



ADMINISTRATIVE COMMUNICATIONS SYSTEM U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL DIRECTIVE

OCIO: 1-106

Page 1 of 40 (07/16/2010) (Original Date)
(12/09/2016) (Re-certified Date)

Distribution:
All Department of Education
Employees

Signed by: Winona H. Varnon
Principal Deputy Assistant
Secretary for Management
Delegated the Authority to Perform
the Functions and Duties of the
Assistant Secretary for Management

Lifecycle Management (LCM) Framework

Table of Contents

I.	Introduction	2
II.	Purpose	2
III.	Policy	2
IV.	Authorization.....	2
V.	Applicability.....	3
VI.	Definitions	3
VII.	Responsibilities	4
VIII.	The Framework.....	5
	APPENDIX A: Acronym List.....	26
	APPENDIX C: Department Document References	32
	APPENDIX D: Tailored Project Guide Template.....	34
	APPENDIX E: Incremental Development.....	36
	APPENDIX F: Open Data.....	38
	APPENDIX G: LCM Framework 2.0 Graphic.....	1

For technical questions concerning information found in this Administrative Communications System (ACS) document, please contact James Hicks at 202-245-8226 or <mailto:James.Hicks@ed.gov>.

This ACS document supersedes OCIO:1-106 "Lifecycle Management (LCM) Framework" dated 07/16/2010. Added Federal Source Code. Re-certified on 12/09/2016

I. Introduction

The U.S. Department of Education (Department) LCM Framework (Framework) describes the management process that is to be used by Department components engaged in the acquisition and development of information technology (IT) solutions. The Framework describes the key activities, deliverables and reviews an IT solution moves through over the course of its lifecycle. The Framework is designed to coordinate and integrate Department processes that impact IT solutions acquisition and development.

II. Purpose

This directive sets forth the Department's policy for using the Department's LCM Framework to provide the foundation for the implementation of standards, processes and procedures for acquiring and developing IT solutions. All LCM-related processes will use the Framework to align and streamline their processes to support effective oversight and management of IT solution acquisition and development.

III. Policy

This directive applies to the development, acquisition, implementation, maintenance and disposal of IT solutions regardless of cost, complexity and time constraints.

IV. Authorization

A. The following are links to Federal regulations and policies that support the Department's use of a LCM approach:

- 1 [Information Technology Management Reform Act of 1996 \(Clinger-Cohen Act\)](#)
- 2 Office of Management and Budget (OMB) Circular A-123 Management's Responsibility for Internal Control
- 3 [OMB Circular A-130 Management of Federal Information Resources](#)
- 4 OMB Circular A-131(Revised) Value Engineering
- 5 [U.S. Department of Education Investment Review Board Charter](#)
- 6 [OMB Memorandum M-13-13 Open Data Policy](#)

- 7 Federal Information Technology Acquisition Reform Act (FITARA) (Part of Public Law 113 – 291, Division A, Title VIII, Subtitle D, Sections 831 – 837)
 - 8 OMB Memorandum M-15-14 (FITARA Implementation Guide)
 - 9 OMB Memorandum M-16-21 (Federal Source Code Policy)
- B. The Department's Office of the Chief Information Officer (OCIO) will own and maintain the Framework; communicate it to the Principal Offices; and provide support for its implementation.

V. Applicability

This directive applies to all Department employees and contractors engaged in the development, acquisition, implementation, maintenance and disposal of IT solutions. Nothing in this directive is meant to excuse or exempt contractors from satisfying all requirements of their contracts.

VI. Definitions

The following are key definitions related to this directive.

- A. **Lifecycle Management (LCM)** is the coordination of activities associated with the documentation and implementation of IT solutions from conception through disposal. Such activities include: defining requirements, designing, building, testing, implementing, establishing operations and disposing of systems.
- B. **Framework** is a structured approach of required stages, key activities and core deliverables that provides a foundation for aligning existing interrelated processes within the Department, regardless of system lifecycle methodology employed.
- C. **Planning and Investment Review Working Group (PIRWG)** assess the effectiveness of the Department's IT investment management process and provides recommendations through the CIO to the Investment Review Board (IRB) for refining and improving the process. The PIRWG is comprised of 2 groups; PIRWG (Core) which consists of voting members and PIRWG (Expanded) which consists of the voting members and those members which use to comprise the Enterprise Architecture Advisory Committee (EAAC).
- D. **Enterprise Architecture Review Board (EARB)** is the Department's governance body that performs technical reviews to assess (1) EA standards compliance, (2) technical design, and (3) opportunities for service and technical component standards reuse.

- E. **Change Advisory Board (CAB)** is the Department's governance body that reviews, approves and implements change requests for the EDUCATE IT Infrastructure.
- F. **IT Solution** pertains to automated information systems, software applications, and manual processes.
- G. **Stage** is a definitive section of the lifecycle that indicates a specific purpose or goal has been achieved. The end of each stage is marked by a "Stage Gate," noting the exit from one stage and entry into the next.
- H. **Key Activity** is a required task, procedure or process.
- I. **Core Deliverable** is a required document that must be completed and approved by the end of a particular stage of the lifecycle.
- J. **Exit /Entry Criteria** refer to requirements that must be completed and approved in order to exit one stage and enter the next.
- K. **Stage Gate Review** is the integration of various business and technical reviews performed primarily by the EARB that ensures core deliverables (and any additional deliverables) required for that stage have been completed.
- L. **Incremental Development** is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery, a time-boxed iterative approach, and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development cycle.
- M. **Open Data** is managing information as an asset throughout its life cycle to promote openness and interoperability, and properly safeguard systems and information.
- N. **Value Engineering(VE)** is the methodology for analyzing functions of an item or process to determine "best value," or the best relationship between worth and cost, where "best value" is represented by an item or process that consistently performs the required basic function at the lowest life-cycle cost while maintaining acceptable levels of performance and quality. The key areas to apply VE are acquisition strategy and project management.

VII. Responsibilities

The following are staff responsibilities associated with this directive:

- A. *The Chief Information Officer (CIO)*** is responsible for authorizing the development and implementation of an LCM Framework and IT Governance Process that ensures Department IT Solutions Development is managed in accordance with Department standards and procedures. The CIO monitors the execution of the IT Governance process, approving the decisions of the IT governance bodies, and adjudicating disputes that may arise between the IT governance bodies and Project Managers.
- B. *Enterprise Architecture staff*** is responsible for developing, implementing and maintaining the LCM Framework and IT Governance process on behalf of the CIO and for reviewing IT investments for adherence to the Department's enterprise architecture current and future state vision.
- C. *Project Managers*** are responsible for creating deliverables and ensuring that business and technical reviews are executed and required deliverables are completed on time and within budget. They are also responsible for:
1. Managing the day-to-day operations of the Department's IT solutions,
 2. Identifying areas of cost reduction and quality improvement, and
 3. Applying principles of VE for appropriate projects¹ throughout all applicable life cycle stages² as discussed in this Framework.
- D. *Deliverable Reviewers*** are responsible for reviewing and approving the content of required deliverables. Deliverable Reviewers are staff from various business and technical areas (e.g. Investment Acquisition Management Team (IAMT), Contracts and Acquisition Management (CAM)) with specific knowledge of the requirement areas.
- E. *EARB Members*** are responsible for authorizing a project's progress into the next LCM stage based on the completion of reviews and deliverables required by the preceding LCM stage.

VIII. The Framework

The Framework is a structured approach of required stages, key activities and core deliverables that provides a foundation for aligning existing interrelated processes such as, the OCIO's IT Governance and Capital Planning and Investment Control processes, OCFO's Acquisition process and processes associated with project management, used in delivering IT solutions. The purpose of the Framework is to help existing Department processes work together more efficiently. It is not intended to reengineer existing processes, but

¹ New projects, existing projects, major acquisitions costing at least \$5 million that were not granted a VE waiver

² Primarily Construction and Validation, Implementation, and Operations and Maintenance

rather, to provide a foundation and frame of reference for aligning them. In addition, Incremental Development should be used whenever and wherever as applicable ([Appendix E](#)).

Staff from various processes related to LCM will be responsible for determining the particulars of how their processes will work within the Framework. In aligning processes, the Framework provides the basis for executing enforcement mechanisms already contained in those processes. Through a stage gate review, the Framework focuses on results obtained at the end of each stage to assist investment oversight, product quality and compliance to Department directives and regulations. However, these stage gate reviews do not represent an additional enforcement layer, but rather are a means to facilitate and coordinate business and technical reviews for each stage already present in existing processes.

