Indian Health Service
Office of Information Technology
Albuquerque, New Mexico

Standard Operating Procedure for **Enterprise Performance Life Cycle Framework**

CPIC-SOP-10-09
Version 1.0
August 2010

Record of Changes

Version	Date	Name	Description	Section
1.0	August 2010	C. Gervais	First published version.	All.

Approval

This Standard Operating Procedure (SOP) has been approved for distribution and implementation. These new procedures are effective immediately and will be enforced. Representatives of management will be authorized to conduct periodic quality checks and audits to assure compliance with these procedures.

Requests for corrections or changes to any procedures should be sent to the IHS Chief Information Officer (CIO). Exceptions or exemptions to any of these procedures must be submitted in writing to the IHS CIO for approval or disapproval.

Approved by:

/Charles Gepford/ August 5, 2010

Charles Gepford **Date**

Deputy Chief Information Officer, IHS

Date of last annual review: **Reviewed by:**

Table of Contents

1. Introduction

1.1 Purpose

The purpose of this document is to establish an Enterprise Performance Life Cycle (EPLC) policy for the Indian Health Service (IHS), which adheres to the United States Department of Health and Human Services (HHS) EPLC Framework. This document:

- Identifies how IHS will incorporate the EPLC phases and deliverables into the Capital Planning and Investment Control (CPIC) process
- Defines the required fundamentals
- Outlines a strategy for tailoring projects within the IHS

This overview document will be supplemented with support materials, such as process guides, checklists, templates, and Program Management Office (PMO) tailoring documents

1.2 Background

Information Technology (IT) plays a critical role in helping IHS carry out its mission and objectives. IHS uses IT projects to support the software and infrastructure systems that provide healthcare to American Indians and Alaska Natives (AI/ANs). IHS will use the EPLC to enhance the overall project management performance of projects over their life cycle, with the goal of reducing software development cost, improving documentation and software quality, and terminating inferior projects.

IHS should approach the management of IT projects with an enterprise perspective that facilitates smooth interfaces among other internal projects, the IHS PMOs, and HHS. These projects and their interfaces must be adequately established through a robust Enterprise Architecture (EA). Adhering to recognized IT standards, as well as to compliance with Section 508 of the Rehabilitation Act (29 U.S.C. 794d), and security and privacy requirements is essential to this goal.

By managing and governing its projects from an enterprise perspective, IHS will also be in a better position to take advantage of economies of scale as it purchases computers, related equipment, and software. Furthermore, this enterprise perspective will enable improved compliance with the Clinger-Cohen Act (CCA) and other legislative and regulatory requirements that require IHS 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, IHS must also ensure that the overall portfolio of IT investments achieves both maximum alignment with IHS strategic goals and maximum return on investment. The IHS IT Governance Program, in conjunction with the CPIC process, brings together the various Critical Partners (CPs)[1] required to ensure maximum IT portfolio performance.

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

1.3 Scope

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

Each IHS investment[2] consists of several logically related Development Modernization and Enhancement (DME) projects and/or steady state activities. Therefore, the Project Manager (PM) is responsible to the Investment Manager (IM), and the Investment Manager is directly responsible to the business sponsor and the IT governance organization for the performance of individual projects and the overall investment. The Information Technology Investment Review Board (ITIRB) acts as the principal independent oversight authority over the individual projects and overall investment.

The IHS EPLC framework is compatible with current IHS and HHS policy. It applies to the PMOs, IMs, PMs, CPs, CPIC Manager, and IT governance organizations within IHS.

1.4 Vision

The IHS EPLC framework will help establish a project management and accountability environment, where IHS IT projects achieve consistently successful outcomes that maximize alignment with HHS goals and objectives and the IHS mission. The IHS EPLC framework will work in conjunction with the IHS CPIC, Earned Value Management (EVM), and IT Governance Policy and Procedure documents.

[1] Critical partners represent the areas of Acquisition, Security and Privacy, Enterprise Architecture, Finance, Performance, and Human Resources

[2] IHS currently has three investments, the Resource and Patient Management System (RPMS), the National Patient Information Reporting System (NPIRS), and the IT Infrastructure-Continuing (ITI-Continuing)

1.5 Benefits and Outcomes

The following benefits and outcomes are expected to increase from implementation of the EPLC framework.

1.5.1 Expected Benefits

- Reduced life cycle cost and implementation time through the successful planning, engineering, implementation, maintenance, management, and governance of IT projects and investments
- Reduction of projects that do not fit within the established EA or information security structures by ensuring strategic changes are made deliberately with approved baseline changes that fully consider EA, information security, and other impacts
- Reduction of project implementation time frames and increased quality project management
- Reduction of the risk of cost overruns, schedule delays, scope creep, and other typical pitfalls by timely identification and resolution of project issues

1.5.2 Expected Outcomes

- Improved project planning and execution by PMs and faster propagation of best practices in the project management community will result in the establishment of a standardized process, which is repeatable throughout all project management activities.
- Improved management response for individual IT projects and the broader IT investment will result in improved project cost controls, better project planning, and improved reporting.
- Improved participation by the Integrated Project Team (IPT) members will improve communication, buy-in, and overall project acceptance.
- Better operational support for production systems will result in improved output and user access.
- Better measurement of IT performance (both at the individual project and at the investment level) will help to determine the types of projects the organization should pursue, project prioritization, and which projects should be terminated.

1.6 Impact

The EPLC framework implementation is likely to shift more time and resources to the planning phases for projects and require additional resources from IMs, PMs, CPs, and the 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 reworking or fixing foreseeable problems.

1.7 Goals and Objectives

IHS has adopted following HHS goals and objectives for EPLC framework implementation:

1.7.1 Goal 1

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

1.7.1.1 Objectives

- Evolve the role of Business sponsors throughout the IT project life cycle to ensure that the projects remain targeted on the highest priority business needs and meet necessary schedule and cost constraints
- Improve project performance by applying repeatable processes and industry best practices for project and EVM
- Provide guidance to PMs 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
- Standardize IT project management within IHS 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

1.7.2 Goal 2

Better integrate IT project planning and execution with IT governance, including more effective multidisciplinary reviews of IT projects

1.7.2.1 Objectives

- Facilitate alignment of IT projects within the investments with the IHS Strategic Plan and Mission.
- Streamline the IT governance process.
- Provide a more effective process for integrating multidisciplinary reviews into the IT governance process.
- Establish clear, reasonable expectations and practical standards.
- Ensure compliance with the EA and prescribed design standards.

1.8 Stakeholders

Each of the following stakeholders plays an essential role in the execution of the EPLC framework and the success of an IT project. The role of each stakeholder varies throughout the life cycle of a project.

- Three IT Governance organizations within IHS are responsible for ensuring that individual projects and overall investments are technically sound, follow established IT project management practices, and meet the business sponsor's needs. The following teams are responsible within the CPIC process:
  - **Technical Review Board (TRB)** is responsible for the technical review and scoring of proposed business cases prior to submission to the CIO and ITIRB
  - **Chief Information Officer (CIO)** is responsible for approving proposed Business Needs Statements and ensuring that funding is obtained for the approved projects
  - **ITIRB** is responsible for approval of projects with a 5-year life cycle estimated cost greater than $500K
- **CPIC Manager** is responsible for ensuring the completion of the Business Needs Statements and the business cases for IT Governance review and monthly monitoring of earned value for each of the investment's projects as they move through the EPLC Framework. The CPIC Manager is also responsible for ensuring that the yearly Office of Management and Budget (OMB) Circular A-11 and Exhibit 300s are completed for each of the IT investments in IHS.

- **CPs** are functional managers in the areas of EA, Information Security, Acquisition Management, Finance, Budget, Human Resources, Section 508 Compliance, and Performance Management. They are considered the subject matter experts for their respective areas during their participation in the IT project reviews and governance decisions. The expertise for these CP roles may be filled from a mixture of organizations or groups, as appropriate.

CPs ensures compliance with policies in their respective areas and makes timely tradeoff decisions where conflicts arise during the planning and execution of a project. An annual review of each investment by the CPs is required by OMB.

- Project management includes the following stakeholders:
  - The **IM** is responsible for the overall success of the investment. The IM is responsible for portfolio management, including EVM of all projects within the investment. The IM is responsible for ensuring that project management principles are applied to all projects within the investment and can be the approving authority for the non-mandatory Stage Gate reviews.
  - The **PM** is responsible for project performance in relation to approved cost, schedule, and performance baselines. The PM maintains information on project status, control, performance, risk, corrective action, and outlook.
  - The **IPT** is chaired by the PM. The IPT members (regardless of the organization of permanent assignment) are responsible for accomplishing assigned tasks as directed by the PM. The IPT members will be assigned by the IM. The IPT members can vary during the different phases of the EPLC, depending on the expertise that is needed.
- The **business sponsor** is the individual who serves as the primary customer and advocate for an IT project. The business sponsor is responsible for identifying the business needs and performance measures to be satisfied by an IT project; establishing and approving changes to cost, schedule, and performance goals; and validating that the IT project meets business requirements and delivers the desired business product.
- IHS out-sources much of its IT development and operations to contractor support. The **contractors** must follow the EPLC framework and be integral partners in the IHS project management process.
- **Users** are those individuals who physically use the final product for data input, reports, and other tasks.
- **Infrastructure support staff** provides common infrastructure equipment and services that both impact on and are impacted by IT project development and operations, and must be an integral part of the EPLC process.

Throughout this document the technological solution is referred to as a "business product," and incorporates both automated systems and manual procedures that have been defined in the IT project.

1.9 Categories of IT Projects

The IHS Investment Portfolio has been organized around investments comprised of multiple related IT projects. The projects are defined by the following three categories.

1. Moderate IT projects, defined as IT projects with a 5-year life cycle cost (planning, development, and operations and maintenance) of $25,000 or greater and less than $500,000.

2. Large IT projects, defined as (1) IT projects with a 5-year life cycle cost (planning, development, and operations and maintenance) of $500,000 or greater and (2) IT projects that do not require HHS review.

3. IT investments that require HHS review. Currently, these consist of the following:
   - Tactical IT investments, defined as IT projects with annual costs of at least $3 million but less than $10 million.
   - Major IT investments, defined as (1) an IT project with annual costs, including development, implementation, operations and maintenance, independent verification and validation (IV&V), and consulting services of $10 million or more; (2) an IT project with full life cycle costs, including development, implementation, operations and maintenance, IV&V, and consulting services of $50 million or more; or (3) a financial system with budget-year cost of $500,000 or greater. Major IT investments are also reviewed by the OMB.
   - IT investments otherwise designated by the HHS CIO for HHS review.

Small project that have a 5-year life cycle cost (planning, development, and operations and maintenance) of less than $25,000 are excluded from capital planning and investment control reviews.

For more information on the IT Governance process, see the IHS *Information Technology (IT) Governance Process and Procedures* document.

2. The EPLC Framework Concept

The EPLC framework provides a project management methodology that guides the activities of IMs, PMs, business sponsors, CPs, the various IT governance organizations, and other stakeholders throughout the life cycle of the project to ensure an enterprise perspective is maintained.

- Only sound, viable IT projects with reasonable baselines for funding and inclusion in each of the established IHS investments will be selected.
- 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 on achievement of their business objectives.
- IT project performance will be measured against established business outcomes and will be subject to changes as appropriate.

The 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 IHS IT investment portfolio. Although one of the objectives of the EPLC framework is to standardize IT project management based on best practices, the framework also allows tailoring to accommodate specific circumstances (e.g., size, duration, complexity, and acquisition strategy) of each project.

The EPLC framework organizes the activities, deliverables, and governance reviews of an IT project into 10 life cycle phases. As an IT project moves through the 10 phases of the EPLC Framework, it passes through a series of project and Stage Gate reviews. There are 10 Stage Gate reviews, of which 5 are mandatory, and a possible 12 project reviews that could be applied to the project depending on its size and scope.

2.1 Relationship between EPLC and CPIC Phases

The CCA mandates that each federal agency implement a **CPIC** process for selecting, controlling, and evaluating IT projects. The CPIC process consists of three phases:

1. The **Select Phase** lays a foundation for subsequent phases by selecting the IT projects that will best support the IHS mission with the greatest impact and rate of success.
2. During the **Control Phase**, IT projects are monitored to ensure that cost, schedule, and performance are managed effectively and that the project continues to meet the IHS' mission.
3. The **Evaluate Phase** begins after an IT project is implemented into production and determines if the business solution continues to be effective in meeting the original business need.

The EPLC Framework has been mandated by HHS and adopted by IHS to enhance the effectiveness the CPIC process, bringing improvement to the CPIC process through a standardized project management methodology.

2.2 EPLC Framework Elements

The basic elements of the EPLC framework include the life cycle phases, stakeholders, phase activities and deliverables, exit criteria, project reviews, and Stage Gate reviews. The following figure illustrates the integration of all these elements, and their relation to the Select, Control, and Evaluate phases of the CPIC process.

