PREFACE TO SELECTED INFORMATION DIRECTIVES

CIO Transmittal No.: 16-009	CIO Approval Date: 09/26/2016

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

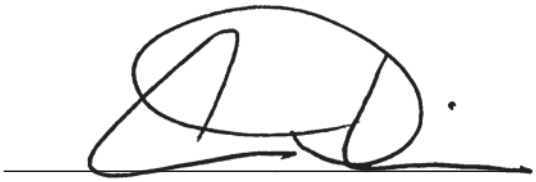
CHIEF INFORMATION OFFICER MEMORANDUM

SUBJECT: Guidance for Hosting Readiness Assessments

In a memorandum to SIOs and IMOs dated July 5, 2016, I introduced OEI's new Hosting Readiness Assessment process at the National Computing Center and indicated that it was in effect for all system and application deployments. It also stated the OEI would start with a "lite" process and finalize as we work with the program offices and get their input.

In order to maximize flexibility for updating the Hosting Readiness Assessment Process, the information and instructions are housed on at the "Enterprise Cloud" and "Templates and Guidelines" sections of the EPA Developer's Guide (https://developer.epa.gov/guide/). These instructions supersede any related direction in the following documents:

- CIO 2121.1, System Life Cycle Management Policy
- CIO 2121-P-03.0, System Life Cycle Management Procedure
- CIO 2121-G-01.0, System Life Cycle Management Guidance



Ann Dunkin
Chief Information Office
Environmental Protection Agency

EPA INFORMATION GUIDANCE

EPA Classification No.: CIO 2121-G-01.0	CIO Approval Date: 09/21/2012
CIO Transmittal No.: 12-004	Review Date: 09/21/2015

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

System Life Cycle Management (SLCM) Requirements Guidance

1. PURPOSE

This guidance defines documents that can be used by Project Managers and System Managers when they follow the System Life Cycle Management (SLCM) Policy and the SLCM Procedure. The documents defined herein are used in various phases of the SLCM procedure. These definitions will enable System Managers and Project Managers to use the most applicable documents for their system development and system operations efforts.

2. SCOPE AND APPLICABILITY

The SLCM Documents Guidance provides definitions and explanations of the documents used during the System Life Cycle of an information system. Project Managers, System Managers and everyone involved in the creation, review, update and approval of SLCM requirements will use these definitions to help them build a complete set of documents (also known as “artifacts”) required for their information system. The decision of which documents to use is based on the system life cycle tailoring activities found in the SLCM Procedure. Further guidance in the form of checklists, document templates, and sample documents is found on the SLCM web site.

This guidance applies to all EPA IT systems and application projects, both applications and general support systems (GSS). It is applicable to custom developed, commercial-off-the-shelf (COTS), or government-off-the-shelf (GOTS) projects. The procedure applies to all systems and contractor developed IT systems, whether hosted at the EPA National Computer Center (NCC) or elsewhere.

The specific SLCM documents, participants in the life cycle process, and the necessary reviews and approvals, vary from system to system. Some of the artifacts listed in this Guidance are components of a larger document, but are listed separately to provide more detail, however this does not mean that each document listed needs to stand on its one; based on the tailoring approach of the system documents may be combined or consolidated.

3. AUDIENCE

This guidance is provided for System Managers and Project Managers (PM) and all those who manage information technology (IT) systems and applications at the Environmental Protection Agency (EPA).

4. GUIDANCE ON SLCM DOCUMENTS

The SLCM documents are listed alphabetically by title and defined in this guidance. The Phases and Control Gates mentioned under the definitions are explained in detail in the SLCM Procedure.

Acquisition Package

(Definition Phase)The Acquisition Package is a collection of documents required to manage the process of acquiring products and/or services, including software products and services. The specific documents in the Acquisition Package (e.g., a bidder's list) vary by system and are a product of the Acquisition Strategy, a component of the Acquisition Package.

For specific guidance on developing required acquisition documents and ensuring compliance with EPA Acquisition Regulations (EPAAR) and Federal Acquisition Regulations (FAR), please consult your Contracts Officer or your Office of Acquisition Management (OAM) Point of Contact (POC).

Related to the Acquisition Package is the Acquisition Strategy, also known as an Acquisition Plan or Source Selection Strategy, is mandated under Federal Acquisition Regulations (FAR) Part 7 as the first step in the acquisition life cycle. Agencies must perform acquisition planning and conduct market research for all acquisitions. The Acquisition Plan describes the resource acquisition process, including assignment of responsibility, for all aspects of resource acquisition. EPA's Office of Acquisition Management (OAM) sets Agency policy for conducting acquisition planning.

The Acquisition Strategy may include:

- Statement of Need
- Applicable Conditions
- Costs
- Capability or Performance
- Delivery or Performance-Period Requirements
- Trade-Offs (between cost, capability, performance, and schedule)
- Risks
- Request for Proposal (RFP)
- Sources of Products
- Competition Strategy
- Source Selection Procedures
- Budgeting and Funding
- Priority Methodology
- Management Information Requirements
- Make or Buy Analysis
- Test and Evaluation
- Security Considerations
- Milestones

Alternatives Analysis

(Definition Phase: Control Gate 2) An alternatives analysis refers to an analysis of alternative approaches to addressing the performance objectives of an investment (project/program/system), performed prior to the initial decision to make an investment. The alternatives analysis should be updated periodically as appropriate to capture changes in the context for an investment decision.