The Framework is flexible concerning core deliverable length and the addition of deliverables to accommodate solutions with varying cost, complexity and time constraints. All Framework activities and core deliverables are required for Non-Major IT projects³; however, the total documentation for a very small project might amount to just one or two pages, for example. Additionally, project staff should rely on existing Department guidance documents and staff expertise relevant to small projects to determine how those projects should align and work within the Framework.

By using this Framework directive, the Department will realize the following benefits:

- A single reference to inform Department employees of expectations, activities and core deliverables associated with IT solutions acquisition and development.
- Improved product quality and reduced rework by establishing standard business and technical reviews throughout the development of IT solutions.
- Improved project management through VE for appropriate projects in all applicable life cycle stages as discussed in this Framework to maximize project's value to the Department for a given level of cost or minimize cost for any acceptable level of outcome.
- Improved oversight by encouraging and enabling integrated and coordinated reviews.

³ Please refer to [Investment Management Process Guide](#) for a description of Non-Major IT. Also see ACS Directive OCIO:3-108 referenced in Appendix D of this directive.

- Improved performance management of projects through review of project cost and schedule and implementation of VE methodology where necessary through all applicable stages in alignment with the Department's mission or objectives.
- A mechanism by which projects can define their deliverables against the scope of the IT solution.
- Improved quality of information used in the IT investment process.

The Framework is comprised of six stages and 1 pre-stage:

1. Pre-Vision;
2. Vision;
3. Definition;
4. Construction and Validation;
5. Implementation;
6. Operations and Maintenance; and,
7. Retirement.

Each stage consists of required key activities and core deliverables that must be completed for entry into the next stage. A stage gate review is conducted by the EARB PIRWG for Stages One and Two and EARB at designated points in the LCM Framework to ensure the key activities, core deliverables, and any additional deliverables required for that stage have been completed. Any deviations from this process must be approved in writing by the CIO. Appendix A is an acronym list and Appendix B, a glossary. A detailed illustration of the Framework, Departmental document references and a template for the Tailored Project Guide can be found in Appendices C-E respectively. The content of the appendices is "for information purposes only" and serves as guidance for those using this directive. [Appendix C](#) is a visual portrayal of the required stages, key activities and deliverables described in this directive.

In this document, the Framework stages are designated by a number followed by supporting information about each stage. The sections in the text are numbered to correspond to the six stages of the Framework. Key activities and core deliverables for each stage are explained in text format. Supporting detail for each core deliverable within a particular stage is contained in tables. The tables support the bulleted list of core deliverables in each stage by providing detail that better explains each deliverable.

Below is key information regarding each stage of the LCM Framework.

1. PRE-VISION

The purpose of the Pre-Vision Stage is to develop and submit the initial budget request and justification (Major IT Business Case); develop an Analysis of Alternatives for the new concept; and a draft Project Tailoring Plan. This stage coincides with the Capital Planning and Investment Control (CPIC) Pre-Selection Phase.

The Pre-Vision Stage contains the following key activities:

- The Project Manager is assigned.
- Develop the initial budget request and justification (Major IT Business Case).
- Develop a draft Tailoring Plan, draft Acquisition Strategy, and draft Analysis of Alternatives:
 - For software needs, document the required Three-Step Software Solution Analysis outlined in [OMB Memorandum M-16-21 \(Federal Source Code Policy\)](#)
- Identify the Integrated Project Team (IPT).
- The feasibility and initial cost of the project will be reviewed and approved by the PIRWG.
- The Enterprise Architect will work with the PM to identify the segment and Segment Owner.

The Pre-Vision Stage contains the following core deliverables:

- **Business case documents:** Major IT Business Case, draft high level project management plan and a project charter, and a draft Analysis of Alternatives
- **Acquisition documents:** Examples would include draft acquisition strategy and solicitation documents, draft initial cost/budget plan.
- **Tailored Project Plan:** A draft Project Tailoring Plan

Table 1. Draft Business Case

Key Components		Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ Project Description and Purpose ▶ Draft Project Charter ▶ Major IT Business Case ▶ Draft Alternatives Analysis (Market Research & Alternative Solution) ▶ Project Scope, Cost and Funding 	<ul style="list-style-type: none"> ▶ Performance Measurements and Risks (includes Security Risks) ▶ Draft High-Level Solution Acquisition Plan ▶ Draft High-Level Project Management Plan 	<ul style="list-style-type: none"> ▶ Project Manager Develops Draft Business Case ▶ IAMT, EA, IA, Privacy Safeguards Program (RIMS), and Other Relevant Staff Reviews Business Case; IAMT, PIRWG Approves 	<p>Clinger- Cohen Act OMB A-11: Preparation, Submission & Execution of the Budget OMB A-94: Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs OMB A-130: Management of Federal Information Resources OMB A-131 (Revised): Value Engineering Federal Information Security Management Act (FISMA) National Institute for Standards and Technology (NIST) OMB M-16-21: Federal Source Code Policy</p>

Table 2. Draft Acquisition Documents

Key Components		Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ Market Research ▶ Draft Source Selection Plan ▶ Draft Acquisition Strategy ▶ Requisition Document ▶ Pre-Select Phase Documents 	<ul style="list-style-type: none"> ▶ Procurement Action Requests ▶ IT Procurements Indicating how Specific Equipment or Resources are to be Acquired ▶ Document Hand-off strategy for Multiple Vendors ▶ Quality Assurance Surveillance Plan (QASP) 	<ul style="list-style-type: none"> ▶ Contracting Officer/Business Area Develops Acquisition Documents 	<p>Clinger- Cohen Act Federal Acquisition Regulation (FAR) Department of Education Acquisition Regulation (EDAR) Department of Education Acquisition Procedures Manual (APM) 508 Compliance, (Electronic & IT Accessibility Standards) OMB A-131 (Revised): Value Engineering ACS Directive: Acquisition Planning (OCFO: 2-107) ACS Directive: Procuring Electronic and Information Technology (EIT) in Conformance with Section 508 of the Rehabilitation Act (OCIO: 3-105) OMB M-16-21: Federal Source Code Policy</p>

2. VISION STAGE

The purpose of the Vision Stage is to further develop a business case, necessary acquisition planning documents for the procurement of services and resources to build new IT solutions or improve existing Federal or Department IT assets and high-level requirements for the new system. During this process, the feasibility and cost of the project will be assessed.

The Vision Stage contains the following key activities:

- Identify needs and define project scope, define high-level requirements and prepare business case.
- Obtain appropriate reviews and approvals for the business case. This will include the OCIO's IAMT staff ensuring that the business case aligns with the Department's IT investment objectives.
- Obtain review and approval of acquisition planning activities. The CAM office will review and approve all acquisition documents.
- Obtain necessary technical reviews and approvals for the project, as envisioned. The EARB, Security, Regulatory Information Management Services (RIMS), PIRWG, EA and Information Assurance (IA) are examples of staff that would participate in the review and approval activities.

The Vision Stage contains the following core deliverables:

- **Business case documents.** Will include a high level project management plan and a project charter.
- **Acquisition documents.** Examples would include acquisition strategy and solicitation documents.
- **Technical documents.** Examples would include presentations for EARB, EA and PIRWG reviews.
- **Security and privacy documents.** An example is the Critical Infrastructure Protection (CIP) Questionnaire.
- **Tailored project guide.** See [Appendix D](#) on page 30 for a template.

The business case includes a request to the Department's senior management for support of an initiative and usually indicates the level of resource investment and financial commitment deemed necessary for the project. The business case provides a business justification for implementing

new or improved Federal or Department IT solutions. Table 3 contains key information for the business case.