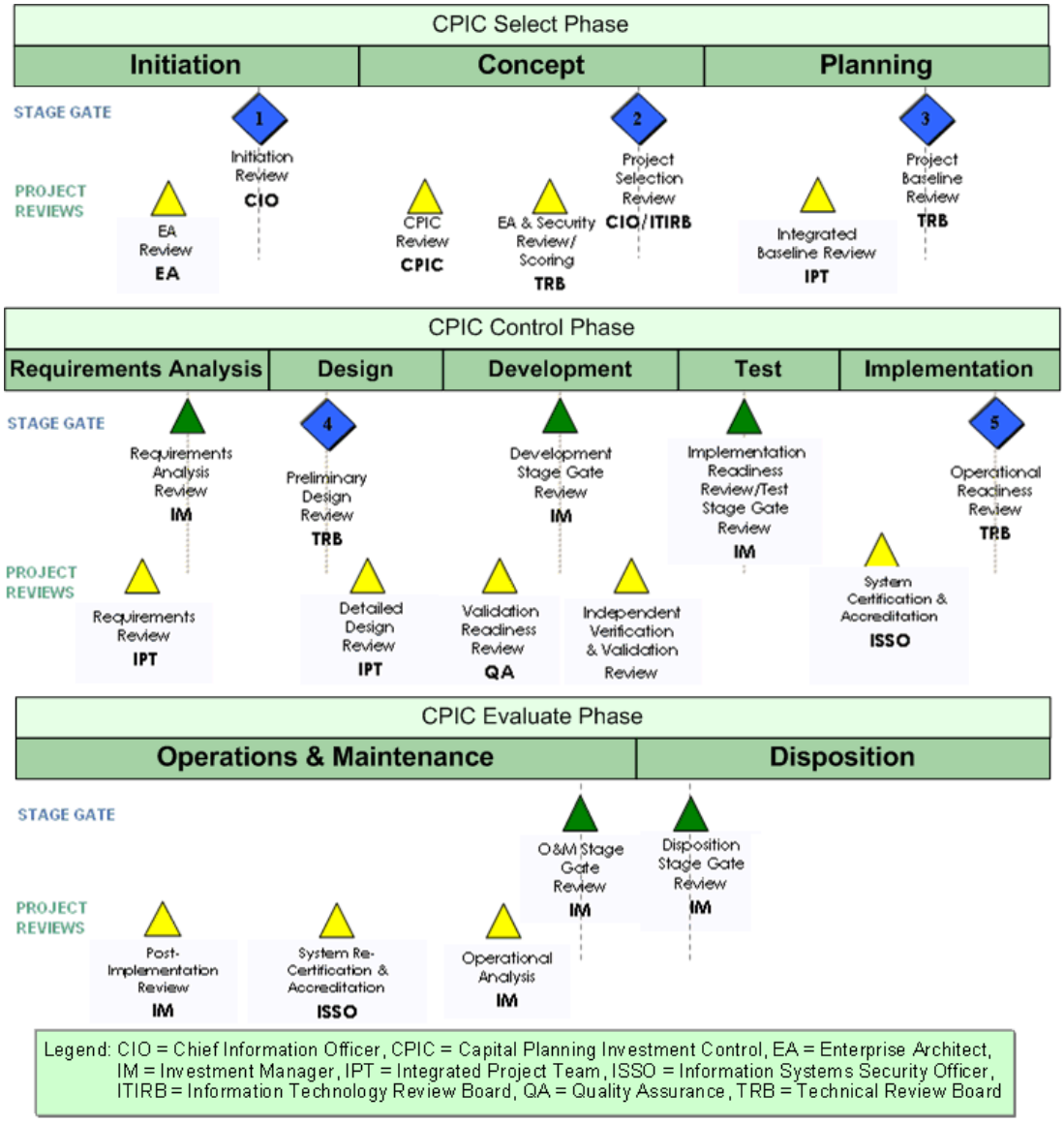

Figure 1: EPLC Framework elements, and the relationship between EPLC life cycle phases and CPIC phases

2.3 EPLC Life Cycle Phases

The following 10 phases make up the EPLC framework life cycle.

1. **Initiation** (CPIC Select Phase)

   Identify the business need, Rough Order of Magnitude (ROM) cost and schedule, and basic business and technical risks. The outcome of the Initiation Phase is the decision to invest in a full business case development.

   The main deliverable for the Initiation Phase:

   - Business Needs Statement
   - EA Checklist

2. **Concept** (CPIC Select Phase)

   Identify the high-level business and functional requirements required to develop the full business case for the proposed business product. The outcomes of the Concept Phase include selection to the appropriate IHS IT investment portfolio; approval of initial project cost, schedule, and performance baselines; and issuance of a Project Charter.

   The main deliverables for the Concept Phase:

   - Business case
   - Project Charter

3. **Planning** (CPIC Select Phase)

   Complete development of the full Project Management Plan (PMP), Work Breakdown Structure (WBS), and development of project cost, schedule, and performance baselines as necessary. Outcome of the Planning Phase is complete and adequate project planning and sufficient requirements determination to validate the planning and project baselines.

   The main deliverables for the Planning Phase:

   - PMP and subsidiaries
   - WBS
   - Privacy Impact Assessment (PIA)
   - Project Process Agreement (PPA)
   - EVM Plan and Reporting

4. **Requirements Analysis** (CPIC Control Phase)

   Develop detailed functional and nonfunctional requirements and award contracts. The outcome of the Requirements Analysis Phase is award of required contracts and approval of the requirements. Further refinement of the project baseline may be needed after the requirements are fully defined.

The main deliverables for the Requirements Analysis Phase:

- Requirements Document (RD)
- Project Baseline
- EVM Reporting

5. **Design** (CPIC Control Phase)

   Develop the Design Document. The outcome of the Design Phase is completion of business product design and successful completion of Preliminary and Detailed Design Reviews (DDRs). In situations where the business product is not developed in house, such as the acquisition of software, there may be minimal to no design requirements needed to interface the purchased software into the current EA. The level of supporting documentation and review would depend on the level of effort needed to match the required design work.

   The main deliverables for the Design Phase:

   - Design Document
   - Computer Match Agreement (CMA) (if required)
   - Draft Test Plan
   - Draft Contingency/Disaster Recovery Plan
   - Draft System of Records Notice (SORN)
   - EVM Reporting

6. **Development** (CPIC Control Phase)

   Develop code and other deliverables required to build the business product and conduct an IV&V assessment of ability of the business product to meet the specified requirements. The outcome of the Development Phase is completion of all coding and associated documentation; user, operator, and maintenance documentation, and test planning. In situations where the business product is to acquire software, there may be minimal to no in house code development. In these cases there would be minimal documentation needed depending on the level of development required.

   The main deliverables for the Development Phase:

   - Final Test Plan
   - Final Draft of Technical Manual and Install Guide
   - Final Draft of the Systems Information Security Plan
   - Final Draft of the Training Plan
   - Final Draft of the Training Materials
   - Final Draft of the User Manual

- Final Draft of the Information Security Risk Assessment
- Final Draft of the Business Project Description
- EVM Reporting

7. **Test** (CPIC Control Phase)

   Conduct thorough testing and auditing 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.

   The main deliverables for the Test Phase:

   - Testing Reports
   - Implementation Readiness Approval
   - EVM Reporting

8. **Implementation** (CPIC Control Phase)

   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.

   The main deliverables for the Implementation Phase:

   - All System Documents
   - System Certification and Accreditation
   - Authority to Operate
   - Service Level Agreements (SLAs)/Memorandums of Understanding (MOU)
   - EVM Reporting

9. **Operations and Maintenance (O&M)** (CPIC Evaluate Phase)

   Operate and maintain the production system and conduct annual operational analyses. The outcome of the O&M Phase is successful operation of the asset against current cost, schedule, and performance benchmarks.

   The main deliverables for the O&M Phase:

   - Annual Operation Analysis
   - Disposition Plan
   - System Recertification and Accreditation
   - Post-Implementation Review

10. **Disposition** (CPIC Evaluate Phase)

    Retire the 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 asset with appropriate consideration of data archiving and information security, migration of data or functionality to new assets, and incorporation of lessons learned over the project life cycle.

    The main deliverables for the Disposition Phase:

    - Lessons Learned
    - Project Archives

It is possible for a project to be in more than one EPLC phase at a time, due to the iterative nature of the process. For a more detailed description of each phase and the various tasks required to be performed during each phase, see Section 3.

2.4 EPLC 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. Based on statute, regulation, policy, and best practices, the activities are designed to reduce project risk.

The IT governance organizations must approve initial documents, as well as any changes to baselines and project plans throughout the project's life cycle. Other deliverables occur on an annual basis, usually during the O&M Phase. For a complete list of deliverables, see Appendix A. Many activities and deliverables are iterative during the life cycle, beginning with an initial effort and progressively elaborated in subsequent phases, resulting in a final deliverable, as shown in Table 1.

An important element of the EPLC framework is the ability to tailor the deliverables to specific circumstances of each project. While the overall framework provides a complete list of activities, deliverables, and reviews that are necessary to properly manage large-scale, mission-critical projects, there are other smaller, less critical projects that may not need the same level of rigor or need to be fast tracked. Section 2.11 on tailoring the EPLC Framework outlines the mandatory activities, deliverables, reviews, and requirements that cannot be waived. The PMO provides tailoring documents that establish the guidelines for projects that can be tailored or fast tracked within a project.

Table 1: Documentation Deliverables (FD-Final Draft, F-Final) by EPLC Phase

Deliverable	Phase									
	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	Operations & Maintenance	Disposition
Business Needs Statement	**F**									
Business Case		**F**								
Project Charter		**F**								
PMP			**F**							
PIA			**F**							
PPA			**F**							
RD				**F**						
Design Document					**F**					
CMA					**F**					
Test Plan					**FD**	**F**				
Contingency/Disaster Recovery Plan					**FD**			**F**		
SORN					**FD**			**F**		
Technical Manual & Install Guide						**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 Description						**FD**		**F**		
Test Reports							**F**			
Implementation Plan							**F**			
Authority to Operate								**F**		
Project Completion Report								**F**		
SLAs/MOUs								**F**		
Annual Operational Analysis									**F**	

	Phase									
Deliverable	**Initiation**	**Concept**	**Planning**	**Requirements Analysis**	**Design**	**Development**	**Test**	**Implementation**	**Operations & Maintenance**	**Disposition**
Plan of Action and Milestones (PAO&M)									**F**	
Disposition Plan									**F**	
Project Archives										**F**

2.5 Project Reviews

Project reviews are formal reviews 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 project reviews are conducted by the IM, IPT, Enterprise Architect, CPIC Manager, Information System Security Officer (ISSO) or Quality Control staff.

If the information provided in the deliverables is incomplete or not fully developed, then the reviewers can request additional information before approving the project to move forward.

2.6 Stage Gate Reviews

Stage Gate Reviews ensure that projects, as they move through their life cycles, fully comply with relevant EPLC framework and IT project management requirements.

These reviews emphasize the:

- Successful accomplishment of the phase objectives
- Plans for the next life cycle phase
- Risks associated with moving to the next life cycle phase

They also address the availability of resources to execute the subsequent life cycle phases.

One or more IT Governance organizations (IHS TRB, IHS CIO, or IHS ITIRB) must conduct the following Stage Gate reviews:

- Initiation Review (at the conclusion of the Initiation Phase)
- Project Selection Review (PSR) (at the conclusion of the Concept Phase)

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

With the exception of these five reviews, the Stage Gate reviews are delegated to the IM. When conducting a Stage Gate review, the IM will apply the same standards and will complete the same review documentation as the IT governance organizations. If the IM conducting a Stage Gate Review determines that a change in project cost, schedule, or performance baselines is required, the IM must elevate the Stage Gate review to the appropriate IT governance organization.

Stage Gate reviews are considered "go/no-go" decision points for a project's advancement to the next phase.

- The IM or IT governance organization may choose to approve the project's continuation to the next phase with or without conditions. Approval with conditions requires the IM or IT governance organization to establish a process for maintaining oversight of the project to ensure conditions are met.
- The IM or IT governance organization may require the PM to resolve one or more issues before approving continuation. If serious issues are not resolved, the IM or IT governance organization is responsible for discontinuing the project.

Stage Gate Reviews are also the most appropriate time for the IT governance organizations, in consultation with the IM, to change project cost, schedule, or performance baselines in response to changing priorities.

2.7 Exit Criteria

Exit Criteria are established as integrated Project Phase fitness measurements that must be achieved before proceeding to the next phase. Before Exit Criteria are reviewed, the PM will verify that the set of deliverables for the Phase is completed and acceptable.

On an exception basis, the IT governance organization or IM 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.

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.

2.8 EPLC Framework Approach

All framework activities fall into three categories:

- Create

- Review
- Approve

These categories of activities form the basic approach used in the EPLC framework.

