison are the responsibility of another Federal agency.
Test Plan (Final Draft) • Test Case Specification	The Test Plan defines the types of tests (e.g. unit, function, integration, system, information security, performance (load and stress), regression, user acceptance, and/or independent verification and validation) to be carried out. The document describes the acceptance criteria for those tests, roles and responsibilities of individuals involved in the testing process, traceability matrix, resources required (hardware and software environments), and other elements relevant to test planning and execution. This plan details the manner of testing (test cases, simulation, etc) of the integrated software/hardware system. It must include as part of the main document or as a separate document detailed Test Case Specifications that describe the purpose and manner of each specific test, the required inputs and expected results for the test, step-by-step procedures for executing the test, and the pass/fail criteria for determining acceptance.
Contingency/Disaster Recovery Plan (Final Draft)	The Contingency/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 plan describes the strategy for ensuring recovery of the business product in accordance with stated recovery time and recovery point objectives.

Deliverable	Deliverable Description
System of Record Notice (SORN) (Final Draft)	The Privacy Act defines a System of Record (SOR) as a group of any records under the control of a Federal agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Additionally, the Privacy Act requires that the Federal government inform the public of any collection of information about its citizens from which data are retrieved by a unique identifier as described above. The System of Record Notice (SORN) fulfills this requirement to inform the public via the publication of a system notice in the Federal Register. This notice describes the SOR and gives the public an opportunity to comment. Without the written consent of the subject individual, the Privacy Act prohibits the release of protected information maintained in a SOR unless one of the 12 defined disclosure exceptions is applicable.
Development	
Test Plan (Final) • Test Case Specification	The Test Plan defines the types of tests (e.g. unit, function, integration, system, information security, performance (load and stress), regression, user acceptance, and/or independent verification and validation) to be carried out. The document describes the acceptance criteria for those tests, roles and responsibilities of individuals involved in the testing process, traceability matrix, resources required (hardware and software environments), and other elements relevant to test planning and execution. This plan details the manner of testing (test cases, simulation, etc) of the integrated software/hardware system. It must include as part of the main document or as a separate document detailed Test Case Specifications that describe the purpose and manner of each specific test, the required inputs and expected results for the test, step-by-step procedures for executing the test, and the pass/fail criteria for determining acceptance.
Operation & Maintenance Manual (Final Draft) • Help Desk Support	The Operations & Maintenance Manual clearly describes the Business Product that will be operating in the production environment and provides the operations and support staff with the information necessary to effectively handle routine production processing, ongoing maintenance, and identified problems, issues, and/or change requests.
Systems Security Plan (SSP) (Final Draft)	The SSP describes managerial, technical and operational security controls (defined by the National Institute of Standards and Technology) that are designed and implemented within the system.
Training Plan (Final Draft)	The Training Plan describes the overall goals, learning objectives, and activities that are to be performed to develop, conduct, control, and evaluate instructions that are to be provided to end users, operators, administrators, and support staff who will use, operate, and/or otherwise support the solution.
Training Materials (Final Draft)	Training Materials include the documentation associated with the deployment of the Business Product. This includes instructor and student guides, audio-visual aids, and computer-based or other media used to disseminate information about the final product to the target audience that is in need of the instruction.

Deliverable	Deliverable Description
Security Risk Assessment (SRA) (Final Draft)	A Security Risk Assessment will document the analysis of the security functional requirements and will identify the protection requirements for the system using a formal risk assessment process. The risk assessment includes the identification of threats to and vulnerabilities in the information system; the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on agency assets or operations and the identification and analysis of information security controls for the information system.
User Manual (Final Draft)	The User Manual clearly explains how a business user is to use the established Business Product from a business function perspective.
Business Product (Final Draft) • Version Description Document	The Business Product is the primary result from the development effort that satisfies the established requirements. In software development efforts, it includes the original source code and machine-compiled, executable computer instructions and data repository (ies). It also includes an identification and description of all configuration items that comprise a specific build or release of the Business Product.
Test	
Implementation Plan (Final)	The Implementation Plan describes how the business product will be installed, deployed, and transitioned into the operational environment.
Test Reports (Final)	Test Reports are completed at the end of each test to verify expected results. A summary report should be created at the end of the testing phases to document the overall test results. These reports summarize the testing activities that were performed and describe any variances between the expected test results and the actual test results and includes identification of unexpected problems and/or defects that were encountered.
Implementation	
Authority to Operate (ATO) with components (Final) • Security Certification & Accreditation Letters • Section 508 Product Certifications/Exceptions	An Authority to Operate (ATO) is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of a Business Product and explicitly accepts the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of information security controls. Though not security-specific, formal documentation of Section 508 Certification or Exception is also required before a Business Product can be released into operation.
System of Record Notice (SORN) (Final)	The Privacy Act defines a System of Record (SOR) as a group of any records under the control of a Federal agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Additionally, the Privacy Act requires that the Federal government inform the public of any collection of information about its citizens from which data are retrieved by a unique identifier as described above. The System of Record Notice (SORN) fulfills this requirement to inform the public via the publication of a system notice in the Federal Register. This notice describes the SOR and gives the public an opportunity to comment. Without the written consent of the subject individual, the Privacy Act prohibits the release of protected