Table 3. Business Case

Key Components		Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ Project Description and Purpose ▶ Project Charter ▶ Business Value of the Initiative ▶ Alternatives Analysis (Market Research & Alternative Solution) ▶ Recommended Solution and Justification ▶ Project Scope, Cost and Funding 	<ul style="list-style-type: none"> ▶ Performance Measurements and Risks (includes Security Risks) ▶ High-Level Solution Acquisition Plan ▶ High-Level Project Management Plan 	<ul style="list-style-type: none"> ▶ Project Manager Develops Business Case ▶ IAMT, EA, IA, Privacy Safeguards Program (RIMS), and Other Relevant Staff Reviews Business Case; IAMT, PIRWG Approves 	Clinger- Cohen Act OMB A-11: Preparation, Submission & Execution of the Budget OMB A-94: Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs OMB A-130: Management of Federal Information Resources OMB A-131 (Revised): Value Engineering Federal Information Security Management Act (FISMA) National Institute for Standards and Technology (NIST) OMB M-16-21: Federal Source Code Policy

Acquisition documents help identify and manage the activities of the acquisition strategy to ensure solution acquisition in a timely, efficient and effective manner. Table 4 contains key information for acquisition documents.

Table 4. Acquisition Documents

Key Components		Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ Market Research ▶ Source Selection Plan ▶ Independent Government Cost Estimate ▶ Acquisition Strategy ▶ Vendor Identification List ▶ Requisition Document ▶ Solicitation: <ul style="list-style-type: none"> – Statement Of Objectives (SOO) – Statement Of Work (SOW) (with appropriate LCM including VE and security language) 	<ul style="list-style-type: none"> ▶ Procurement Action Requests ▶ IT Procurements Indicating how Specific Equipment or Resources are to be Acquired ▶ Document Hand-off strategy for Multiple Vendors ▶ Quality Assurance Surveillance Plan (QASP) ▶ Final EA Review ▶ Award Document 	<ul style="list-style-type: none"> ▶ Contracting Officer/Business Area Develops Acquisition Documents ▶ CAM Reviews and Approves 	Clinger- Cohen Act Federal Acquisition Regulation (FAR) 508 Compliance, (Electronic & IT Accessibility Standards) OMB A-131 (Revised) : Value Engineering ACS Directive: Acquisition Planning (OCFO: 2-107) ACS Directive: Procuring Electronic and Information Technology (EIT) in Conformance with Section 508 of the Rehabilitation Act (OCIO: 3-105) OMB M-16-21: Federal Source Code Policy

Technical documents will substantiate solution technical needs. These documents are presented to technical staff during the Vision Stage to obtain initial technical review and approval. Table 5 contains key information for technical documents.

Table 5. Technical Documents

Key Components	Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ Solution Functionality ▶ High-Level Functional Requirements ▶ Operational Requirements ▶ Presentation Summarizing Data Presented in Business Case and Components Above 	<ul style="list-style-type: none"> ▶ Project Manager develops Technical Documents ▶ Groups such as EARB, Security, PIRWG, EA, IA Review & Approve 	Clinger-Cohen Act

Security and privacy documents consist of various types of security documentation necessary for the Vision Stage. These documents contain security and privacy requirements and controls for protecting the solution. Table 6 contains key information for security and privacy documents.

Table 6. Security and Privacy Documents

Key Components	Key Roles and Responsibilities	Key Legislative/Policy Drivers	
<ul style="list-style-type: none"> ▶ Identify Certification & Accreditation (C&A) Team ▶ Determine Initial System Security Requirement ▶ Complete CIP Questionnaire ▶ Complete a General Support System (GSS) and Major Applications (MA) Inventory Form 	<ul style="list-style-type: none"> ▶ Project Manager develops Security & Privacy Documents ▶ POC Computer Security Office (CSO) reviews security documents. ▶ IA reviews; C&A approves & Accepts as Part of Larger C&A Process, Privacy Safeguards Program (RIMS) reviews CIP Questionnaire, and evaluates business case for PII and SSN collection, use, and disclosure. 	<ul style="list-style-type: none"> ▶ Clinger-Cohen Act ▶ OMB A-130: Management of Federal Information Resources ▶ E-Government Act 2002 ▶ FISMA ▶ NIST ▶ ACS Handbook for IA Security Policy (OCIO-1) ▶ Family Educational Rights and Privacy Act (FERPA) ▶ Electronic Signatures and Records Act (ESRA) 	<ul style="list-style-type: none"> ▶ ACS Handbook for IT Security Risk Assessment Procedures (OCIO-7) ▶ ACS Handbook for IT Security GSS & MA Inventory (OCIO-9) ▶ ACS Handbook for IT Security Contingency Planning Procedures (OCIO-10) ▶ ACS Handbook for IT Security Configuration Management (CM) Planning Procedures (OCIO-11)

The [Tailored Project Guide](#) is a document for planning, recording and tracking the completion of required deliverables for an IT solution. All project managers will be required to develop a Tailored Project Guide to track the completion of core deliverables throughout the lifecycle. [Appendix E](#) at the end of this document is a Tailored Project Guide Template suggested for use. Project managers may develop their own tailored project guide as long as one is used to plan and track the completion of all project deliverables.

End of Vision Stage - Moving Forward: Once the key activities and deliverables aforementioned have been fulfilled, the project manager for the system being developed should arrange a Vision Stage Gate Review with the EARB to authorize the project’s progress into the Definition Stage and the PIRWG to ensure the project is financially on track.

3. DEFINITION STAGE

The purpose of the Definition Stage is to define functional requirements that address both the business and technical solutions. The project team will produce a high-level functional design and a detailed solution design to be used to guide work in the Construction and Validation Stage.

The Definition Stage contains the following key activities:

- Review existing business case. Submit a Baseline Change Request to IAMT, as necessary.
- Develop and obtain approval of detailed project management plan.
- Develop high-level business, functional and security requirements.
- Develop high-level architecture.
- Obtain technical reviews and approvals. EARB, Security, RIMS, EA, IA, PIRWG are examples of entities that would participate in review and approval activities.
- Design solution.

The Definition Stage contains the following core deliverables:

- *Review previous deliverables and update as necessary.*
- Project management plan.
- Configuration management (CM) plan.
- Requirements documentation.
- Design documentation.
- Security and privacy documentation. Business continuity plan, disaster recovery plan, contingency plan and security risk assessment and mitigation plan are examples of security and privacy documentation.
- Test Plan.

“Review previous deliverables and update as necessary” is listed to remind project managers to review documents from the previous stage and make updates, if needed, to ensure documents stay current with any project or solution changes. Project managers who originally developed the deliverables in question will review and update them.

Following industry standards such as, the Project Management Body of Knowledge (PMBOK), the project management plan outlines a performance-based management approach (current and estimated cost, schedule and performance goals) including project milestones and associated resources, tools, techniques and organizational roles and responsibilities.

The project management plan will define project activities throughout the lifecycle, will describe how the project team will complete the deliverables within schedule and cost while meeting or exceeding quality, and apply value engineering methodology including contractor developed VECPs and agency developed VEPs through all life cycle stages Table 7 contains key information for the project management plan.

Table 7. Project Management Plan

Key Components		Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ Project Charter ▶ Project Management Approach ▶ Scope ▶ Work Breakdown Structure (WBS) (with cost & schedule estimates and baselines) ▶ Responsibility Assignments ▶ System or Software Development Plan ▶ High-Level Risk Assessments and Plan ▶ Value engineering methodology, VEP and VECP 	<ul style="list-style-type: none"> ▶ PMBOK Subsidiary Management Plans, such as: <ul style="list-style-type: none"> – Comms Plan – QA Plan ▶ Open Issues ▶ Supporting Detail: <ul style="list-style-type: none"> – Deliverables – Constraints and Assumptions – Relevant Standards – and Policies 	<ul style="list-style-type: none"> ▶ Project Manager develops Project Management Plan ▶ Program and Technical Staff Reviews and Approves 	<ul style="list-style-type: none"> ▶ Clinger-Cohen Act ▶ OMB A-131 (Revised): Value Engineering ▶ OMB M-16-21: Federal Source Code Policy

The configuration management plan identifies the configuration items, components and related work products that will be placed under configuration management using configuration identification, configuration control, and configuration status accounting and configuration audits. This plan will establish and maintain the integrity of work products throughout the lifecycle. Table 8 contains key information for the configuration management plan.

Table 8. Configuration Management Plan

Key Components	Key Roles and Responsibilities	Key Legislative / Policy Drivers
<ul style="list-style-type: none"> ▶ Baseline Work Products ▶ Mechanism to Track and Control Changes ▶ Change Requests ▶ Mechanism to Establish and Maintain Baseline Integrity 	<ul style="list-style-type: none"> ▶ Project Manager develops Configuration Management Plan ▶ POC Computer Security Office (CSO) reviews security documents. ▶ IA Reviews and C&A Reviews and Accepts as Part of Larger C&A Process 	<ul style="list-style-type: none"> ▶ Clinger-Cohen Act ▶ OMB A-130: Management of Federal Information Resources ▶ FISMA ▶ NIST ▶ ACS Handbook for IT Security CM Planning Procedures (OCIO-11)

Requirements documentation consists of all the detailed requirements associated with the solution. The requirements documentation will identify and validate the business, technical, security and solution requirements. Table 9 contains key information for requirements documentation.