2.8.1 Project Management Orientation (Create)

The PM is ultimately responsible for planning and conducting phase activities within established project cost, schedule, and performance baselines, subject to guidance and direction from the IM, the business sponsor, and the IT governance organizations.

The primary means for planning, execution, and accountability of project activities is the collection of managerial documents defined as the PMP. IHS 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. The PM maintains the PMP, keeping it current by updating its subordinate-level plans as required, to reflect changes and refinements during the life cycle.

2.8.2 Investment Management (Review)

The primary responsibility of IMs is to review the progress of an IT project at specified Stage Gate reviews, to ensure that the project meets the respective requirements. IMs are responsible for evaluating the completeness, accuracy, and adequacy of phase deliverables, and whether the project meets exit criteria for advancement to the next phase. Based on their review, IMs provide recommendations and any issues identified to the business sponsor and the IT governance organizations.

The CPIC Manager facilitates the review by IMs, and ensures that cross-functional issues are either resolved at the staff level or articulated to the appropriate IT governance organization for resolution. The CPIC Manager also consolidates IM recommendations for presentation to the appropriate IT governance organization.

2.8.3 IT Governance (Approve)

- The CIO has approval authority for moderate projects (projects with a 5-year life cycle estimated cost of $500K or less).
- The ITIRB is responsible for selecting projects for the IHS IT investment portfolio for large projects (projects with a 5-year life cycle estimated cost of greater than $500K).

- The TRB is responsible for approving project baselines and controlling changes to those baselines, monitoring performance against project baselines and requiring corrective actions where necessary, conducting Stage Gate reviews and approving Stage Gate completion.

2.9 Impact on IHS IT Project Management

Implementation of the EPLC framework will have the following impact on IT project management:

- Increased training requirements for IT Governance organization, IMs, PMs, IPT 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 sponsors, IMs, IT Governance organization, 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 as possible within the organization.
- 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.

2.10 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:

- Ongoing updates to the PMP.
- Ongoing EVM and status reporting to measure compliance with baselines to provide for timely corrective action.
- Ongoing configuration management of scope and change requests.
- Ongoing communications to ensure all stakeholders are apprised appropriately.
- Project management deliverables to be submitted on an established periodic basis include:

- 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.

2.11 Tailoring the EPLC Framework

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 project, less expensive, non-mission-critical, lower risk projects do not need as much documentation to maintain appropriate oversight and control.

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 project. However, not all IHS projects fall into this category. To meet the needs of non-major systems, the EPLC framework provides criteria to assist IMs, PMs, and IT Governance personnel in assessing appropriate tailoring of EPLC deliverables. By doing so, IHS will be able to preserve a consistent and repeatable project management methodology, while recognizing when certain elements of the framework are not applicable or not cost-effective for a particular project.

Tailoring consists of waiving particular life cycle phases, activities, deliverables, or performing reviews at the lowest possible responsibility level. The tailoring strategy will provide the justification for the tailoring, as well as identify the specific elements of the framework to be tailored.

Each IHS PMO is responsible for establishing the thresholds and requirements in which different size projects can be tailored within the scope outlined in the IHS EPLC Framework document. The PMO is responsible for documenting the investment's program tailoring strategy. The PMO Tailoring Strategy document will outline how the PMO will address all fast-track, non-mission-critical and/or lower risk projects.

At the project level, any tailoring needed for a project is described in the PPA document, which is formally approved by the TRB at the PBR during the Planning Phase of the EPLC. This is to ensure than any changes in the level of review is identified early in the development of the project and those involved know to what level of rigor the project will be subjected. Any subsequent change to the PPA document must be approved by the TRB.

2.11.1 Project Thresholds for Framework Tailoring

When determining if a project should be tailored, project life cycle costs and project risk levels must be considered. Moderate projects with a low project risk level are possible candidates for tailoring, as the following table illustrates.

Table 2: Projects Eligible for Tailoring

Eligible for Tailoring	Project Cost	Project Risk Level
No	HHS Review $500K or greater 5-year life cycle cost	Low-Medium-High
No	Moderate Project: $25K to $500K 5-year life cycle costs	Medium-High
Yes	Moderate Project: $25K to $500K 5-year life cycle costs	Low

2.11.2 Evaluation Factors and Framework Tailoring

Some fundamental elements can never be removed from the EPLC framework through tailoring. These include:

- Identifying the business need
- Obtaining authorization and approval from the CIO and/or ITRIB
- Documenting correct, clear and adequate functional requirements
- Documenting Earned Value reporting
- Following processes that ensure the system will be able to operate within the as-is and/or target EA
- Adequate testing
- Information Security certification and accreditation
- Appropriate operations and maintenance documentation

2.11.3 Stage Gate Reviews and Tailoring

There are five Stage Gate reviews that cannot be removed from the EPLC process or delegated away from the assigned IT governance organizations, as shown in the following table.

Table 3: The Five Mandatory Stage Gate Reviews

EPLC Phase	Stage Gate Review	Review Action/Outcome	Responsible Governance Organization
Initiation	**Initiation** Review	Business case Request is approved or denied.	CIO
Concept	**PSR**	Business case is approved or denied.	CIO/ITIRB
Planning	**PBR**	The approved project is baselined.	TRB
Design	**Preliminary Design** Review	The design requirements are approved or denied.	TRB
Implementation	**Operational Readiness** Review	Determines if the final business product is ready for release into the production environment.	TRB

Other than these restrictions, IMs, PMs, and the IPT should consider the following factors to determine the tailoring strategy for a project:

- **Cost.** As the cost of a project decreases, framework elements that are relatively expensive are candidates for tailoring.
- **Risk.** Framework elements that alleviate low-level risks are candidates for tailoring.
- **Schedule.** Framework elements that provide institutional knowledge, continuity over time, or support 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 contractor-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 contractor risk.

Note that while COTS projects are candidates for tailoring of development-oriented framework elements, COTS projects must accomplish many nondevelopmental EPLC framework elements to ensure proper project selection, EA compliance, information security compliance, implementation, and O&M support.

- **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.
- **IV&V.** The 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 project and governance requirements. Depending on the project size, risk and other factors, the IT Governance organization may approve tailoring or waving the IV&V requirement to match the project requirements.

2.12 Fast Track Projects

Fast tracking is a project management technique used to ensure that projects are completed within the shortest time possible. Projects identified as mission-critical or urgent demand rigorous planning and monitoring. The EPLC is intended to enable IHS to successfully manage risk; thus, it is especially important that the EPLC be applied to fast track projects.

The *Program Management Office (PMO) Tailoring Strategy* document defines how projects in an investment are to be tailored. There are three fast tracking techniques that can be applied within the EPLC:

1. **Acceleration:** The shortening of the project schedule through the acceleration of project review timetables and/or reducing the rigor of the required documentation, while still demonstrating the proposed project will meet the requirements stated.
2. **Consolidation:** It is possible to tailor the EPLC framework so that phases are consolidated.
3. **Deferral:** At Stage Gate Reviews, the IT governance organizations have the option to approve with conditions. If all exit criteria are not met, the reviewing 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.

2.13 Development Methodologies/Iterative Nature

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

2.14 Multiple Levels

The EPLC framework is intended to operate on many levels simultaneously. Two specific areas where this is true are among the various organizational levels (i.e., Departmental and the IHS) and among the hierarchy of investments, projects, and systems.

2.14.1 Department vs. IHS Review

The IHS EPLC framework is compatible with current HHS CPIC policy. IHS has established IT governance processes that are consistent with HHS CPIC policy and procedures, including the EPLC framework. The HHS focus is on ensuring IHS processes are compliant rather than conducting direct reviews of IHS-level projects as a matter of course. However, HHS reserves the right to conduct reviews of IHS-level projects when necessary to review process compliance or to otherwise fulfill its HHS IT investment and portfolio management responsibilities.

2.14.2 Investment/Project/System

There is significant variation in designation of IT investments, projects, and systems. The EPLC framework should be considered a "nested" framework for purposes of this hierarchy. For example, in IHS, an investment consists of several logically related projects. PMs are responsible to the IM for project compliance with the framework, and the IM is responsible to the ITIRB for overall investment compliance with the framework.

2.15 EPLC Guidance and Support

Implementation of the EPLC framework requires 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 a SharePoint site. This site will be directed at internal IHS stakeholders, with access granted through the CPIC Manager.

The SharePoint site will contain the following types of information:

- **Assessment Criteria**

  Assessment criteria help to determine the applicability of various elements of the EPLC framework for specific projects. Such criteria will assist both PMs and the IT governance organizations in tailoring the framework to specific projects.

- **Process Guides**

  Process Guides help IPTs comply with Federal regulations along with HHS and IHS policies and standards by (1) presenting requirements in a concise, easy-to-understand, and consistent format; (2) setting the requirements in the context of their purpose; (3) providing step-by-step instructions for completing the activities required for compliance with each process; and (4) showing the integration points between processes.

- **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.

- **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 boilerplate text.

- **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/CPIC phase, along with the stakeholder responsibilities, activities, deliverables, exit criteria, and Stage Gate Reviews required in each phase, as illustrated in Figure 2.

3.1 Initiation Phase (CPIC Select Phase)

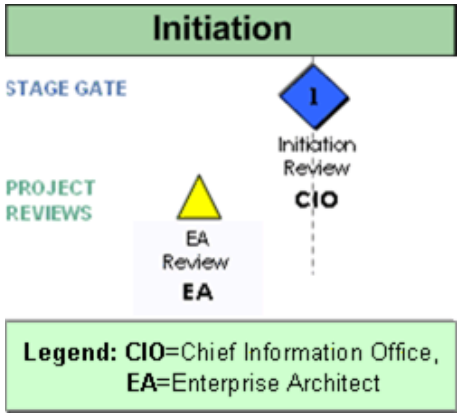

Figure 2: EPLC Initiation Phase (CPIC Select Phase)

During the EPLC Initiation Phase, a business sponsor identifies a business need for which a technological solution is required. A technological solution, referred to as a "business product," includes both technical (automated) procedures and processes, and administrative (manual) procedures and processes.

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 government mandates. When an opportunity to improve business or mission accomplishments or to address an identified deficiency, the business sponsor documents these opportunities and notifies the CIO for approval to move forward with development of a full business case. The level of supporting information is based on the project categories established by IHS.

3.1.1 Responsibilities

- **Business sponsor.** The business sponsor is the principal authority on matters regarding the expression of business need. The business sponsor is responsible for providing the documentation and communication needed to move the business case forward; this includes the completion of the **Business Needs Statement (BNS)**. The business sponsor champions the proposed IT project to the appropriate IT Governance organization to gain approval.

- **IM.** The IM is responsible for reviewing the BNS to ensure that the proposed project is within the scope of the investment. They also serve as the point person in the assignment of the PM once the BNS is approved.
- **EA.** The EA validates alignment of the proposed business product and determines if the preliminary EA review reveals any duplication, interference, or contradictions, or if it can leverage another existing or proposed project. The EA also determines if the proposed IT project addresses compliance with IHS mission and goals, and if there is any impact on the EA or the infrastructure.
- **CPIC Manager.** The CPIC Manager provides support and resource information on the development the BNS. In addition, the CPIC Manager coordinates the review process and ensures that the BNS is reviewed and approved by IM, EA, and the CIO. The BNS and business case Templates and How to Guides are posted on the CPIC Web site for reference (http://www.ihs.gov/cio/cpic).
- **CIO.** The CIO is the first member of the IT Governance organization who receives proposed business product information from the business sponsor for development of a new IT project. For moderate or large projects, the CIO must approve the expenditure of funds to develop a full business case. The CIO is also responsible for ensuring that adequate financial and business process resources are made available to support the project once approved.

3.1.2 Activities

Activities during the Initiation Phase are designed to determine if the proposed project aligns with the IHS EA and mission, supports the achievement of a short-term or long-term goal(s), and justifies development of a full business case, and if there is sufficient justification to proceed to the Concept Phase.

The initiation process begins when the business sponsor completes a BNS and forwards the completed form to the appropriate IM for review. Once the BNS is approved by the IM, the information is forwarded to the EA to review. The EA interviews the business sponsor, and once the EA checklist has been applied and there are no concerns regarding the impact of the project on the architecture, the BNS is forwarded to the CIO for final approval.

3.1.3 Project Review

The project review in the Initiation phase is the EA Review, a preliminary review that is performed to ensure that the proposed IT project is consistent with the EA. The EA Review consists of a checklist that will be presented to the CIO along with the BNS.

3.1.4 Stage Gate Review

The **Initiation Stage Gate Review** considers whether a proposed IT project presents a resolution that fits within the IHS EA. In addition, the Initiation Stage Gate Review justifies proceeding to the Concept Phase and the completion of a full business case. The Initiation Phase is completed once the proposed BNS is approved by the CIO. The Initiation Review is one of the reviews that cannot be delegated.