Deliverable	Deliverable Description
	information maintained in a SOR unless one of the 12 defined disclosure exceptions is applicable.
Service Level Agreement(s) (SLAs) and/or Memorandum(s) of Understanding (MOU)	A Service Level Agreement(s) (SLAs) is a contractual agreement between a 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 each parties requirements, responsibilities and period of performance.
Operation & Maintenance Manual (Final) • Help Desk Support	The Operations & Maintenance Manual clearly describes the Business Product that will be operating in the production environment and provides the operations and support staff with the information necessary to effectively handle routine production processing, ongoing maintenance, and identified problems, issues, and/or change requests.
Systems Security Plan (SSP) (Final)	The SSP describes managerial, technical and operational security controls (defined by the National Institute of Standards and Technology) that are designed and implemented within the system.
Training Plan (Final)	The Training Plan describes the overall goals, learning objectives, and activities that are to be performed to develop, conduct, control, and evaluate instructions that are to be provided to end users, operators, administrators, and support staff who will use, operate, and/or otherwise support the solution.
Training Materials (Final)	Training Materials include the documentation associated with the deployment of the Business Product or software. This includes instructor and student guides, audio-visual aids, and computer-based or other media used to disseminate information about the final product to the target audience that is in need of the instruction.
Security Risk Assessment (SRA) (Final)	A Security Risk Assessment will document the analysis of the information security functional requirements and will identify the protection requirements for the system using a formal risk assessment process. The risk assessment includes the identification of threats to and vulnerabilities in the information system; the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on agency assets or operations and the identification and analysis of information security controls for the information system.
User Manual (Final)	The User Manual clearly explains how a business user is to use the established Business Product from a business function perspective.
Business Product (Final) • Version Description Document	The Business Product is the primary result from the development effort that satisfies the established requirements. In software development efforts, it includes the original source code and machine-compiled, executable computer instructions and data repository (ies). It also includes an identification and description of all configuration items that comprise a specific build or release of the Business Product.
Project Completion Report (Final)	The Project Completion Report describes any differences between proposed and actual accomplishments, documents lessons learned, provides a status of funds, and provides an explanation of any open-

Deliverable	Deliverable Description
• Closeout Certification • Lessons Learned	ended action items, along with a certification of conditional or final closeout of the development project.
Contingency/Disaster Recovery Plan (Final)	The Contingency/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 plan describes the strategy for ensuring recovery of the business product in accordance with stated recovery time and recovery point objectives.
Plan of Action and Milestones (POA&M)	A management process that outlines weaknesses and delineates the tasks necessary to mitigate them. The HHS Information Security Program POA&M process will be used to facilitate the remediation of information security program- and system-level weaknesses, and will provide a means for: Planning and monitoring corrective actions; • Defining roles and responsibilities for weakness resolution; • Assisting in identifying the security funding requirements necessary to mitigate weaknesses; • Tracking and prioritizing resources; and • Informing decision makers.
Privacy Impact Assessment	A PIA is an agency review of how collected information is handled by and protected in a manner consistent with Federal standards for privacy and information security. The PIA determines what kind of information in identifiable form is contained within a system, what is done with that information, and how that information is protected. Though the PIA specifically refers to "privacy", a PIA also typically covers confidentiality, access to data, and use of data.
Operations & Maintenance	
Annual Operational Analysis (AOA) (Final)	The Annual Operational Analysis (AOA) combines elements from the CPIC evaluation and results from monitoring the performance of the Business Product during normal operations against original user requirements and any newly implemented requirements or changes. This document assists in the analysis of alternatives for deciding on new functional enhancements and/or modifications to the business product, or the need to dispose of or replace the business product altogether.
Disposition Plan (Final) • Records Management	The Disposition Plan addresses how the various components of an operating Business Product (e.g., system) are to be handled at the completion of operations to ensure proper disposition of all the Business Product components and to avoid disruption of the individuals and/or any other Business Products impacted by the disposition. Includes the planning for the deliberate and systematic decommissioning of the asset with appropriate consideration of records management.
Plan of Action and Milestones (POA&M)	A management process that outlines weaknesses and delineates the tasks necessary to mitigate them. The HHS Information Security Program POA&M process will be used to facilitate the remediation of information security program- and system-level weaknesses, and will