Table 9. Requirements Documentation

Key Components	Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ Business Requirements Accomplished by Manual Processes ▶ Technical/Systems Requirements, Accomplished by Automation ▶ Infrastructure, Accomplished by Telecommunications, Facilities and Desktop 	<ul style="list-style-type: none"> ▶ Project Manager develops Requirements Documentation ▶ Program and Technical Staff Reviews and Approves 	<ul style="list-style-type: none"> ▶ FISMA ▶ OMB A-130: Management of Federal Information Resources ▶ Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government

Design documentation reflects the functional and technical solutions of what will be delivered and is traceable back to the requirements. The preliminary versus defined design should be depicted through graphic models, process flows, or block diagrams. The design documentation includes all the detailed requirements associated with the solution. The design documentation will define functional and technical components required to implement the solution. Table 10 contains key information for design documentation.

Table 10. Design Documentation

Key Components	Key Roles and Responsibilities	▶ Key Legislative / Policy Drivers
<ul style="list-style-type: none"> ▶ Technical Architecture: Telecommunications, hardware (HW) and software (SW) ▶ Data Architecture ▶ Entity Relationship Diagrams (ERDs) ▶ Data Dictionary ▶ Interface Specification (to Other Systems) ▶ Application Design: User Interface Input/Output, Design/Layout, System Security Management ▶ Federal Code Policy Analysis 	<ul style="list-style-type: none"> ▶ Project Manager develops Design Documentation ▶ Project Manager provides ▶ Program and Technical Staff Reviews and Approves 	<ul style="list-style-type: none"> ▶ OMB A-130: Management of Federal Information Resources ▶ FISMA ▶ Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government ▶ OMB M-16-21: Federal Source Code Policy

Security and privacy documentation will help protect the confidentiality, integrity and availability of the solution. It describes and addresses information associated with risk, risk mitigation, security requirements and

controls. Security and privacy documentation will contain detailed security and privacy requirements and controls for protecting the solution. Table 11 contains key information for security and privacy documentation.

Table 11. Security and Privacy Documentation

Key Components	Key Roles and Responsibilities	Key Legislative / Policy Drivers	
<ul style="list-style-type: none"> ▶ Business Continuity Plan ▶ Disaster Recovery Plan ▶ Contingency Plan ▶ Risk Assessment and Mitigation ▶ System Security Plan ▶ Privacy Impact Assessment (PIA) ▶ System of Records Notice (SORN) 	<ul style="list-style-type: none"> ▶ Project Manager develops Security & Privacy Documents ▶ POC Computer Security Office (CSO) reviews security documents. ▶ IA Reviews and C&A Reviews and Accepts as Part of Larger C&A Process ▶ Privacy Safeguards Program (RIMS) reviews and approves PIA and Privacy Act SORN, if required. 	<ul style="list-style-type: none"> ▶ Clinger-Cohen Act ▶ OMB A-130: Management of Federal Information Resources ▶ E-Government Act 2002 ▶ Federal Educational Rights and Privacy Act (FERPA) ▶ FISMA ▶ NIST ▶ Privacy Act of 1974, as amended ▶ ACS Handbook for IA Security Policy (OCIO-1) ▶ Family Educational Rights and Privacy Act (FERPA) ▶ Electronic Signatures and Records Act (ESRA) 	<ul style="list-style-type: none"> ▶ ACS Handbook for IT Security Risk Assessment Procedures (OCIO-7) ▶ ACS Handbook for IT Security GSS & MA Inventory (OCIO-9) ▶ ACS Handbook for IT Security Contingency Planning Procedures (OCIO-10) ▶ ACS Handbook for IT Security CM Planning Procedures (OCIO-11)

The test plan outlines the types of testing, testing participants and timeframe for testing and provides a detailed strategy for testing the solution. Table 12 contains key information for the test plan.

Table 12. Test Plan

Key Components	Key Roles and Responsibilities	Key Legislative / Policy Drivers
<ul style="list-style-type: none"> ▶ Organizational Structure with Roles and Responsibilities ▶ Types of Testing ▶ Testing Scenarios ▶ Timeframes 	<ul style="list-style-type: none"> ▶ Project Manager develops Test Plan ▶ POC Computer Security Office (CSO) reviews security documents. ▶ IA Reviews and C&A Reviews and Accepts as Part of Larger C&A Process ▶ Program and Technical Staff Reviews and Approves 	<ul style="list-style-type: none"> ▶ OMB A-130: Management of Federal Information Resources ▶ FISMA

End of Definition Stage - Moving Forward: Once the key activities and deliverables aforementioned have been fulfilled, the project manager for the system being developed should arrange a Definition Stage Gate Review with

the EARB for a technical review and the PIRWG to ensure the project is meeting its budget. At this stage, the PIRWG can decide to allow the project to go on to the Construction and Validation Stage; cancel the project, or request the project to implement changes to get within budget.

4. CONSTRUCTION AND VALIDATION STAGE

The purpose of the Construction and Validation Stage is to build, test and validate the solution, transform specifications developed in the Definition Stage into an executable solution and validate solution functionality to ensure it meets or exceeds business and technical expectations.

The Construction and Validation Stage contains the following key activities:

- Build and/or acquire solution.
- Test and monitor solution. Telecommunications, applications and manual processes are aspects of the solution that project staff will test and monitor.
- Identify areas for improvement and apply VE methodology to achieve quality improvement and reduce resource commitment.
- Obtain security certification and accreditation.
- Obtain technical reviews and approval for implementation.
- Prepare implementation documents and maintenance and operations plan.

The Construction and Validation Stage contains the following core deliverables:

- *Review previous deliverables and update as necessary.*
- Testing documentation. A Fully Tested and Accepted Solution and test execution results and reports are examples of testing documentation.
- Implementation documents. Implementation plan, training plan, solution user manual, data conversion plan, system start-up (a.k.a. system change over plan) are examples of implementation documents.
- Maintenance and operations plan.
- Network, HW/SW documentation.

As in the Definition Stage, “review previous deliverables and update as necessary” is listed to remind project managers to review documents from the previous stage and make updates, if needed, to ensure that documents stay current with any project or solution changes. Project managers are responsible for reviewing and updating deliverables.

Testing documentation contains testing approaches and standards, provides a record of the completion of all necessary testing and helps gauge whether or not the solution meets all business and technical requirements. Testing documentation ensures that the solution is properly constructed in relation to requirements and business needs. Table 13 contains key information for testing documentation.

Table 13. Testing Documentation

Key Components	Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ Fully Tested & Accepted Solution ▶ Test Execution Results and Reports 	<ul style="list-style-type: none"> ▶ Project Manager develops Testing Documentation ▶ IA Reviews and C&A Reviews & Accepts as Part of Larger C&A Process ▶ Program and Technical Staff Reviews and Approves ▶ Project Manager coordinates accessibility (Section 508 compliance) testing with OCIO Assistive Technology Team, if required. 	<ul style="list-style-type: none"> ▶ OMB A-130: Management of Federal Information Resources ▶ FISMA

Implementation documents are the plans for executing solution activities, roles and responsibilities, dependencies and timelines. Implementation documents provide guidance and consideration for all activities necessary to deploy the solution. Table 14 contains key information for implementation documents.