3.1.5 Deliverables

BNS (Final)	A BNS 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 BNS provides sufficient information to justify a decision whether or not the organization should move forward with the development of a full business case.

3.1.6 Exit Criteria

3.1.6.1 Objective

To determine if this project proposal is worth pursuing. Several of the questions being answered during this phase are:

- Is there a business sponsor associated with the proposed business solution?
- Does the project fit within the current EA?
- 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?

3.1.6.2 Phase Specific Exit Criteria

- A business sponsor has been identified and confirmed. This is someone who will champion the project, and define the business needs and project requirements.
- The proposed business product fits within the current EA.
- Project supports the goals and objectives of IHS.
- Project description is sufficient to permit development of an acceptable business case.

3.2 Concept Phase (CPIC Select Phase)

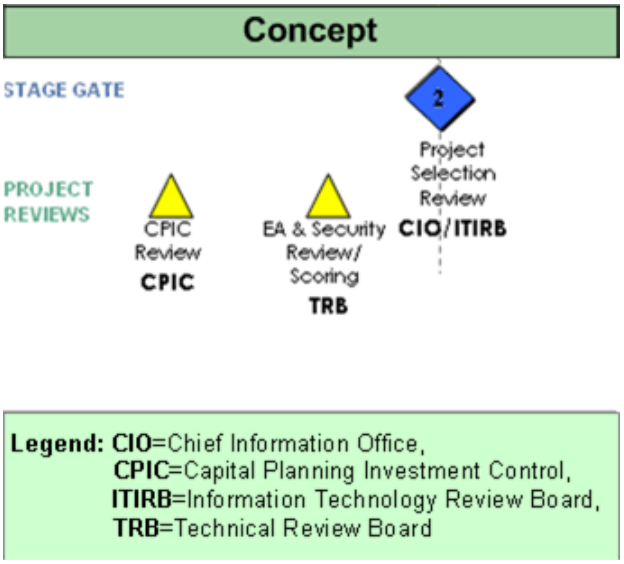

Figure 3: EPLC Concept Phase (CPIC Select Phase)

The Concept Phase:

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

The Concept Phase begins when the CIO approves the BNS and the business sponsor completes the business case template which outlines in detail the business process improvement activities, changes in business functions, advances in IT, or government mandates.

During the Concept Phase, sufficient requirements detail is developed to support the detailed cost and schedule estimates, alternatives analyses, risks, performance management, earned value, and other elements of the business case.

The primary outcomes of the Concept Phase are:

- Concurrence that the business product is a technically sound solution to a Business Need
- Concurrence that the business product adheres to the IHS EA and Information Security requirements
- A completed business case proposal and approval of the high-level cost, schedule, and performance baselines outlined in the business case

3.2.1 Responsibilities

Business Sponsor. The business sponsor 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 sponsor must understand what constitutes a requirement, and must take ownership of the requirements and input and output. The business sponsor is also responsible for ensuring that adequate financial and business process resources are made available to support the project after its approval. The business sponsor is responsible for developing the business case.

CPIC Manager. The CPIC Manager reviews the proposed business case for completeness. Once it is determined that the business case is complete, it is forwarded to the TRB for scoring. The CPIC Manager is responsible for ensuring that business cases requiring HHS review are entered into the **Portfolio Management Tool (PMT)** correctly.

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 National Institute of Standards and Technology (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
- The Initial Security Risk Assessment Report has been completed in accordance with NIST guidelines

Information Systems Advisory Committee (ISAC). An information copy of the business case is forwarded to the ISAC for review. This is to provide information prior to the formal review by the ISAC members during the ITIRB approval meeting.

TRB. The TRB is responsible for reviewing the business case to determine if the proposed solution fits within the current EA, meets the current Information Security requirements, and identifies records management and record keeping requirements. If the proposed business case does not meet the EA or Information Security requirements, then the business case is returned to the business sponsor for more information or another solution. The TRB evaluates and scores all proposed IT business cases (Moderate, Large, and HHS level) for technical soundness, and identifies opportunities to leverage and reuse existing IHS IT projects. The TRB is responsible for the business case review prior to approval by the CIO or the ITIRB.

CIO. The CIO is responsible for reviewing and approving proposed Moderate IT business cases. The CIO has the authority to request ITIRB review of Moderate IT business cases if deemed necessary. The CIO is responsible in conjunction with the ITIRB for review and approval of Large and Major Business cases.

ITIRB. The ITIRB is the primary IHS IT Governance Organization. The ITIRB approves or disapproves proposed IT business cases with life cycle cost of more than $500,000.00.

3.2.2 Activities

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

- Identify and establish the business case for the proposed project.
- Assign the approved project to an investment.
- Document the analysis and planning activities.
- Review and approve advancement to the next phase.

The Concept Phase involves the appointment of a PM by the IM who carries both the responsibility and accountability for project planning and execution. The appointment of the PM is completed after the ITIRB approves funding of the business case.

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 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 CIO or ITIRB whether to approve commitment of the necessary resources to solve the identified business need.

3.2.3 Project Reviews

There are two project reviews completed during the Concept Phase of the EPLC.

- The **CPIC Review** is completed prior to the Architecture and Information Security Review (ASR). During the CPIC Review, the business case is examined for completeness, consistency, compliance with guidelines, and rationality. The business case will be returned to the business sponsor for additional information, if it is determined that there is insufficient information. If the business case is determined to be complete, it is then forwarded on to the TRB for scoring.
- The **ASR** is completed by the TRB. The TRB reviews and scores the proposed business case to ensure that the request supports a sound business product that adheres to the EA and Information Security requirements.

After the scoring of the business case is completed, it is forwarded back to the business sponsor for additional updates if required.

3.2.4 Stage Gate Review

The Stage Gate review for the Concept Phase of the EPLC is the PSR. The PSR is a formal inspection of a proposed IT project by the CIO and/or ITIRB to determine if it is sound, viable, worthy of funding, and supports inclusion in the organization's IT investment portfolio. The PSR is conducted after the TRB reviews and scores the proposed business case. The PSR is one of the reviews that cannot be delegated.

The *Information Technology (IT) Governance Process and Procedure* document has information on the scoring criteria for PSR. This Stage Gate review cannot be delegated from the CIO or ITIRB.

3.2.5 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.

3.2.6 Exit Criteria

3.2.6.1 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 the high-level requirements meet the business need.
- The project organizational structure is scaled to support the project, and the PM is selected.
- The high-level analysis demonstrates that the outcomes will be aligned with the Target EA.
- All applicable information 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 boundaries have been established.

3.3 Planning Phase (CPIC Select Phase)

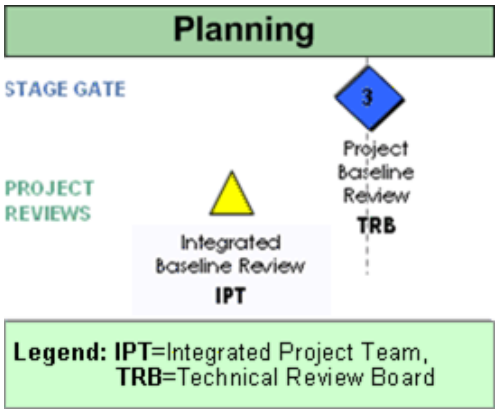

Figure 4: EPLC Planning Phase (CPIC Select Phase)

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 PMP and development activities.

During the Planning Phase, sufficient requirement details are specified to support the development of the project's PMP and permit outside validation of the deliverable.

Acquisition activities are performed, if necessary, to obtain contractor support. The project work is broken down into specific tasks and subtasks, the WBS, which includes 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 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 PMP is determined, and a scope-schedule-cost plan for how the project work will be measured (Performance Measurement Baseline (PMB)) is approved.

3.3.1 Responsibilities

IM. The IM is responsible for authorizing and ensuring that the funding and resources are in place to support the project. The IM determines if the project has been tailored, if approvals for any alteration of deliverables and reviews have been obtained, and if the PMP is fully developed. The IM also assigns the members of the IPT.

PM. The PM is responsible and accountable for the successful execution of the Planning Phase. The PM is responsible for leading the IPT that accomplishes the Phase activities and deliverables, in addition to communicating with the IM and business sponsor throughout the process.

IPT. The IPT members (regardless of the organization of permanent assignment) are responsible for completing assigned tasks as directed by the IM. The IPT provides oversight, advice, and counsel to the PM on the conduct and requirements of the planning effort. The IPT is charged with assessing the:

- Completeness of the Planning Phase activities.
- Robustness of the plans for the next life cycle phase.
- Availability of resources to execute the next phase.
- Acceptability of the acquisition risk of entering the next phase.

Additionally, the IPT provides information, judgments, and recommendations to the IM, TRB, and business sponsor during project reviews and in support of project baselines. For applicable projects, this assessment also includes the readiness to award any major contracting efforts needed to execute the next phase.

TRB. During the PBR, the TRB 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.

3.3.2 Activities

The following activities are performed as part of the Planning Phase. The results of these activities are captured in the **PMP**, the primary managerial document in the life cycle of a project.

The components of the PMP document should be tailored to the particular project's circumstances and typically, can include new or updated plans for

- Success and Completion Criteria
- Responsibility Matrix
- Risk Management
- Acquisition
- Change Management
- Configuration Management
- Project Categorization
- Requirements Management
- Communications
- WBS/Project Schedule
- IV&V
- Quality Assurance
- Records Management
- Staff Development
- Information Security Approach

The PM works with the IM and business sponsor to verify the scope of the proposed project, 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 PM plans the subsequent phases to allow development of the project schedule, budget requirements, definition of expected performance benefits, and outline of the success and completion criteria.

The PM also prepares a **PPA** that specifies project deliverables and their expected levels of detail, and documents the justification for tailoring any EPLC elements. Detailed activities and timelines for preparing acquisition documents, selecting vendors, and awarding contracts are developed.

The IPT identifies any programmatic or technical risks. The risks associated with further development are also studied. The results of these assessments are summarized in the PMP. To ensure that Privacy Act considerations are addressed early in the project life cycle, the PM also prepares a **PIA**.

3.3.3 Project Review

The **Integrated Baseline Review (IBR)** is an internal inspection led by the IPT to verify that the project baseline is established, a realistic budget is in place to accomplish all planned work, and the completion and success criteria are fully developed. The IBR includes an evaluation of the Performance Measurement Baseline for realism and inherent risks.

3.3.4 Stage Gate Review

The **PBR** is a formal inspection of the entire project and performance measurement baseline initially developed for the IT project by the IPT. 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 PMP 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. Support and training issues may become very important from this perspective. The PBR is one of the Stage Gate Reviews that cannot be delegated.

3.3.5 Deliverables

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 PM with the authority to apply up to a certain level of organizational resources to project activities.
PMP with components (Final) Risk Management Acquisition Strategy Change Management Configuration Management Project Categorization Requirements Management	The 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.

Communications Plan WBS/Project Schedule IV&V Planning Quality Assurance Records Management Staffing Management Plan Security Approach (i.e., C&A and its components)	
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.
PPA (Final) Deliverable & Stage Gate Waivers Authorization to Proceed	The 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.

3.3.6 Exit Criteria

3.3.6.1 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 PMP is fully scaled, and the details of all the appropriate components that address the needs of the project are approved. 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 (CO), 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 the highest impact have been sufficiently addressed with either mitigation or contingency plans.

3.3.6.2 Generic Exit Criteria

- Variances from baselines have been identified and managed.
  - Cost and schedule variances and scope changes are identified.
  - Significant variances are explained.
- 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 PMP and component plans have been reviewed and updated appropriately. They include:
  - 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
  - Information Security Approach

3.4 Requirements Analysis Phase (CPIC Control Phase)

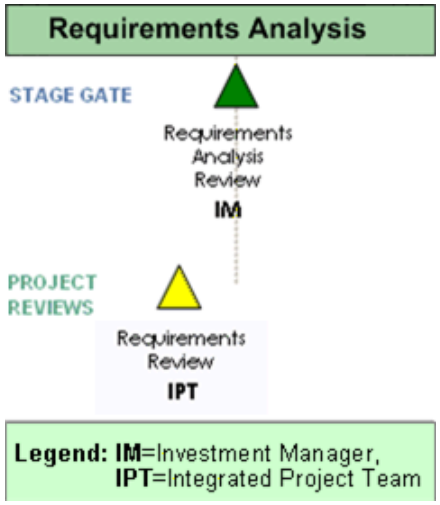

Figure 5: EPLC Requirements Analysis Phase (CPIC Control Phase)

During the Requirements Analysis Phase, the previously documented business requirements are revalidated and further analyzed. High-level system (functional and non-functional) requirements are developed that define the business product in more detail with regard to inputs, processes, outputs, interfaces, and changes to user processes and procedures. If appropriate, a logical diagram is created of the data entities, relationships, and attributes of the business product.