Deliverable	Deliverable Description
	provide a means for: • Planning and monitoring corrective actions; • Defining roles and responsibilities for weakness resolution; • Assisting in identifying the security funding requirements necessary to mitigate weaknesses; • Tracking and prioritizing resources; and • Informing decision makers.
Privacy Impact Assessment	A PIA is an agency review of how collected information is handled by and protected in a manner consistent with Federal standards for privacy and information security. The PIA determines what kind of information in identifiable form is contained within a system, what is done with that information, and how that information is protected. Though the PIA specifically refers to "privacy", a PIA also typically covers confidentiality, access to data, and use of data.
Disposition	
Project Archives (Final)	Project Archives preserve vital information, including both documentation of project execution and the data from the production system.
Annual	
Continued ATO	Resulting from a periodic review of an operating Business Product, a Continued ATO is a formal declaration by a DAA that a Business Product is approved to continue to operate at an acceptable level of risk in the designated production environment.
Recurring or As Needed	
Data Use Agreement (DUA)	A Data Use Agreement (DUA) is a legal binding agreement between a Federal agency and an external entity (e.g., contractor, private industry, academic institution, other Federal government agency, or state agency), when an external entity requests the use of personal identifiable data that is covered by the Privacy Act of 1974. The agreement delineates the confidentiality requirements of the Privacy Act, information security safeguards, and the Federal agency's data use policies and procedures. The DUA serves as both a means of informing data end users of these requirements and a means of obtaining their agreement to abide by these requirements. Additionally, the DUA serves as a control mechanism through which the Federal agency can track the location of its data and the reason for the release of the data. A DUA requires that a System of Records (SOR) be in effect, which allows for the disclosure of the data being used.
Independent Verification & Validation (IV&V) Reports	Independent Verification &Validation (IV&V) Reports document the findings obtained during a specific IV&V Assessment that is conducted by an independent third party.
Privacy Impact Assessment	A PIA is an agency review of how collected information is handled by and protected in a manner consistent with Federal standards for privacy and information security. The PIA determines what kind of information in identifiable form is contained within a system, what is done with that information, and how that information is protected. Though the PIA specifically refers to "privacy", a PIA also typically

Deliverable	Deliverable Description
	covers confidentiality, access to data, and use of data.
Periodically, as Established in Project Plan	
Integrated Baseline Documentation	Performance Measurement Baseline (PMB) documents, such as the Work Breakdown Structure (WBS), the WBS Dictionary, the Responsibility Assignment Matrix, Project schedules, Control Account Plans, and Work Authorization Document.
Contractor Performance Report (CPR), or acceptable equivalent, if full EVM standards compliance is not required	The Contract Performance Report (CPR), a periodic Earned Value report, presents the cost, schedule, and performance data for the current period and cumulatively. Typically, the CPR presents costs organized by WBS element at a level pre-determined by the HHS IT Project team, and includes explanations for cost and schedule variances that have exceeded thresholds and descriptions of contractor plans to resolve variance causes.
Contract Fund Status Report (CFSR), or acceptable equivalent, if full EVM standards compliance is not required	A status report that provides investment and project managers with the following information necessary to: • Update and forecast contract fund requirements. • Plan and decide on funding changes. • Develop fund requirements and budget estimates to support approved investments or projects. • Determine funds in excess of contract needs and available for de-obligation. • Develop rough estimates of termination costs. • Determine if sufficient funds are available by fiscal year to execute the contract. Typically, the investment or project manager requires only the minimum data necessary for effective management control. The contracting officer and contractor negotiate reporting provisions in the contract, including level of detail and reporting frequency. In addition, the CFSR is not applied to Firm-Fixed Price contracts unless unusual circumstances dictate specific funding visibility.
Project Schedule (Updated)	The project schedule is developed so that tasks and milestones are clearly defined. It is updated regularly to identify IT project elements that are behind as well as those ahead of schedule. The project schedule maps directly to the WBS, providing the project management team with a single point of reference for all activities.
Periodic Investment Status Report	Periodic Status Report describes work accomplished as of the reporting period, work planned for the next reporting period, and any issues that require management attention. The status report also typically includes project cost and schedule data for the reporting period and cumulatively
Meeting Minutes	Meeting Minutes are a written record of what transpired during a meeting. Meeting minutes provide the purpose of a meeting, list of attendees, topics discussed, decisions made, the status of actions from previous meeting, new action items and the individuals assigned responsibility for the actions.