Table14. Implementation Documents

Key Components	Key Roles and Responsibilities	Key Legislative/Policy Drivers	
<ul style="list-style-type: none"> ▶ Implementation Plan ▶ Training Plan ▶ Solution User Manual ▶ Data Conversion Plan ▶ System Start-up Plan (a.k.a. System Change Over Plan) 	<ul style="list-style-type: none"> ▶ Project Manager develops Implementation Documents ▶ POC Computer Security Office (CSO) reviews security documents. ▶ IA Reviews and C&A Reviews and Accepts as Part of Larger C&A Process ▶ Program and Technical Staff Reviews and Approves 	<ul style="list-style-type: none"> ▶ Clinger-Cohen Act ▶ OMB A-130: Management of Federal Information Resources ▶ OMB A-131 (Revised): Value Engineering ▶ E-Government Act 2002 ▶ FISMA ▶ NIST ▶ ACS Handbook for IA Security Policy (OCIO-1) 	<ul style="list-style-type: none"> ▶ ACS Handbook for IT Security C&A Procedures (OCIO-5) ▶ ACS Handbook for IT Security Risk Assessment Procedures (OCIO-7) ▶ ACS Handbook for IT Security GSS & MA Inventory (OCIO-9) ▶ ACS Handbook for IT Security Contingency Planning Procedures (OCIO-10) ▶ ACS Handbook for IT Security CM Planning Procedures (OCIO-11)

The maintenance and operations plan establishes an approach for continued operational use and maintenance of the solution. The plan provides the processes and procedures used to maintain the solution. For solutions using custom developed software code, the plan must address how that code is reviewed and released as Open Source Software under the Federal Source Code Policy (FSCP). Table 15 contains key information for the maintenance and operations plan.

Table 15. Maintenance and Operations Plan

Key Components	Key Roles and Responsibilities	Key Legislative / Policy Drivers	
<ul style="list-style-type: none"> ▶ Plan to Maintain Technical Solution ▶ Points of Contact ▶ Notification and Escalation Process with Issues Resolution ▶ Job Execution Workflow Schedule ▶ Run Book ▶ Restart Procedures ▶ Open Source Software Release Procedure 	<ul style="list-style-type: none"> ▶ Project Manager develops Maintenance and Operations Plan ▶ POC Computer Security Office (CSO) reviews security documents. ▶ IA Reviews and C&A Reviews and Accepts as Part of Larger C&A Process ▶ Program and Technical Staff Reviews and Approves 	<ul style="list-style-type: none"> ▶ Clinger-Cohen Act ▶ OMB A-130: Management of Federal Information Resources ▶ E-Government Act 2002 ▶ FISMA ▶ NIST ▶ ACS Handbook for IA Security Policy (OCIO-1) ▶ ACS Handbook for IT Security Risk Assessment Procedures (OCIO-7) ▶ ACS Handbook for IT Security GSS & MA Inventory (OCIO-9) ▶ ACS Handbook for IT Security Contingency Planning Procedures (OCIO-10) ▶ ACS Handbook for IT CM Planning Procedures (OCIO-11) ▶ OMB M-16-21: Federal Source Code Policy 	

End of Construction and Validation Stage - Moving Forward: Once the key activities and deliverables aforementioned have been fulfilled, the project manager for the system being developed should arrange a Construction and Validation Stage Gate Review with the EARB to authorize the project’s progress into the Implementation Stage.

5. IMPLEMENTATION STAGE

The purpose of the Implementation Stage is to install the new or enhanced solution in the production environment, train users, convert data as needed and transition the solution to end-users.

The Implementation Stage contains the following key activities:

- Execute implementation plan.
- Obtain program and technical review and approval to ensure successful implementation.

The Implementation Stage contains one core deliverable: the Accepted Operational/Running Solution.

The Accepted Operational/Running Solution is a fully operational solution installed in the production environment. The documentation associated with the solution accepted for implementation will facilitate executing the solution in the operating environment. Table 16 contains key information for the Accepted Operational/Running Solution.

Table16. Accepted Operational/Running Solution

Key Components	Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ Execution of Implementation Plan to include: Application of VE, and Notification of Implementation to End Users ▶ Execution of Training Plan ▶ Data Entry or Conversion ▶ Security, C&A and Post Implementation Evaluation ▶ Execution of Open Source Release Procedure (Inventory, Source Code) 	<ul style="list-style-type: none"> ▶ Project Manager oversees Installation of Solution in Production Environment ▶ POC Computer Security Office (CSO) reviews security documents. ▶ Program and Technical Staff Reviews and Approves 	<ul style="list-style-type: none"> ▶ Clinger-Cohen Act ▶ OMB A-130: Management of Federal Information Resources ▶ OMB A-131 (Revised): Value Engineering ▶ OMB M-16-21: Federal Source Code Policy

End of Implementation Stage - Moving Forward: Once the key activities and deliverables aforementioned have been fulfilled, the project manager for the

system being developed should arrange an Implementation Stage Gate Review with the EARB to authorize the project's progress into the Operation and Maintenance Stage.

6. OPERATION AND MAINTENANCE STAGE

The purpose of the Operations and Maintenance Stage is to document operational and practicing procedures for solution modification and enhancement and align operational and practicing procedures with Department information technology business and technical standards.

The Operations and Maintenance Stage contains the following key activities:

- Operate and manage solution.
- Evaluate and enhance operations.
- Conduct annual contract review.
- Conduct annual business case review through the Capital Planning and Investment Control (CPIC) process.
- Conduct annual technical reviews. Security, RIMS, IA and EA are all examples of technical reviews.
- Update business case and budget, as necessary.
- Conduct Post-Implementation Review (PIR) 6 -18 months after the implementation of the solution to measure success in meeting initial investment goals.
- Conduct an operational analysis annually during the Operations and Maintenance Stage to identify opportunities through VE for improved service delivery, cost savings, changes driven by legislation or regulation, etc.
- For systems using Custom Code, update the enterprise code inventory.

The Operations and Maintenance Stage contains the following core deliverables:

- *Review previous deliverables and update as necessary.*
- Amended Business Case for Solution Enhancements.

As with the Definition and Construction and Validation Stages, “review previous deliverables and update as necessary” is listed to remind project managers to review documents from the previous stage and make updates, if needed, to ensure that documents stay current with any project or solution changes. In the Operations and Maintenance Stage, however, a solution change or enhancement, depending on the magnitude, may require new deliverables—not just updates to previous ones. Project managers who originally developed the deliverables in question will review and update them. There is also the potential for new project managers to make changes or enhancements and create new deliverables. A Stage Gate Review should be arranged with the EARB to authorize changes that introduce new functionality or technology components to the system.

The Amended Business Case for Solution Enhancement contains updates to the business case to reflect solution enhancements or changes. Table 17 contains key information for the amended business case.

Table17. Amended Business Case for Solution Enhancement

Key Components	Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ Baseline Change Request for any Section of the Original Business Case Requiring Update ▶ Explanation for Change in Cost/Schedule Variance ▶ PIR Report 	<ul style="list-style-type: none"> ▶ Project Manager submits Amended Business Case for Solution Enhancement ▶ Relevant Process Groups Review ▶ IAMT Reviews and Approves 	<ul style="list-style-type: none"> ▶ Clinger-Cohen Act ▶ OMB A-11: Preparation, Submission & Execution of the Budget ▶ OMB A-130: Management of Federal Information Resources ▶ OMB A-131 (Revised): Value Engineering ▶ OMB M-16-21: Federal Source Code Policy

End of Operations and Maintenance Stage - Moving Forward: Once the key activities and deliverables aforementioned have been fulfilled, the project manager for the system being developed should to arrange a Stage Gate Review with the EARB to authorize the project’s progress into the Retirement Stage.

7. RETIREMENT STAGE

The purpose of the Retirement Stage is to execute the systematic termination of the system and preserve vital information for future access and or reactivation.

The Retirement Stage contains the following key activities:

- Develop retirement plan. Sections of the retirement plan will include shut down system or continue service decision and the data and documentation plan.
- Develop disposal plan.
- Obtain program and technical reviews and approvals for retirement and disposal plans. The OCIO’s PIRWG is an example of a review board that will approve the retirement and disposal plan.
- Dispose system (at end of life) and archive SW, data and documentation.

The Retirement Stage contains the following core deliverables:

- Retirement plan.
- Disposal plan.

The retirement plan outlines activities to ensure orderly termination of the system and preservation of vital information about the system, so that information may be reactivated in the future, if necessary. It will contain the strategy for elimination, removal, or transitioning of services provided. Table 18 contains key information for the retirement plan.