Detailed application requirements (both functional and nonfunctional) are required to permit detailed project management planning, execution, and control. The initial strategy for testing and implementation is also begun, and if necessary, the work planned for future phases is redefined.

The purpose of acquisition planning in the Requirements Analysis Phase is to allocate the requirements among development segments, research, and apply lessons learned from previous projects, develop a schedule that lists activities for completion and work products to be produced with appropriate estimated completion dates, identify potential product and service providers, and award contracts.

The Requirements Analysis Phase ends with a review to determine readiness to proceed to the Design Phase.

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 will be requested. In the cases in which a project needs to be rebaselined, the project may need an additional PBR by the appropriate IT governance organization.

3.4.1 Responsibilities

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

PM. The PM is responsible and accountable for the successful planning and execution of the Requirements Analysis Phase. The PM is responsible for leading the IPT that accomplishes the phase tasks and deliverables.

CPIC Manger. The CPIC Manager is responsible for reviewing monthly the EVM reports for each investment and to provide information to the CIO if there are excessive variances in the investments.

IPT. The IPT members (regardless of the organization of permanent assignment) are responsible for completion of the IBR.

CO. The CO is responsible and accountable for preparing solicitation documents under the guidance of the PM and Head of Contracting Activity.

Quality Assurance (QA). The QA team is notified of the finalized requirements and is responsible for reviewing the RD for completeness.

3.4.2 Activities

The following tasks are performed during the Requirements Analysis Phase:

- 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.
- Requirements for changes in business processes and user procedures are identified.
- Requirements for records management and recordkeeping are established.
- The **RD** is a record of the requirements. This can be established as a matrix and tracked for satisfaction of every module of the system or process.
- Documentation from prior phases may need to be revised or updated.
- The following activities are performed as part of the Requirements Analysis Phase:
    - Requirements Analysis
    - Analysis of Alternatives
    - Procurement of Government Human Resources and Services
    - Procurement Plan
    - Acquisition of Contractor Services

- Solicitation of Services
- Technical Evaluation Report
- Source Selection Recommendation
- Contract Award
- Adjustment of Funds
- Contract Performance

The results of these activities (along with additional items) are captured in the Acquisition Strategy.

- The Acquisition Strategy should provide adequate information to enable the following actions:
  - Making management decisions concerning procurement of government human resources and services (MOUs and SLAs), contractor services procurement, including ensuring the availability of funding
  - Performing a technical analysis and evaluation of vendor proposals
  - Preparing for vendor bids

The Acquisition Strategy becomes critical after the RD has been approved. Several acquisitions may be needed to procure an entire solution and are a continuous part of the life cycle. The Acquisition Strategy is updated continuously, with the active involvement of the IM and CO.

3.4.3 Project Review

The **Requirements Review** is completed after QA has reviewed the requirements for completeness. The Requirements Review is conducted by the IPT to do the following:

- Verify that the requirements are complete, accurate, consistent, and problem-free
- Evaluate the responsiveness of the requirements to the business requirements
- Ensure that the requirements are a suitable basis for subsequent design activities
- Ensure traceability within the requirements and between the design documents
- Affirm final agreement regarding the content of the RD

Upon successful completion of this review, the RD is baselined.

3.4.4 Stage Gate Review

The IPT forwards their findings to the IM for review. The IM conducts the **Requirements Analysis Stage Gate Review** and determines whether the project should proceed to the Design Phase or needs to submit the project back to the appropriate IT governance organization for rebaseline review and approval. The Requirements Analysis State Gate Review can be delegated by the IM within the established tailoring guidelines of the PMO.

3.4.5 Deliverables

RD with components (Final) Functional and Nonfunctional Requirements Requirements Traceability Matrix (RTM) BPM Expansion Logical Data Model	The RD describes both the project and product requirements. It outlines the technical, functional, performance and other requirements necessary to deliver the end business product.

3.4.6 Exit Criteria

3.4.6.1 Objective

To determine if the project requirements have been defined sufficiently to be translated into the business product.

3.4.6.2 Phase Specific Exit Criteria

- 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.
- The initial test strategy is defined and Quality Assurance is notified of the strategy.

3.4.6.3 Generic Exit Criteria

- Variances from baselines have been identified and managed:
  - Cost and schedule variances and scope changes are identified
  - Significant variances are explained
- 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 PMP and component plans have been reviewed and updated appropriately. They include:
  - 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
  - Information Security Approach

3.5 Design Phase (CPIC Control Phase)

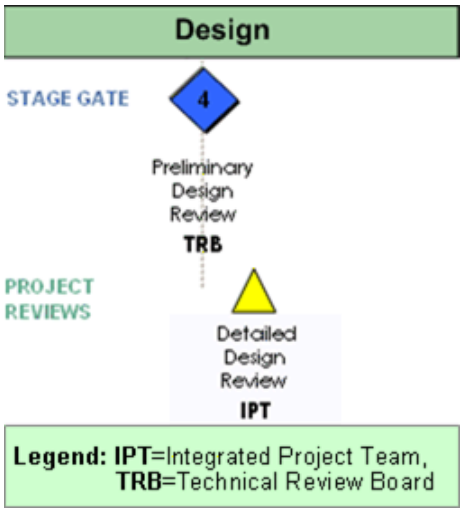

Figure 6: EPLC Design Phase (CPIC Control Phase)

The Design Phase seeks to develop detailed specifications that emphasize the physical solution to IT needs of the user. 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 specifications suitable for implementation within the constraints of a physical environment.

A formal review of the high-level architectural design is conducted prior to detailed design of the process or software to do the following:

- Ensure that the design satisfies the system requirements and is in conformance with the EA and prescribed design standards
- Raise and resolve any critical technical or project-related issues
- Identify and manage project, technical, information security, 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.

3.5.1 Responsibilities

Business sponsor. The business sponsor participates in the Preliminary Design Review.

PM. The PM is responsible and accountable for the successful execution of the Design Phase. The PM is responsible for leading the IPT that accomplishes the Phase activities and deliverables.

IPT. The IPT members (regardless of the organization of permanent assignment) are responsible for completion of the Requirements Review.

CO. The CO is responsible and accountable for preparing solicitation documents under the guidance of the PM and Head of Contracting Activity.

TRB. The TRB 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 EA.

3.5.2 Activities

The following tasks are performed during the Design Phase.

- The Design Document is developed by the PM and IPT, identifying the steps used in the design of the business product. The prerequisites for this phase are the business case, PMP, and RD. The PM and IPT identify the target environment, the development environment, and the design environment. The business organization, roles, and procedures for designing this business product 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 accordance with the Privacy Act of 1974, if an IT project involves personally identifiable data or data that could be shared by multiple agencies, then the following additional deliverables may likely be required:
  - **SORN.** Based on the PIA, developed during the Planning Phase, an SORN is prepared, if required, to inform the public of any information collection by the Business Product about citizens.
  - **CMA.** A CMA is also prepared during the Design Phase, if needed, to establish the conditions, safeguards, and procedures under which IHS agrees to disclose data, where there is a computerized comparison of two or more automated System of Records (SORs). The CMA is to be completed by the end of the Implementation Phase.
- A Contingency or 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 a process or software.
- 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 system 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.

3.5.3 Project Review

The **DDR** is conducted by the IPT subsequent to a PDR to achieve confidence that the individual design components of a business product, 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 base-lined.

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

- System-wide or subsystem-wide design decisions
- Architectural design of the business product
- business product design decisions
- Architectural design of a process or solution item
- Detailed design of a process or solution item

3.5.4 Stage Gate Review

The **PDR** is a formal inspection of the high-level architectural design of a process or software, which is conducted to achieve agreement and confidence that the design satisfies the functional and non-functional requirements and is in conformance with the EA. Overall project status, proposed technical solutions, evolving software products, associated documentation, and capacity estimates are reviewed to

- Determine completeness and consistency with design standards
- Raise and resolve any technical or project-related issues
- Identify and manage project, technical, information security, or business risks affecting continued detailed design and subsequent development, testing, implementation, and operations and maintenance activities

The TRB is responsible for the PDR, one of the Stage Gate Reviews that cannot be delegated.

3.5.5 Deliverables

Design Document with components (Architectural and 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.
CMA (Final)	A 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 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 IV&V) 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.

SORN (Final Draft)	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. The 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.

3.5.6 Exit Criteria

3.5.6.1 Objective

To determine if the design process will create a business product that meets the requirements within a specified project budget and schedule.

3.5.6.2 Phase Specific Exit Criteria

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

3.5.6.3 Generic Exit Criteria

- Variances from baselines have been identified and managed:
  - Cost and schedule variances and scope changes are identified
  - Significant variances are explained
- 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 PMP and component plans have been reviewed and updated appropriately. They include:
  - 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
  - Information Security Approach

3.6 Development Phase (CPIC Control Phase)

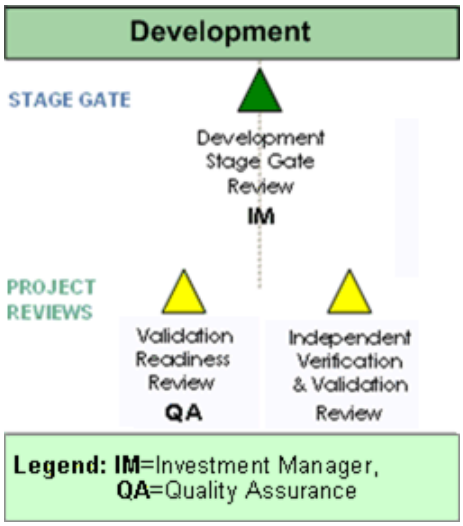

Figure 7: EPLC Development Phase (CPIC Control Phase)

During the Development Phase, the system developer takes the detailed specifications documented in the Design Phase and ensures that all of the individual components of the automated system function correctly and interface properly with other components within the system. As necessary and appropriate, system hardware, networking, and telecommunications equipment, and COTS/GOTS software are 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 and test results documented appropriately. Data conversion and training plans are finalized and user procedures are baselined, while operations, office and maintenance procedures are initially developed. The Development Phase ends with a Stage Gate Review to determine readiness to proceed to the Test Phase.

3.6.1 Responsibilities

PM. The PM is responsible and accountable for the successful execution of the Development Phase. The PM is responsible for leading the staff who accomplishes the Development Phase activities and deliverables.

IPT. The IPT members (regardless of the organization of permanent assignment) are responsible for completion of the DDR.

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

QA. The QA conducts the Validation Readiness Review to determine if the business product is complete and the user documentation is ready for testing.

IM. The IM conducts the Development State Gate Review to provide assurance that the project met testing requirements and should move to the next phase.

3.6.2 Activities

The Development Phase includes several activities that are the responsibility of the developer, including

- Placing the outputs under configuration control and performs change control
- Documenting and resolves problems and non-conformances found in the business product
- Selecting, tailoring, and using those standards, methods, and tools 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.

Development Phase activities also include the following:

- Verify that the software product covering the documented and baselined requirements is in a sufficient state of readiness for integration and formal testing by an assigned test group.
- Prepare the final Test Plan.
- Develop final drafts of the following project deliverables:
  - Business Product
  - Technical Manual and Install Guide, 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 security controls
  - Information Security Risk Assessment, documenting the analysis of 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 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

3.6.3 Project Reviews

The following two project reviews are conducted during the Development Phase:

- The first review, the **Validation Readiness Review (VRR)**, is conducted to provide assurance that the business product about to enter validation testing has completed thorough integration testing during the development of the automated system 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, the **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 to identify problems before they occur and thus avoid loss and minimize the cost of any necessary corrective action. The IV&V Assessment also provides management with an independent perspective on the full scope of project activities, from planning through implementation.

3.6.4 Stage Gate Review

The Development Stage Gate Review evaluates whether the project should proceed to the Test Phase. This Stage Gate Review is conducted by the IM.

3.6.5 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 IV&V) 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.
Technical Manual and Install Guide (Final Draft) Help Desk Support	The Technical Manual and Install Guide 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 NIST) 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 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/repositories. It also includes an identification and description of all configuration items that comprise a specific build or release of the business product.

3.6.6 Exit Criteria

3.6.6.1 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.

3.6.6.2 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

3.6.6.3 Generic Exit Criteria

- Variances from baselines have been identified and managed:
  - Cost and schedule variances and scope changes are identified
  - Significant variances are explained
- 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 PMP and component plans have been reviewed and updated appropriately. They include:
  - 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
  - Information Security Approach

3.7 Test Phase (CPIC Control Phase)

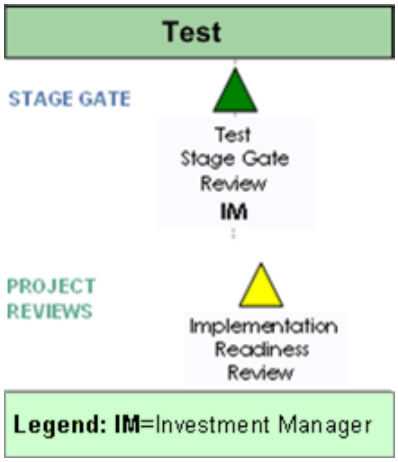

Figure 8: EPLC Test Phase (CPIC Control Phase)

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 on the specific circumstances of the project. The Test Phase ends with a review to determine readiness to proceed to the Implementation Phase.