APPENDIX D: REFERENCES

Acquisition

Acquisition Strategy Guidance, July 29, 2009

Acquisition Strategy Template, July 29, 2009

Capital Planning and Investment Control

HHS-OCIO Pilot Policy for Information Technology Investment Performance Baseline Management, November 3, 2009

HHS OCIO Policy for IT Capital Planning and Investment Control, December 30, 2005

Earned Value Management

OMB Memorandum 05-23, Improving Information Technology (IT) Project Planning and Execution, August 5, 2005

Acquisition Policy Memorandum, October 10, 2008

Enterprise Architecture

HHS OCIO IT Policy for Enterprise Architecture, August 7, 2008

Information Resource Management

OMB Circular A-11, Preparation, Submission and Execution of the Budget

OMB Circular A-127, Financial Management Systems

OMB Circular A-130, Management of Federal Information Resources

HHS Policy for Section 508 Electronic and Information Technology, January 2005

Finance

GAO Cost Estimating Guide, March 2009

Records Management

HHS OCIO Policy for Records Management, September 15, 2005

HHS OCIO Policy for Electronic Records Management, September 15, 2005

Security & Privacy

HHS-OCIO Policy for Information Systems Security and Privacy (IS2P) – Policy, June 25, 2009

HHS-OCIO Policy for Information Systems Security and Privacy (IS2P) - Handbook, June 25, 2009

HHS Security Policies, Standards, Memorandums, and Guides

FIPS – 199 Minimum Security Requirements for Federal Information and Information Systems

NIST Special Publication 800-30 (Risk Management Guide for IT)

NIST Special Publication 800-37 (Guide to Certification and Accreditation)

NIST Special Publication 800-53 (Recommended Security Controls for Federal IT Systems)

NIST Special Publication 800-100 (Information Security Handbook – A Guide for Managers)

APPENDIX E: SECURITY DELIVERABLES

Security Deliverable	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	Operations & Maintenance	Disposition	References
System Accreditation Boundary Scope Memo		FD	F								FASP Boundary Memo Template
FIPS 199 Security Categorization Memo [part of Business Case]		FD	F								FIPS 199/NIST SP 800-60 Rev 1
E-Auth Risk Assessment		FD	F								OMB M-04-04/NIST SP 800-63
Privacy Threshold Assessment (PTA)		FD	F						O		OMB M-03-22
Privacy Impact Assessment (PIA), if needed			P					F	O		OMB M-03-22
Minimum Baseline Security Requirements (MBLSR)			FD	F							NIST SP 800-53
Initial Risk Assessment Report		P	FD	F					O		NIST SP 800-30
Final Baseline Security Requirements (FBLSR)		P	FD	F							NIST SP 800-53
System Security Plan (SSP)			P		FD			F	O		NIST SP 800-18
IT Contingency Plan (ITCP)			P			FD		F			NIST SP 800-34
Security Self-Assessment Plan [part of Test Plan]				P	FD	F					NIST SP 800-53a
System Rules of Behavior			P				F				OMB Circular A-130
System of Records Notice (SORN)					FD			F	O		Privacy Act
Interconnection Security Agreements (ISA)			P		FD		F				NIST SP 800-47
Service Level Agreements (SLA) / Memorandums of Understanding (MOU)			P		FD		F				NIST SP 800-37
Certification Security Assessment Plan					FD	F					NIST SP 800-53
Certifying Authority Security Assessment Report (SAR)								F	O		NIST SP 800-53a
Plan of Action and Milestones (POA&M)								F	O		OMB M-09-29
Final Risk Assessment Report								F	O		NIST SP 800-30
Continuous Monitoring Plan								F	O		NIST SP 800-37
Certification Letter								F			NIST SP 800-37
Accreditation Letter								F			NIST SP 800-37
Authority to Operate (ATO)								F	O		NIST SP 800-37
Annual Security Control Test Plan and Results Report									O		NIST SP 800-53a
Annual ITCP Test Plan and Results Report									F		NIST SP 800-34
Disposition Plan									F		NIST SP 800-64
Document/Artifact Archival Memo										F	NIST SP 800-64
Media Sanitization and Component Disposal Memo										F	NIST SP 800-88

Legend: P = Preliminary, FD = Final Draft, F = Final, O = On-going