Table 18. Retirement Plan

Key Components	Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ System Disposal Strategy ▶ Retirement Strategy ▶ Solution (SW, HW) Retirement Requirements List ▶ Event Tracking Procedures ▶ Data/Documentation Plan ▶ Updates to CM Plan to Track Document Versions ▶ Final updates to inventory and open source software 	<ul style="list-style-type: none"> ▶ Project Manager develops Retirement Plan ▶ POC Computer Security Office (CSO) reviews security documents. ▶ Program and Technical Staff Reviews and Approves ▶ Appropriate Records Liaison Officer reviews and approves based on Records Schedule. 	<ul style="list-style-type: none"> ▶ Clinger-Cohen Act ▶ OMB A-130: Management of Federal Information Resources ▶ FISMA ▶ NIST ▶ Family Educational Rights and Privacy Act (FERPA) ▶ OMB M-16-21: Federal Source Code Policy

The disposal plan emphasizes the proper preservation of the data processed by the solution, so that it can be effectively migrated to another solution or archived and restored in accordance with applicable record management regulations and policies.

The disposal plan will outline the strategy for termination of a solution’s HW and SW. Table 19 contains key information for the disposal plan.

Table19. Disposal Plan

Key Components	Key Roles and Responsibilities	Key Legislative/Policy Drivers
<ul style="list-style-type: none"> ▶ Identify how the Termination of the Solution/ Data will be Conducted and When ▶ Solution Termination Date ▶ SW Components to be Preserved ▶ Data to be Preserved ▶ Disposition of Remaining Equipment ▶ Archiving of Lifecycle Products 	<ul style="list-style-type: none"> ▶ Project Manager develops Disposal Plan ▶ POC Computer Security Office (CSO) reviews security documents. ▶ Program and Technical Staff Reviews and Approves ▶ Appropriate Records Liaison Officer reviews and approves based on Records Schedule. 	<ul style="list-style-type: none"> ▶ Clinger-Cohen Act ▶ OMB A-130: Management of Federal Information Resources ▶ FISMA ▶ NIST

APPENDIX A: Acronym List*(For information purposes only)*

ACRONYM	DESCRIPTION
ACS	Administrative Communications System
AD	Agile Development
AoA	Analysis of Alternatives
C & A	Certification and Accreditation
CAB	Change Advisory Board
CAM	Contracts and Acquisition Management
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CM	Configuration Management
CPIC	Capital Planning and Investment Control
CSO	Computer Security Officer
DST	Development Services Team
EA	Enterprise Architecture
EARB	Enterprise Architecture Review Board
EIT	Electronic and Information Technology
FAR	Federal Acquisition Regulation
FERPA	Family Educational Rights and Privacy Act
FISMA	Federal Information Security Management Act
FSA	Federal Student Aid
FSCP	Federal Source Code Policy
GSS	General Support System
IAMT	Investment Acquisition Management Team
IM	Information Management
IRB	Investment Review Board
IT	Information Technology
LCM	Lifecycle Management
MA	Major Application
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PIR	Post Implementation Review
PIRWG	Planning and Investment Review Working Group
PMBOK	Project Management Body of Knowledge
PMP	Project Management Plan
PO	Principal Office
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
RIMS	Regulatory Information Management Services
SDLC	Systems Development Lifecycle
SOO	Statement of Objectives

ACRONYM	DESCRIPTION
SORN	System of Records Notice
SOW	Statement of Work
VE	Value Engineering
VECP	Value Engineering Change Proposal
VEP	Value Engineering Proposal
WBS	Work Breakdown Structure

APPENDIX B: Glossary

(For information purposes only)

TERM	DEFINITION
508 Compliance	A section of the Rehabilitation Act that requires compliance with the Electronic and Information Technology Accessibility Standards.
Business Area	The office or offices within the Department responsible for managing an IT solution and whose purpose will be to support that business function.
Capital Planning and Investment Control (CPIC)	This process is an integrated approach to managing Information Technology (IT) investments.
Certification and Accreditation (C&A)	This activity entails a comprehensive analysis of the technical and non-technical security features and other safeguards of an IT solution to establish the extent to which a particular solution meets a set of specified security requirements.
Clinger-Cohen Act	This public law is formally known as the Information Technology Management Reform Act or ITMRA. It requires each agency to undertake capital planning and investment control by establishing a process for maximizing the value and assessing and managing risks of IT acquisitions of the executive agency.
Computer Security Officer (CSO)	These individuals implement security within their PO, as their duties require.
Contracts & Acquisitions Management (CAM)	Departmental offices (i.e. CAM or Federal Student Aid's (FSA) contract office) that review and approve acquisition planning documents.
Core Deliverable	A document that must be completed and approved by the end of a particular stage.
E-Government Act of 2002	This public law requires agencies to develop performance measures for implementing e-government. In addition, the act requires agencies to conduct and submit to OMB, Privacy Impact Assessments (PIAs) for all new IT investments administering information in identifiable form collected from or about members of the public. (Refer to the CPIC process for more information).
Enterprise Architecture (EA)	This functional area provides resources and processes to help the Department link its business needs with the best available technologies. EA helps the Department accomplish more with existing resources by using common or shared technology features to deliver needed capabilities faster, reduce new technology risks and free key program staff to focus on more important work.
Enterprise Architecture Review Board (EARB)	Department governing body whose purpose is to govern the technical standards and procedures that are used to develop ED's IT systems and affect the reliability, availability, integrity and performance of those systems and the network infrastructure that supports them.
Exit/Entry Criteria	The required Framework deliverables that must be completed and approved to exit one stage and enter the next.
Family Educational Rights and Privacy Act (FERPA)	A Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the Department.

TERM	DEFINITION
Federal Information Security Management Act (FISMA) of 2002	Federal legislation that requires agencies to integrate IT security into their capital planning and enterprise architecture processes at the agency, conduct annual IT security reviews of all programs and systems and report the results of those reviews to OMB.
Framework	A structured approach of required stages, key activities and core deliverables that provides a foundation for aligning existing interrelated processes within the Department—regardless of system lifecycle methodology employed.
General Support System (GSS)	Interconnected information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, facilities and people. It provides support for a variety of users or applications, or both.
Information Assurance (IA)	The continuous application of security policies, procedures and processes that protect and defend information and information resources from unauthorized disclosure, modification or denial of services to authorized consumers.
Information Technology (IT)	A term used to describe equipment or an interconnected system or subsystem of equipment, which is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data by an executive agency.
Investment Acquisition Management Team (IAMT)	A process area within the Department that provides an integrated management mechanism for the continuous selection, control and evaluation of investments in information systems and resources over the course of their lifecycles. (Refer to the Department's IAMT Process Guide for more information).
Key Activity	Any task, procedure or process that enables and supports the development and/or approval of a core deliverable (see definition for core deliverable above).
Key Component	Critical documents, sections of documents or categories of information that pertain to a core deliverable.
Lifecycle Management (LCM)	The coordination of activities associated with the implementation of information systems from conception through disposal, which include defining requirements, designing, building, testing, implementing and disposing of systems.
Major Application	An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application.
National Institute for Standards and Technology (NIST)	This organization is a non-regulatory Federal agency within the U.S. Commerce Department's Technology Administration division. NIST's mission is to develop and promote measurement, standards and technology to enhance productivity, facilitate trade and improve the quality of life.
OMB Circular A-11	The title of this legislation is "Preparing, Submitting and Executing the Budget." A-11 provides guidance on preparing the Fiscal Year Budget

TERM	DEFINITION
	submissions for Presidential review and includes instructions on budget execution.
OMB Circular A-123	The revised version of this policy will have the title, "Management's Responsibility for Internal Control," and is effective as of FY 2006. This legislation defines management's responsibility for internal control in Federal agencies and has a strong emphasis on financial reporting, as opposed to IT Capital Planning.
OMB Circular A-130	The title of this policy is "Management of Federal Information Resources," A-130, provides information resource management policies on Federal Information Management/Information Technology (IM/IT) resources. The Department's OCIO recommends that all offices investing in IT resources become familiar with OMB A-130.
OMB Circular A-94	The title of this policy is "Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs." A-94 offers guidelines to promote efficient resource allocation through well-informed decision-making.
OMB Circular A-131 (Revised)	The title of this policy is "Value Engineering" A-131 (Revised) requires Federal Departments and Agencies to use value engineering (VE) as a management tool, where appropriate, to reduce program and acquisition costs.
OMB Memorandum M-16-21	The title of this memorandum is "Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software" and is effective August 2016. This memorandum seeks to ensure that new custom-developed Federal source code is made broadly available for reuse across the Federal Government.
Paperwork Reduction Act of 1995	Federal legislation intended to minimize the paperwork burden resulting from the collection of information by or for the Federal Government in an effort to reduce cost by better managing Federal Government information.
Planning and Investment Review Working Group (PIRWG)	Department governing body that conducts IT investment analysis reviews and evaluates IT investments and makes recommendations to the CIO. The PIRWG also advises the CIO on Strategic IT investment management issues.
Principal Office (PO)	Offices within the Department which are responsible for ensuring that they develop automated systems that use information technology in accordance with the Framework.
Privacy Act of 1974, as amended	All Department IT systems processing data that is protected under the Privacy Act must have measures implemented to protect individually identifiable information. Interconnecting systems owned by other departments and agencies that process Department data must also be considered. Protection measures must consist of management, technical and operational controls and ensure an acceptable level of risk. An acceptable level of risk should be determined in accordance with the Department's Risk Management Procedures.
Process Guides	Documents for various process areas within the Department (e.g. IAMT, EARB, CAB).
Project Manager	Staff person who is responsible for creating deliverables and ensuring that business and technical reviews are executed and required deliverables