3.7.1 Responsibilities

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

IPT. The IPT members (regardless of the organization of permanent assignment) are responsible for accomplishing assigned testing tasks as directed by the PM.

PM. The PM is responsible and accountable for the successful execution of the Test Phase. The PM is responsible for leading the team that accomplishes the Test Phase activities and deliverables.

Test and Evaluation Team. The Test and Evaluation Team is responsible for business product testing and documentation of test results.

Users. Selected users may be required to participate in testing.

IM. The IM conducts the Implementation Readiness Review (IRR) and determines if the project is ready to move to the next phase.

3.7.2 Activities

The following activities are completed during the Test Phase:

- The PM, in conjunction with the IM, is responsible for establishing the test team.
- The Test and Evaluation Team is responsible for creating and loading the test database(s) if necessary 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 the test database(s) and execute information security (penetration) 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 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 PM 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.

3.7.3 Project Review

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

3.7.4 Stage Gate Review

The **Test Stage Gate Review** evaluates whether the project should proceed to the Implementation Phase. The IM is responsible for review.

3.7.5 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.

3.7.6 Exit Criteria

3.7.6.1 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.

3.7.6.2 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 supports the decision to move to the Implementation Phase
- Implementation Plan provides detailed information on the move of the business product into production

3.7.6.3 Generic Exit Criteria

- Variances from baselines have been identified and managed:
  - Cost and schedule variances and scope changes are identified
  - Significant variances are explained
- 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 PMP and component plans have been reviewed and updated appropriately. They include:
  - 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
  - Information Security Approach

3.8 Implementation Phase (CPIC Control Phase)

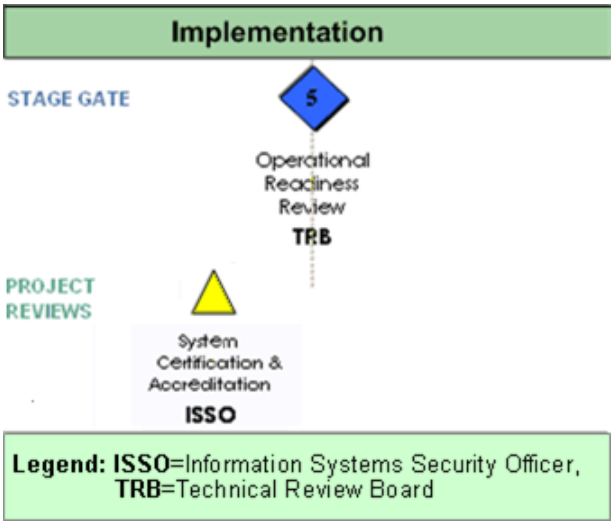

Figure 9: EPLC Implementation Phase (CPIC Control Phase)

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. From an information system security perspective, the final system must be Certified and Accredited (C&A) for 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 O&M Phase, through the **Operational Readiness Review (ORR)** stage gate review.

3.8.1 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.

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.

PM. The PM is responsible for leading the IPT to ensure that the Implementation Phase activities and deliverables are accomplished.

IM. The IM is the approval authority for the final outcome of the PIR and is responsible for authorizing the project to be released into the O&M Phase.

ISSO. The ISSO is responsible for official management decision to authorize the System **C&A**.

IPT. The IPT members (regardless of the organization of permanent assignment) are responsible for accomplishing assigned tasks as directed by the IM.

TRB. The TRB conducts the ORR and determines if the project is ready to be released into the O&M phase.

3.8.2 Activities

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

All users and organizations affected are notified of the implementation. The notification should include this information:

- The schedule of the implementation
- A brief synopsis of the benefits of the new solution
- The difference between the old and new solution
- Responsibilities of end user affected by the implementation
- The process to obtain support, including contact names and phone numbers

During this phase, the documentation from all previous phases is finalized to align it with the delivered system. The PM coordinates these update activities. The documentation associated with the project is archived on the IHS EPLC SharePoint site.

Prior to the ORR, the **Authority to Operate (ATO)** must be obtained by the ISSO, during the System Accreditation review, and if required, the SORN must be published.

Final versions of the following documents are prepared during the Implementation Phase, and are required before the project proceeds to the O&M Phase:

- Business Product
- Project Completion Report
- MOU and SLAs
- Contingency/Disaster Recovery Plan
- O&M Manual
- Information Systems Security Plan
- Information Security Risk Assessment (ISRA)
- Training Plan

- Training Materials
- User Manual

3.8.3 Project Reviews

During the Implementation Phase, the following two project reviews must be performed prior to the ORR:

- The first review, **System Certification**, is the comprehensive evaluation of the management, operational, and technical security controls implemented for an information system to ensure compliance with information security requirements.

  The certification evaluation includes review of the **ISRA**, **System Security Plan (SSP)**, other system life cycle documentation, and any findings from past assessments, reviews 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 or ISRA is 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 ISSO.

- The second review, **System Accreditation**, is the official management decision to authorize operation of an information system. To make an informed decision, the ISSO must have sufficient knowledge and understanding of the current status of the information security programs and 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 on current, credible, comprehensive documentation and test results provided in the System Certification package. The ISSO must explicitly accept or reject any identified residual risks to the operations and assets remaining after the implementation of the prescribed set of information security controls as documented in the SSP or ISRA.

  Ultimately, the ISSO must strike a firm balance between authorizing the operation of information systems necessary to support completion of the business mission, and 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.

3.8.4 Stage Gate Review

The stage gate review for the Implementation phase is the **ORR**, which 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 ORR is one of the Stage Gate reviews that cannot be delegated.

3.8.5 Deliverables

Authority to Operate (ATO) with components (Final) Security Certification & Accreditation Letters Section 508 Product Certifications/Exceptions	An 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.
SORN (Final)	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. The 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.
SLAs and/or MOU	A 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 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.
Technical Manual & Install Guide (Final) Help Desk Support	The Technical Manual and Install Guide 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.
SSP (Final)	The SSP describes managerial, technical and operational security controls (defined by the NIST) 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 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)	An SRA 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/repositories. 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.

3.8.6 Exit Criteria

3.8.6.1 Objective

To verify the operational readiness of the business product for release into the production environment.

3.8.6.2 Phase Specific Exit Criteria

- Business product is ready for production service and notification of the new system is provided to all users and staff who are affected.
- No outstanding concerns among stakeholders regarding implementation.
- Information security and authorization to operate documents are complete and the system is considered certified and accredited.

3.8.6.3 Generic Exit Criteria

- Variances from baselines have been identified and managed:
  - Cost and schedule variances and scope changes are identified
  - Significant variances are explained
- 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 PMP and component plans have been reviewed and updated appropriately. They include:
  - 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
- Information Security Approach

3.9 O&M Phase (CPIC Evaluate Phase)

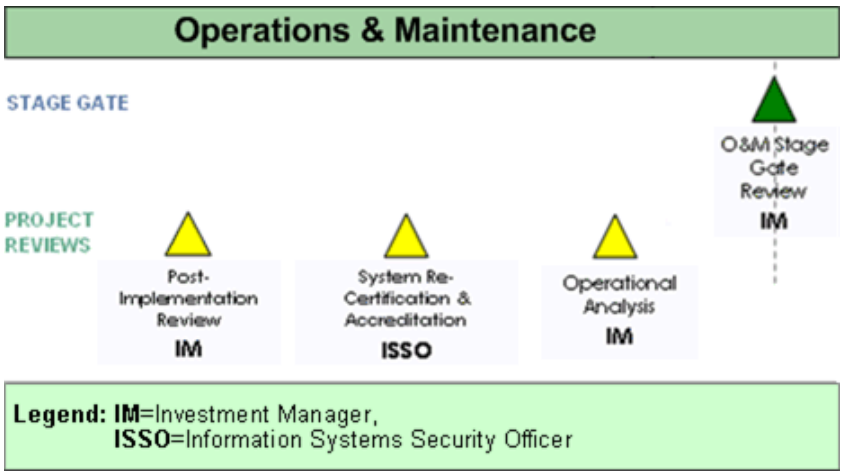

Figure 10: EPLC O&M Phase (CPIC Evaluate Phase)

During the O&M Phase, the C&A system is released into the full-scale production environment for sustained use and operations and maintenance support. In this phase of the EPLC, the project becomes a steady state IT system. Changes and problems with the system may continually be identified and resolved to ensure that the solution meets ongoing functional and non-functional needs.

It is during this phase that the system undergoes a Post Implementation Review (PIR). Periodically, the system will need to be re-certified and re-accredited for continued operation in the production environment. In addition to a periodic C&A, the system will also need to under go a yearly update to the Alternatives Analysis and have an annual Operational Analysis (OA) completed. When the system is no longer needed or will be replaced, a plan for final disposition of the system must be prepared and approved prior to moving into the Disposition Phase.

3.9.1 Responsibilities

IM. The IM is responsible for ensuring that the system is supported through its steady state life cycle. The IM executes plans and procedures for conducting activities and tasks which include:

- Managing communication between the maintenance personnel, business sponsor, and IPT
- Prioritizing tasks
- Reviewing the final PIR report and incorporating findings into the PMO process as lessons learned
- Scheduling the completion of the Alternative Analysis
- Scheduling the completion of the AOA
- Scheduling the completion of the C&A

The IM is also the approval authority to move the system from the O&M Phase to the Disposition Phase.

PM. The PM is responsible for ensuring that the PIR is completed with 6 to18 months from the project's release in the O&M Phase. The PM is released from the project once the PIR is completed.

ITIRB. The ITIRB is responsible for yearly approval of investments into the IHS Exhibit 300s. The ITIRB is also responsible for reviewing investments out of variance with the EVM guidelines. Reviews are conducted of the CAPs that are in place, and updates are made on recommendations by the ITIRB.

CIO. The CIO is responsible for reviewing the PIR. The CIO has the final say on whether the PIR is complete, and whether the outcomes are approved by IHS. In addition, as part of the ITIRB, the CIO is involved in review of investments out of variance of the EVM guidelines. The CIO is also responsible for helping to ensure that the CAP is effective and actually being implemented.

Business Analyst. The business analyst provides business process user support to the system. The business analyst works with the customer to obtain issues, concerns, or improvements that have been identified out in the field. The business analyst is responsible for providing Tier II customer service support, as well as provide information for the development of projects associated with their assigned packages.

Help Desk. Help Desk personnel provide the day-to-day user help for the system. Help Desk personnel should be kept informed of all changes or modifications to the system. Help Desk personnel are contacted by the 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 system.

Users. The user must be able to share the need for improvements or the existence of problems. Some users live with a situation or problem because they feel they must. Users may feel that change will be slow or disruptive, so they create workarounds. A user has the responsibility to report problems, make recommendations for changes to a system, and contribute to OA. The problems and recommendations come to Operations through contacts with the Help Desk and User Support personnel.

Program Developer. The Program Developer interprets user requirements, designs, and writes the code for specialized programs. User changes, improvements, and enhancements may be discussed in **Joint Application Design (JAD)** sessions. The Program Developer also 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 system. 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.

Database Administrator (DBA). The DBA performs tasks which ensure that accurate and valid data are entered into the system. Sometimes this person creates the information systems database, maintains the security of the database, and develops plans for disaster recovery. The DBA may be called upon to create queries and reports for a variety of user requests. DBA responsibilities include maintaining the database data dictionary, which provides a description of each field in the database, the field characteristics, and the data maintained in the field.

ISSO. The ISSO is required 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 security posture of the system. The ISSO is responsible for official management decision to authorize the system recertification and reaccreditation.

Records Officer. The records officer is responsible for determining how records and record-keeping will be managed over the life cycle of the business product.

CPIC Manager. The CPIC Manager is responsible for ensuring that monthly EV reporting is reviewed for variances and entered into the PMT. The CPIC Manager is responsible for reviewing the outcome of the PIR and will incorporate improvements to the CPIC process that are found during the review. During the O&M phase, the CPIC Manager is responsible for coordination with the IM to ensure that the Operational Analysis is within acceptable limits, the Annual Alternative Analysis is updated yearly, and a C&A is completed periodically. The CPIC Manager is responsible for ensuring that the yearly Exhibit 53 and 300s are completed.

3.9.2 Activities

Operations support is an integral part of the day-to-day operation of a system. The Technical Manual and Install Guide are completed in the Implementation Phase. The 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 running and available during the defined hours of operation.
- Implement nonemergency requests during scheduled outages, as prescribed in the Technical Manual and Install Guide.
- Ensure all processes, manual and automated, are documented in the operating procedures. These processes should comply with the system documentation.
- Acquire and store supplies; for example, paper, toner, tapes, removable disks.
- Perform and test backups (day-to-day protection, contingency).
- Perform the physical security functions, including ensuring adequate uninterruptible power supply, and ensuring that personnel have proper clearances and proper access privileges.
- Ensure contingency planning for disaster recovery is current, tested, and funded.
- Ensure users are trained on current 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 security controls and performance statistics, report the results, and escalate problems when they occur.

In the case of software development, database 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 administration volume backups. The backup and recovery process of the databases should be performed as a database administration task. A checklist of database 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 corrections
- Installing, configuring, upgrading and maintaining database(s), which includes updating processes, data flows, and objects (usually shown in diagrams)
- Developing and performing database backup and recovery routines for data integrity and recoverability
- Ensuring all processes are documented properly
- Developing and maintaining a performance and tuning plan for online process and databases
- Performing configuration, security, and design 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

The RD for the system 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 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 capabilities.

At the beginning of this phase, any outstanding POA&Ms must be completed. Throughout the phase, continuous security monitoring of selected controls must be conducted. In addition, periodic reviews of controls, periodic reevaluation of information categorization, and recertifications and revision of risk assessments and information security plans, and recertification and reauthorizations to process (reaccreditation) 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 IM must be sure that the information security operating procedures are updated accordingly.

Review and update system documentation including the operations from the previous phases. In particular, the Technical and User Manuals, Install Guide, 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.

Periodically, a Continued Authority to Operate must be prepared to assure that risks are assessed and the approving authority explicitly identifies risks to IHS operations, assets, and individuals.

System changes may also create new privacy risks. For such changes, OMB requires that 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 the system. 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 system.

3.9.3 Steady State Reviews

There are four steady state reviews that are conducted in the O&M Phase.

- The first review, the **PIR,** is conducted of the completed business product that was released into the production environment, after a period of sustained operation (approximately 6 to 18 months or after at least one full processing and reporting cycle has been completed and all users have been trained and are comfortable with the operation), 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 expectations of the business sponsor)
  - Examine the efficacy of all elements of the working business solution to see if further improvements can be made to optimize the benefit delivered
  - Learn lessons from the project that can be used to improve future project work and add to the improvement to the CPIC process

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 must be able to make recommendations for upgrades to hardware, architecture, and streamlining processes. These modification requests may be addressed in the RD, may take the form of a change package, and may require justification and cost benefits analysis for approval by a review board. The PM is responsible for ensuring that the PIR is completed, along with the business sponsor who is to review the findings, and the CIO or designee who is responsible for approving the outcome of the PIR. The PIR will be performed on projects over $100,000.00 or projects that are determined by the CIO or IM to be a high level of risk.

- The second review, **System Recertification**, is the periodic comprehensive re-evaluation of the management, operational, and technical security controls implemented for an information system 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 security controls. Information security controls typically become outdated and less effective as threats and vulnerabilities evolve. The objective of the System Recertification is to ensure that system certification is an on-going process, and that information security is managed throughout the life of the system.
- The third review, **System Reaccreditation**, is the official management decision to authorize continued operation of an information system after acceptable System Recertification and any necessary adjustments have been completed.
- The fourth review, **OA**, is performed annually 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 OA ultimately determines whether the system should continue, be modified, or terminated.

3.9.4 Stage Gate Review

The **O&M Stage Gate Review** evaluates whether the system should proceed to the Disposition Phase. The IM is the approval authority for this Stage Gate Review.

3.9.5 Deliverables

Annual Operational Analysis (AOA) (Final)	The 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.
PIA	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.
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.

3.9.6 Exit Criteria

3.9.6.1 Objective

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

3.9.6.2 Phase Specific Exit Criteria

- Annual review of the operation provides a framework for deciding what enhancements or modifications are needed, or whether the system should be replaced or disposed
- Documentation and the training programs include input from stakeholders

3.9.6.3 Generic Exit Criteria

- Variances from baselines have been identified and managed:
  - Cost and schedule variances and scope changes are identified
  - Significant variances are explained
- 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 PMP and component plans have been reviewed and updated appropriately. They include:
  - 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
  - Information Security Approach

3.10 Disposition Phase (CPIC Evaluate Phase)

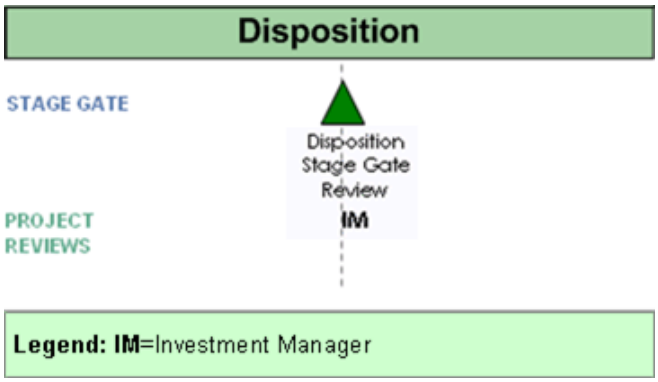

Figure 11: EPLC Disposition Phase (CPIC Evaluate Phase)

During the Disposition Phase, the operation of an IT system is formally ended in accordance with organization needs and pertinent laws and regulations. The system is retired or disposed, based on the formal Disposition Plan approved during the O&M Phase. The disposition activities ensure the orderly termination of the system and preservation of vital information, 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 system, so that the data is effectively migrated to another solution or archived in accordance with applicable records management regulations and policies for potential future access.

3.11 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 IT project no longer continues to meet business requirements and may be orderly shutdown according to the disposition plan developed.

IM. The IM ensures that all aspects of the Disposition Plan are followed. The Disposition Plan should outline all roles and responsibilities for all actions related to closing down and archiving 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 system. Technical Support personnel or Operators may perform the cutoff of user 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 system 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, and would also be involved with identifying and migrating data to a new or replacement system.

User Services (Training and Help Desk). 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, User Services may assist with the retraining of users to facilitate the transfer to a new or replacement system.

Operations (turn off systems, start tasks, backup, etc.). Operations personnel interface with the computer facility that hosts the system 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. Operations 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 application systems. 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 users. Any users that only use the application should be removed from the system, while others that use other applications as well as this one may still need access to the overall system, but not to the application being shutdown. If there is another application that is taking the place of this application, the security managers should coordinate with the new security managers.

CPIC Manager. The CPIC Manager ensures that Lessons Learned have been prepared so that other IHS projects can benefit from them, and ensures that all documentation is completed and archived.

3.11.1 Activities

The tasks and activities required are dependent on the nature of the system. 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 and when the retirement of the system will be conducted
- The system retirement date
- Software 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 are archived or transferred; the software components must be transferred to the new system, or if that is not feasible, decommissioned appropriately.

The documentation that resulted from the development of the application or system must be archived, so it can be referenced, if needed, at a later date.

Follow the Disposition Plan for the orderly breakdown of the system, 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 dispose properly all obsolete hardware components.

3.11.2 Stage Gate Review

A Disposition Review is conducted by the IM to ensure that a system has been completely and appropriately disposed, thereby ending the life cycle of the system.

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

3.11.3 Deliverables

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

3.11.4 Exit Criteria

3.11.4.1 Objective

To have an orderly shutdown of the system 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.

3.11.4.2 Generic Exit Criteria

- The PMP and component plans have been reviewed and updated appropriately. They include:
  - 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
  - Information Security Approach
  - IHS EPLC Workgroup Participants

4. IHS EPLC Workgroup Participants

Name	Phone	E-Mail
Carl Gervais	(505) 248-4197	Carl.Gervais@ihs.gov
Michelle Riedel	(505) 248-4446	Michelle.Riedel@ihs.gov

5. Appendix A: Deliverables Descriptions

This appendix includes all of the required deliverables for projects that fall under HHS level review. The EPLC Framework gives some flexibility to the individual PMOs, to determine levels of rigor and the required documentation based on the size of projects. For guidelines, see Section 2.11 on tailoring the EPLC Framework.

5.1 Initiation Phase

5.1.1 BNS (Final)

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

5.2 Concept Phase

5.2.1 Business Case (Final)

The business case is a documented, structured proposal for business improvement that is prepared to facilitate a selection decision for a proposed project by organizational decision makers. The business case describes the reasons and justification for the 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.

5.2.2 Project Charter

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 PM with the authority to apply up to a certain level of organizational resources to project activities.

5.3 Planning Phase

5.3.1 PMP with Components (Final)

- Risk Management
- Acquisition Strategy
- Change Management

- Configuration Management
- Project Categorization
- Requirements Management
- Communications Plan
- WBS/Project Schedule
- IV&V Planning
- Quality Assurance
- Records Management
- Staff Development Plan
- Information Security Approach

The 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.

5.3.2 PIA (Final)

The assessment required by the Privacy Act and/or E-Government Act of 2002, to conduct assessments on investments before developing or procuring IT that collects, maintains, or disseminates personal information in identifiable form, based on the initial FIP 199 categorization and the identification of the need or potential to collect Privacy Act data/information.

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 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.

5.3.3 PPA (Final)

- Deliverable and Stage Gate Waivers
- Authorization to Proceed

The 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 project, including the expected level of detail to be provided.

5.4 Requirements Analysis Phase

5.4.1 RD with Components (Final)

- Functional and Nonfunctional Requirements
- Requirements Traceability Matrix (RTM)
- Business Process Model (BPM) Expansion
- Logical Data Model

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

5.5 Design Phase

5.5.1 Design Document with Components (Architectural and 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.

5.5.2 CMA (Final)

A 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 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.

5.5.3 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 IV&V) 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.

5.5.4 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 do not 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.

5.5.5 SORN (Final Draft)

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. The 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.

5.6 Development Phase

5.6.1 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 IV&V) 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.

5.6.2 Technical Manual and Install Guide (Final Draft)

- Help Desk Support

The Technical Manual and Install Guide 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.

5.6.3 SSP (Final Draft)

The SSP describes managerial, technical, and operational security controls (defined by the NIST) that are designed and implemented within the system.

5.6.4 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 users, operators, administrators, and support staff who will use, operate, and/or otherwise support the solution.

5.6.5 Training Materials (Final Draft)

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.

5.6.6 SRA (Final Draft)

An SRA will document the analysis of the informational 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 security controls for the information system.

5.6.7 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.

5.6.8 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 repositories. It also includes an identification and description of all configuration items that comprise a specific build or release of the business product.

5.7 Test

5.7.1 Implementation Plan (Final)

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

5.7.2 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.

5.8 Implementation Phase

5.8.1 ATO with components (Final)

- Information Security Certification and Accreditation Letters
- Section 508 Product Certifications/Exceptions

An ATO is a formal declaration by the ISSO 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.

5.8.2 SORN (Final)

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. The 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.

5.8.3 SLAs and/or MOUs

A SLA 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 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.

5.8.4 Technical Manual and Install Guide (Final)

- Help Desk Support

The Technical Manual and Install Guide 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.

5.8.5 SSP (Final)

The SSP describes managerial, technical, and operational security controls (defined by the NIST) that are designed and implemented within the system.

5.8.6 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 users, operators, administrators, and support staff who will use, operate, and/or otherwise support the solution.

5.8.7 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.

5.8.8 SRA (Final)

An SRA 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 security controls for the information system.

5.8.9 User Manual (Final)

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

5.8.10 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 repositories. It also includes an identification and description of all configuration items that comprise a specific build or release of the business product.

5.8.11 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.

5.8.12 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 do not 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.

5.9 O&M

5.9.1 AOA (Final)

The 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.

5.9.2 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.

5.10 Disposition Phase

5.10.1 Project Archives (Final)

Project archives preserve vital information, including both documentation of project execution and the data from the production system.

5.11 Annual

5.11.1 Continued ATO

Resulting from a periodic review of an operating business product, a Continued ATO is a formal declaration by an ISSO that a business product is approved to continue to operate at an acceptable level of risk in the designated production environment.

5.12 Recurring or As Needed

5.12.1 Data Use Agreement (DUA)

A DUA is a legally 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, security safeguards, and the federal agency's data use policies and procedures. The DUA serves as both a means of informing data 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 SOR be in effect, which allows for the disclosure of the data being used.

5.12.2 IV&V Reports

IV&V Reports document the findings obtained during a specific IV&V Assessment that is conducted by an independent third party.

5.12.3 PIA

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.

5.13 Periodically, as Established in Project Plan

5.13.1 Integrated Baseline Documentation

PMB documents, such as the WBS, the WBS Dictionary, the Responsibility Assignment Matrix, project schedules, Control Account Plans, and Work Authorization Document. For a description of these documents and the IBR process and procedures, see HHS-OCIO-2007-0001.001, *HHS OCIO IT Earned Value Management Processes and Procedures*, June 11, 2007.