TERM	DEFINITION
	are completed. This individual is also responsible for managing the day-to-day operations of the Department's IT solutions.
Quality Assurance (QA)	A discipline within project management to objectively monitor control and ensure the completion of key activities and required core deliverables throughout the lifecycle.
Solution	A term to describe all automated information systems, software applications and manual processes at the Department (see System below).
Stage	Definitive sections of the lifecycle that indicate a specific purpose or goal (e.g. Vision Stage, Design Stage). The end of each stage is marked by a "stage gate," which marks the exit from one stage and entry into the next.
Stage Gate Review	The integration of various business and technical reviews that ensures core deliverables (and any additional deliverables) required for that stage have been completed.
System	A collection of components (hardware, software, interfaces) organized to accomplish a specific function or set of functions; generally considered to be a self-sufficient item in its intended operational use.
Tailored Project Guide	A document to be used by program and project managers to plan, record and track the completion of all deliverables required for that solution. Project managers should list all Framework core deliverables and any additional required deliverables for their solution.
Usable Functionality	A well-tested functional set of software code, developed incrementally, that is executable and has been successfully deployed to end-users in support of a defined set of business requirements.
User	An individual or organization operating or interacting directly with the system; one who uses the services of a system.
Value Engineering	A systematic process of reviewing and analyzing the requirements, functions and elements of systems, project, equipment, facilities, services, and supplies for the purpose of achieving the essential functions at the lowest life-cycle cost consistent with required levels of performance, reliability, quality, or safety.
Value Engineering Plan	An in-house agency-developed proposal, or a proposal developed by a contractor under contract to provide VE services, to provide VE studies for a Government project/program.
Value Engineering Change Proposal	A proposal submitted by a contractor consistent with the VE clause(s) in the contract that, through a change in the contract, would lower the project's life-cycle cost to the Government without impairing essential functions, characteristics, or performance.

APPENDIX C: Department Document References*(For information purposes only)*

DOCUMENTATION	OFFICE	POINT OF CONTACT (POC)	CONNECTED LINK
Acquisition Planning ACS Directives	Contracts and Acquisition Management (CAM)	James Hairfield (James.Hairfield@ED.gov)	http://connected.ed.gov/index.cfm?id=573cdc27-cea7-5f77-75d1-e49fee89a29d *
Department Level ACS Directive on Configuration Management	Enterprise Architecture Program Management Office	Jim will send new name	http://connected.ed.gov/document_handler.cfm?id=10064
Policy and Procedures: ConnectED	Development Services Team (DST)	Carollynn Hammersmith (Carollynn.Hammersmith@ED.gov)	http://connected.ed.gov/doc_img/policy_proc.doc
ED's Enterprise Architecture	Enterprise Architecture Program Management Office	Steven Corey-Bey (Steven.Corey-Bey@ed.gov)	http://connected/index.cfm?office=ea
A Guide to the Information Collection Clearance Process	Regulatory Information Management Services	Angela Arrington (Angela.Arrington@ED.gov)	http://wdcrobiis08/doc_img/ticol.doc
Privacy Impact Assessments and System of Records Notices	Regulatory Information Management Services	Kristen Lefevre (Kristin.Lefevre@ed.gov)	▶ http://connected.ed.gov/index.cfm?office=om&cid=be9ae700-b2b4-e2e1-fcbe-b2d9beb90b93
IAMT Policy ACS Directive OCIO:3-108	Investment Acquisition Management Team (IAMT)	Steven Corey-Bey (Steven.Corey-Bey@ed.gov)	▶ http://connected.ed.gov/document_handler.cfm?id=5090 *
System Security Plan Template	Information Assurance (IA)	Ann Kim (Ann.Kim@ED.gov)	http://connected.ed.gov/doc_img/System%20Security%20Plan%20Template%20102903%20v1%201.doc
IT Security Systems Development Lifecycle (SDLC) Integration Guide	Information Assurance (IA)	Ann Kim (Ann.Kim@ED.gov)	http://connected.ed.gov/doc_img/SDLC%20Security%20Integration%20Guide%20v3.doc

For technical questions concerning information found in this Administrative Communications System (ACS) document, please contact James Hicks at 202-245-8226 or <mailto:James.Hicks@ed.gov>.

This ACS document supersedes OCIO:1-106 "Lifecycle Management (LCM) Framework" dated 07/16/2010. Added Federal Source Code. Re-certified on 12/09/2016

DOCUMENTATION	OFFICE	POINT OF CONTACT (POC)	CONNECTED LINK
Information Assurance (IA) ACS Directives	Information Assurance (IA)	Ann Kim (Ann.Kim@ED.gov)	http://connected.ed.gov/index.cfm?cid=96c32e02-bbd6-df2f-40ee-f01d3c85243c *
EARB Information	Enterprise Architecture Program Management Office	James Hicks (James.Hicks@ed.gov)	http://connected/index.cfm?office=ea&navid=1627

*Link is to the ACS Directives library on ConnectED.

APPENDIX D: Tailored Project Guide Template⁴

(For information purposes only)

1. Pre-Vision Stage	
Core Deliverables	Notes
Draft Business Case	Major IT Business Case; draft high-level project management plan; draft project charter; draft AoA
Draft Acquisition Documents	
Draft Tailored Project Guide	
Additional Deliverables	
2. Vision Stage	
Core Deliverables	Notes
<i>Review previous deliverables and update/finalize as necessary</i>	
Business Case	
Acquisition Documents	
Technical Documents (e.g. EARB, EA)	
Security and Privacy Documents	
Tailored Project Guide	
Additional Deliverables	
3. Definition Stage	
Core Deliverables	Notes
<i>Review previous deliverables and update as necessary</i>	
Project Management Plan (PMP): Scope, Cost, Schedule, Quality, Staffing, Communications, Risk and Procurement.	
Configuration Management Plan (CM Plan)	
Requirements Documentation	
Design Documentation	
Security and Privacy Documentation	
Test Plan	
Additional Deliverables	

⁴ A list of stage-specific deliverable templates is available in [LCM Templates SharePoint site](#).

RIMS Deliverables: (consult the Department's "A Guide to the Information Collection Clearance Process" about whether your solution requires RIMS deliverables)	
<ul style="list-style-type: none"> • Systems of Record Update • Privacy Impact Assessment (PIA) • Information Collection Clearance • System of Records Notice (SORN) 	

4. Construction and Validation Stage

Core Deliverables	
<i>Review previous deliverables and update as necessary</i>	
Testing Documentation	
Implementation Documents	
Maintenance and Operation Plan	
Additional Deliverables	

5. Implementation Stage

Core Deliverables	
Accepted Operations / Running Solution	
Additional Deliverables	

6. Operations and Maintenance Stage

Core Deliverables	
<i>Review previous deliverables and update as necessary</i>	
Amended Business Case for Solution Enhancements	
Additional Deliverables	

7. Retirement Stage

Core Deliverables	
Retirement Plan	
Disposal Plan	
Additional Deliverables	

APPENDIX E: Incremental Development

(For information purposes only)