5.13.2 CPR, or acceptable equivalent, if full EVM standards compliance is not required

The CPR, a periodic EV 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 IHS IT Investment team, and includes explanations for cost and schedule variances that have exceeded thresholds and descriptions of contractor plans to resolve variance causes. For a description of this document and how it is used, see HHS-OCIO-2007-0001.001, *HHS OCIO IT Earned Value Management Processes and Procedures,* June 11, 2007. Guidelines for tailoring the CPR are provided in Section 8.5-2, of the *Earned Value Management Implementation Guide* (EVMIG).

5.13.3 CFSR, or acceptable equivalent, if full EVM standards compliance is not required

A status report that provides investment and PMs 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 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 IM or PM requires only the minimum data necessary for effective management control. The CO 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.

5.13.4 PMO Tailoring Document

The PMO Tailoring document defines how each investment determines which projects can be tailored, within the EPLC guidelines.

5.13.5 Project Schedule (Updated)

The project schedule is developed so that tasks and milestones are clearly defined. It is updated regularly to identify elements that are behind as well as those ahead of schedule. The project schedule maps directly to the WBS, providing the PMO with a single point of reference for all activities. Contract DID elements for a project schedule are provided in HHS-OCIO-2007-0001.001, *HHS OCIO IT Earned Value Management Processes and Procedures*, June 11, 2007.

5.13.6 Periodic Project 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.

5.13.7 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.

6. Appendix B: References

6.1 Acquisition

Acquisition Strategy Guidance, July 29, 2009:
http://dhhs.gov/asfr/ogapa/acquisition/index.html

6.2 CPIC

HHS-OCIO Pilot Policy for Information Technology Investment Performance Baseline Management, November 3, 2009:
http://www.hhs.gov/ocio/policy/#Capital

HHS OCIO Policy for IT Capital Planning and Investment Control, December 30, 2005:
http://www.hhs.gov/ocio/policy/

6.3 EVM

OMB Memorandum 05-23, Improving Information Technology (IT) Project Planning and Execution, August 5, 2005:
http://www.whitehouse.gov/omb/memoranda/fy2005/m05-23.pdf

Acquisition Policy Memorandum, October 10, 2008:
http://dhhs.gov/asfr/ogapa/acquisition/index.html

6.4 EA

HHS OCIO IT Policy for EA, August 7, 2008:
http://www.hhs.gov/ocio/policy/#Enterprise

6.5 IRM

OMB Circular A-11, Preparation, Submission and Execution of the Budget:
http://www.whitehouse.gov/omb/circulars_a11_current_year_a11_toc/

OMB Circular A-127, Financial Management Systems:
http://www.whitehouse.gov/omb/rewrite/circulars/a127/a127.html

OMB Circular A-130, Management of Federal Information Resources:
http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

HHS Policy for Section 508 Electronic and Information Technology, January 2005:
http://www.hhs.gov/od/Final_Section_508_Policy.html

6.6 Finance

GAO Cost Estimating Guide, March 2009:
http://gao.gov/new.items/d093sp.pdf

6.7 Records Management

HHS OCIO Policy for Records Management, September 15, 2005:
http://www.hhs.gov/ocio/policy/2005-0002.002.html

HHS OCIO Policy for Electronic Records Management, September 15, 2005:
http://www.hhs.gov/ocio/policy/2005-0001.html#4

6.8 Security and Privacy

HHS OCIO Information Security Program Policy, December 15, 2004:
http://www.hhs.gov/ocio/policy/

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)

6.9 Web Sites

HHS, Office of the Chief Information Officer (OCIO)

http://www.hhs.gov/ocio/policy/index.html

HHS, Office of Disability

http://www.hhs.gov/od/index.html

IHS CPIC

http://www.ihs.gov/cio/cpic

OMB

http://www.whitehouse.gov/omb/circulars/

7. Appendix C: Abbreviations/Acronyms

Abbreviation /Acronym	Term
ASR	Architecture and Security Review
ATO	Authority to Operate
BNS	Business Needs Statement
C&A	Certification & Accreditation
CCA	Clinger Cohen Act, 1996
CAP	Corrective Action Plan
CIO	Chief Information Officer
CMA	Computer Match Agreement
CO	Contracting Officer
COTS	Commercial Off-the-Shelf
CP	Critical Partner
CPIC	Capital Planning and Investment Control
CPR	Contract Performance Support
DBA	Database Administrator
DDR	Detailed Design Review
DME	Development, Modernization, and Enhancement
EA	Enterprise Architecture or Enterprise Architect
EPLC	Enterprise Performance Life Cycle
EVM	Earned Value Management
GOTS	Government Off-the-Shelf
IBR	Integrated Baseline Review
IM	Investment Manager
IPT	Integrated Project Team
IRR	Implementation Readiness Review
ISRA	Information Security Risk Assessment
ISSO	Information Systems Security Officer
IT	Information Technology
ITIRB	Information Technology Investment Review Board

Abbreviation /Acronym	Term
IV&V	Independent Verification & Validation
JAD	Joint Application Design
MOU	Memorandum of Understanding
OA	Operational Analysis
ORR	Operational Readiness Review
PBM	Performance Baseline Management
PBR	Project Baseline Review
PDR	Preliminary Design Review
PIA	Privacy Impact Assessment
PIR	Post-Implementation Review
PM	Project Manager
PMB	Project Management Baseline
PMO	Program Management Office
PMP	Project Management Plan
POA&M	Plan of Action and Milestones
PPA	Project Process Agreement
PSR	Project Selection Review
RD	Requirements Document
ROM	Rough Order of Magnitude
RTM	Requirements Traceability Matrix
SLA	Service Level Agreement(s)
SOR	System of Records
SORN	System of Records Notice
SSP	System Security Plan
ST&E	Security Test and Evaluation
VRR	Validation Readiness Review
WBS	Work Breakdown Structure

Glossary

A

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.

Architecture and Security Review (ASR)

The ASR is completed by the TRB during the Concept Phase of the EPLC Framework. The ASR is completed to determine if the business case supports a sound business product that will work within the system structure of IHS. The business case is scored and if the score meets the approval criteria then the business case moves on to the PSR.

B

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 project is intended to accomplish, expressed in quantitative terms, if possible.

Business sponsor

The executive in charge of the organization, who serves as the primary customer and advocate for an IT project. The business sponsor 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.

C

CPIC

The CPIC process is an integrated, structured methodology to managing IT projects, which ensures that projects within the IT investments align with the IHS mission, and support business needs while minimizing risks and maximizing returns throughout the project's life cycle. CPIC uses a systematic selection, control, and continual evaluation process to ensure that projects in an investment support the IHS' mission and business needs.

C&A

C&A is composed of those activities and processes required to maintain security of information systems, periodically review the 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 security process is where the system staff (outlined in the security documentation) performs the day-to-day functions required to maintain an appropriate level of security to protect the system. This phase is ongoing while the system is in operation.

CIO

The Office of the CIO 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.

COTS

"COTS" refers 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.

CO

The CO 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 CO acting within limits of their authority as delegated by the CO. The CO and/or its representative is accountable for preparing solicitation documents with technical support from the PM 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.

CP

CPs are functional managers in EA, Information Security, Acquisition Management, Finance, Budget, and Human Resources that participate in 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.

D

DDR

The DDR is completed by the CPs assigned to the project in the Design Phase of the EPLC Framework. The outcome of the review is to determine if the design elements of the business product are fully defined and documented. The project is considered baselined, if the approval of the DDR is positive and the project will move forward to the Development Phase.

E

EVM

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

EA

EA is a strategic information asset base that 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. EA includes baseline architecture, target architecture, and a sequencing plan.

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 IHS 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 IHS policies and standards.

Evaluate Phase

This phase of the CPIC process involves comparing actual to expected results once a project 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.

F

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 PMP. A functional requirement is a tangible service, or function, that the business product must provide and is a nontechnical requirement. See also Nonfunctional Requirements.

G

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 preestablished functionality and little or no customization.

I

IRR

The IRR is conducted by the IM at the end of the Test Phase of the EPLC Framework. The main objective of the IRR is to ensure that the finalized business product is ready for implementation. If the IM determines that the business product is complete, then it is ready for implementation.

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.

ISRA

During the Implementation phase of the EPLC Framework, the ISRA considers the risk of incorporating a new business product into a current system by determining if there is adequate security to minimize the effects of threats, vulnerabilities, and the effectiveness of current or proposed safeguards. The ISRA is approved by the ISSO.

IT

IT, as defined by the CCA 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.

ITIRB

The ITIRB is a cross-functional executive review committee responsible for overseeing the management of the IHS IT portfolio, approving and prioritizing IT projects to best achieve IHS strategic goals and objectives. The ITIRB shall ensure that the IHS IT investment portfolio is of the highest quality and meets the business needs of IHS 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 projects 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 IT 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.

IPT

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

IM

The IM is responsible for the planning and executing of the investment's projects to ensure that they achieve approved baselines. The IM may or may not be a subject matter expert in the business area supported by the project.

IT Governance Organization

The IT governance organization at IHS is responsible for ensuring that projects are technically sound, follows established project management practices, and meets the business sponsor's needs. Components of the IT governance organization are the ITIRB, the TRB, the CIO, and CPIC Manager.

J

JAD

A JAD session is a structured meeting that evolves key participants of a business product project. A major outcome of the JAD is to collect business requirements and work out project issues during the development of the new business product. During these sessions the business product design is tested and problems debugged.

N

Nonfunctional Requirements

Nonfunctional 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 nonfunctional requirements are reliability, scalability, accessibility, performance, availability, and cost. Other terms for non-functional requirements are "constraints," "quality attributes," and "quality of service requirements." Nonfunctional requirements also specify the laws, regulations, and standards with which the business product must comply.

O

ORR

The 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 ORR is performed during the Implementation Phase of the EPLC Framework by the TRB.

P

PBM

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.

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 resource
  - Identifying those risks deemed acceptable that will not be mitigated
  - Informing decision makers

Post Implementation Review (PIR)

A PIR is performed 6 to 18 months after the business product has been implemented to ascertain the degree of success that the outcome satisfies the business sponsor and to determine lessons learned that can be incorporated into the CPIC process for continuous improvement. The PIR is conducted during the O&M Phase of the EPLC Framework. The IM is responsible for ensuring that the PIR is completed within 6 to 18 months of first operation.

PDR

The PDR is a formal inspection of the high-level architectural design of a process or software, which is conducted to achieve agreement and confidence that the design satisfies the functional and non-functional requirements and is in conformance with the EA. The PDR is performed during the Design Phase of the EPLC Framework by the TRB.

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.

PBR

The PBR is performed during the Planning Phase of the EPLC Framework by the ITIRB. The outcome of this review is to obtain management approval of the scope, cost and schedule of the proposed project.

PMB

The PMB outlines how the approved integrated scope-schedule-cost plan for project work is measured for successful performance. The time-phased budget plan against which project performance is measured.

PM

The PM is responsible for project performance in relation to approved cost, schedule, and performance baselines. The PM maintains information project status, control, performance, risk, corrective action, and outlook. This person is accountable to the business sponsor for meeting business requirements and to IT governance for meeting IT project management requirements. The PM shall develop the business case in conjunction with the business sponsor 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 IHS policies that apply to IT projects. PMs shall be responsible for timely reporting of significant variances from approved baselines and providing CAPs or re-baselining proposals as appropriate.

PSR

The PSR is the Stage Gate Review performed at the end of the Concept Phase of the EPLC Framework. The outcome of the review is a final approval to commit necessary resources to fund the proposed business product. The CIO or the ITIRB are the approval authority based on the dollar amount of the business case.

R

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 a 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.

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.

S

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.

Security Test and Evaluation (ST&E)

The 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. This review is completed during the Implementation Phase of the EPLC Framework.

Select Phase

This phase of the CPIC process ensures that IT project are chosen that best support the Agency's mission and align with IHS' approach to EA.

Solution

A comprehensive architectural response to a business problem. Solutions address all layers of the EA–strategy, business, data, applications, and technology/security.

Stage Gate

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

SOR

The Privacy Act defines an 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

SSP

The SSP provides guidelines to establish system security and privacy requirements. It identifies the current information security environment, establishes scope and objectives, and outlines the activities required for information security implementation. The SSP describes the system's security requirements, the controls in place or planned, and roles/responsibilities of all authorized individuals who use the system.

V

Validation Readiness Review (VRR)

The VRR is conducted during the Development Phase of the EPLC Frame work. The main outcome of the VRR is to provide assurance that the business product is ready for turnover to the formal, controlled test environment where validation testing will be conducted. QA performs this review.

8. Contact Information

If you have any questions or comments regarding this document, please contact the OIT Help Desk at IHS:

Phone: 505.248.4371 or 888.830.7280

Fax: 505.248.4363

Web: http://www.ihs.gov/GeneralWeb/HelpCenter/Helpdesk/index.cfm

E-Mail: support@ihs.gov