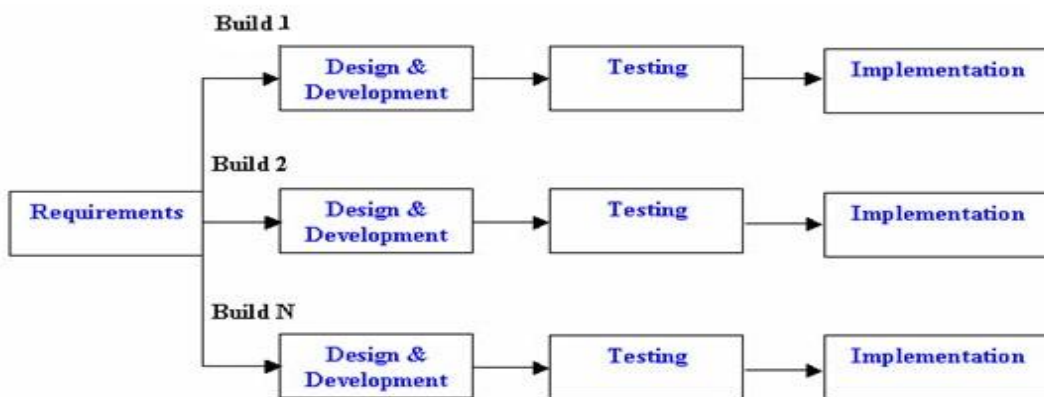
According to FITARA Implementation guidance (OMB Memorandum M-15-14) the CIO should certify that information technology investments are adequately implementing incremental development. In FITARA Implementation guidance incremental development is defined as “For development of software or services, planned and actual delivery of new or modified technical functionality to users occurs at least every six months.” To meet this requirement investment owners are required to produce usable functionality every six months. If usable functionality cannot be produced every six months or the project cannot be planned to produce usable functionality every six months an explanation needs to be provided as to why. Stage gate reviews will be used to validate the certification that IT resources are adequately implementing incremental development.

In the incremental model the whole requirement is divided into various builds. Multiple development cycles take place, making the life cycle a multi-waterfall cycle. Cycles are divided up into smaller, more easily managed modules. Each module passes through the Vision, Definition, Construction and Validation and Implementation stages. A working version is produced during the first module, so you have working version early on during the lifecycle.

Each subsequent release (every six months) of the module adds usable functionality to the previous release.

The process continues till the complete system is achieved.

Diagram of Incremental model:



Incremental Life Cycle Model

Advantages of Incremental model:

- Generates working software quickly and early during the software life cycle.
- This model is more flexible – less costly to change scope and requirements.
- It is easier to test and debug during a smaller iteration.
- In this model customer can respond to each built.
- Lowers initial delivery cost.
- Easier to manage risk because risky pieces are identified and handled during its iteration.

When to use the Incremental model:

- Can be used when the requirements of the complete system are clearly defined and understood.
- Major requirements must be defined; however, some details can evolve with time.
- There is a need to get a product to the market early.
- A new technology is being used
- Resources with needed skill set are not available
- There are some high risk features and goals.

APPENDIX F: Open Data

(For information purposes only)

Through their acquisition and technology management processes, the organization must build or modernize information systems in a way that maximizes interoperability and information accessibility, to the extent practicable and permitted by law. To this end, the CIO will validate that the following minimum requirements have been incorporated into acquisition planning documents and technical design for all new information system and those preparing for modernization, as appropriate:

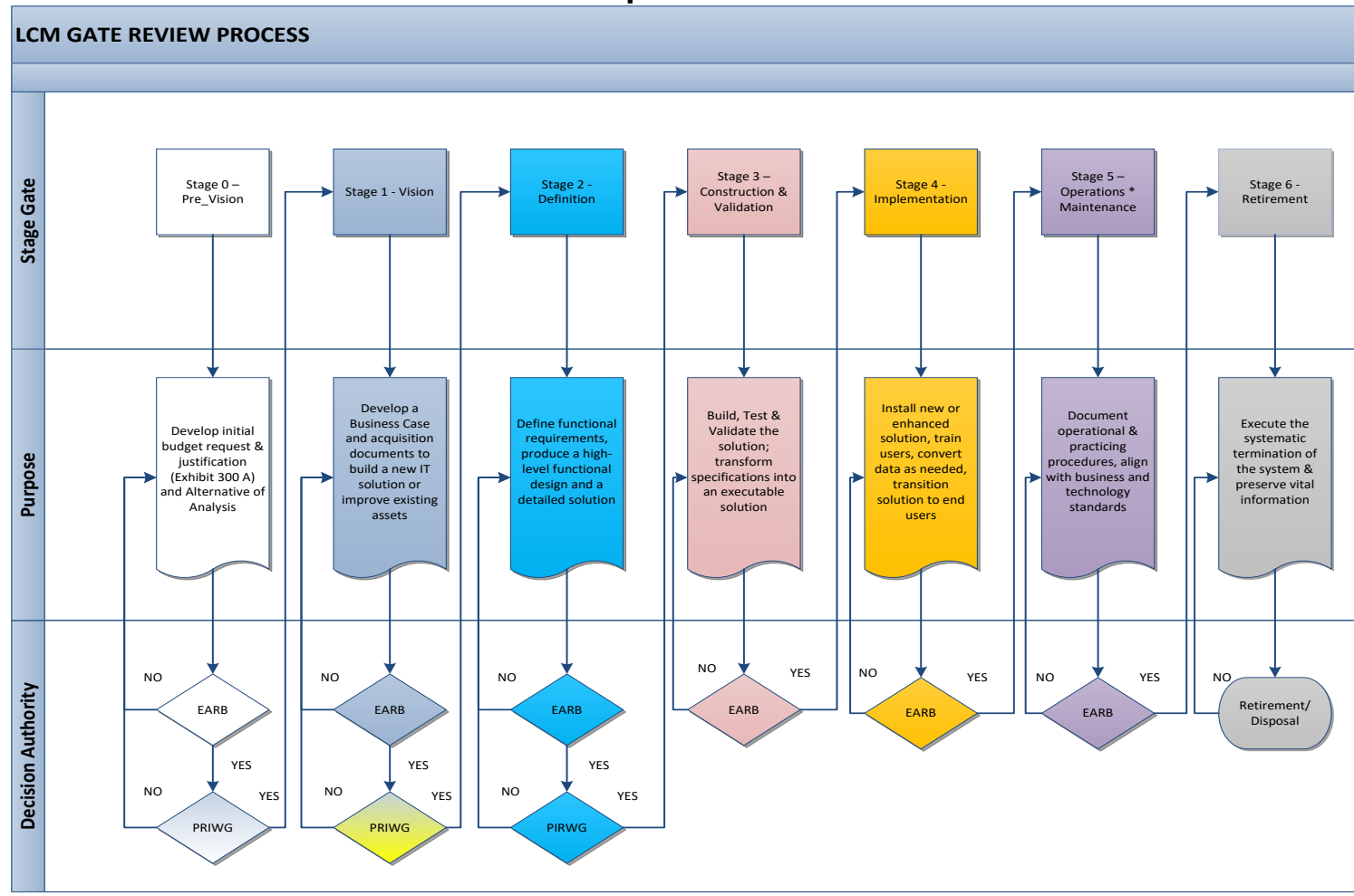
- The system design must be scalable, flexible and facilitate extraction of data in multiple formats and for a range of uses as internal and external needs change. This will involve the use of standards and specifications in the system design that promote industry best practices for information sharing and separation of data from the application layer to maximize data reuse opportunities.
- All data outputs associated with the system must create and maintain an enterprise data inventory; create and maintain a public data listing; create a process to engage with customers to help facilitate and prioritize data release; and clarify roles and responsibilities for promoting efficient and effective data release.
- Data schema and dictionaries have been documented and shared with internal partners and the public, as applicable.

New or significantly modified information systems need to support interoperability and information accessibility. The following is the minimum required for compliance:

- Ensure the system can export data in a machine-readable format
- Ensure data is separated from the application layer of the system to maximize future export and/or reuse of the data
- Store and export data using open data standards whenever possible, including common core metadata
- Document all data schemas and dictionaries used by the system
- Consider the use of applicable data standards and codesets that exist for common data elements
- Consider implementing a front-end automated data QA system that can provide lookup services
- Consider implementing a back-end data QA framework that can automate many data QA functions

- Consider developing a robust data stewardship community and governance structure

APPENDIX G: LCM Framework 2.0 Graphic



For technical questions concerning information found in this Administrative Communications System (ACS) document, please contact James Hicks at 202-245-8226 or <mailto:James.Hicks@ed.gov>.

This ACS document supersedes OCIO:1-106 "Lifecycle Management (LCM) Framework" dated 07/16/2010. Added Federal Source Code. Re-certified on 12/09/2016