Application Deployment Checklist (ADC)

(Operations & Maintenance Phase) The Application Deployment Checklist (ADC) is required for all Agency applications housed on a server located in EPA's National Computer Center (NCC). The checklist guides system managers through the deployment process, and OTOP uses it to assess system compatibility with EPA's central hosting environment.

The Project Manager should consider ADC requirements during the System Planning step of the Definition phase to ensure the system design is compatible with EPA's shared hosting environment and to comply with Agency policies and standards. The Project and System Manager is responsible for base-lining the ADC in the Design step of the Acquisition phase and submitting it to OTOP to begin the Review and Approval process. The Project Manager is responsible for updating the ADC as necessary during the Development and Implementation phases.

ADC submission forms, along with more information about the ADC process, are available on the OTOP intranet: http://cfint.rtpnc.epa.gov/otop/resources/adc/ApplicationDeploymentChecklist.cfm.

Approvals (Decision Papers)

To effectively manage system development and comply with EPA SLCM requirements, achievement of critical milestones is typically documented and approved by various stakeholders at various points throughout the life cycle framework. The scope of the approval process will vary depending on the system size, scope, complexity, risk and impact. The Project Manger is responsible for documenting the decisions in the form of Decision Papers, maintained with the set of documents for the information system.

Typical decision papers produced by the life cycle include:

- **Initiation Decision Paper** – Documents justification/approvals for a system development effort.
- **Development Decision Paper** – Documents justification/approval for beginning the Development phase of an approved system development effort.
- **Implementation Decision Paper** – Documents justification/approval for beginning the Implementation phase of an approved system development effort.
- **Retirement Decision Paper** – Documents justification/approval for beginning the Termination/Retirement phase of an approved system development effort.

This work products list defines each specific decision paper individually.

Archive/Incorporate Data and Software

(Termination Phase) Archive/Incorporate Data and Software refers to activities at the conclusion of a system development project necessary to: (1) archive data and software documents (e.g., data and system documents) for systems being retired or (2) incorporate (or migrate) data and software (e.g., data elements) into a new or modified system. Data and software incorporation activities occur in accordance with the requisite components of the retirement and data conversion plans.

Note: Archival and/or incorporation activities should integrate with the Security Plans containing security considerations for archiving and Contingency Plans for re-establishing system functionality in the event of an incident that impacts system performance.

Archived or incorporated data may include:

- All system documentation
- All data and data elements
- All software, code, and system elements

Authorization to Operate (ATO)

(Acquisition/Development Phase: Control Gate 4) The Authorization to Operate (ATO) is an official management decision (signoff) granted by a senior Agency official to authorize the implementation and operation of a system. By granting a system the authority to operate, the approver explicitly accepts any risk to Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals that may occur in the implementation of an agreed-upon set of security controls. The ATO is also referred to as an Accreditation.

A system must receive an ATO during the Control Gate #4 review in order to move into the Implementation phase and deploy the system.

The Authorization to Operate includes:

- Date of issuance, effective date
- Senior Agency official signature and date

Business Justification

The Business Justification emphasizes how an investment addresses a mission performance gap within an Agency. The Business Justification is a component of the SLCM set of documents. It is also one of the elements of an investment abstract submitted annually in coordination with the CPIC Exhibit 300 and Exhibit 53 process at EPA for budget review and may contain:

- A description of the investment
- The spending summary
- A justification for the project

The Business Justification usually contains a performance gap analysis to identify mission gaps in an Agency's strategy, an assessment that is captured at a higher level in the Mission Need Statement. A performance gap analysis includes a detailed evaluation of the capacity of the Agency and/or the Agency's assets to satisfy existing and emerging demands for services.

The Business Justification should clearly describe the organizational business capability shortfall and/or the impact of not satisfying the shortfall to Agency customers and stakeholders. The justification may also identify a technological opportunity and the increases in efficiency expected from implementing a particular solution.

The Business Justification also must describe the criticality and timeframe of the need, and roughly estimate the resources the Agency should commit to an investment based on value, mission impact and the scope of likely changes to the Agency's IT Investment Portfolio. This information forms the basis for establishing the priority of this need in competition with all other Agency investments.

The Business Justification is a critical work product for the system selection review conducted during Control Gate #2 at the end of the Definition phase.

Certifier's Statement

(Acquisition/Development phase: Control Gate 4) The Certifying Agent creates and signs a certification statement upon successful completion of the security certification. The security certification determines the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The Certifier's Statement is a component of the Security Accreditation Package.

The Certifier's Statement may include:

- Results based upon the review and observation of the security controls for a system
- Recommendations for establishing a Plan of Actions and Milestones (POA&Ms), including a timeline for resolving issues
- Certifying Agent signature, title, and date

Change Control

Change Control is an activity governed by the project's Configuration Management Plan. Refer to the definition of Configuration Management Plan for more information.

Change Implementation Notice

(Implementation Phase) The Change Implementation Notice records formal requests and approvals for any changes to a system made during the Implementation Phase. Use it to document user requests for fixes to problems and to limit misunderstandings between the end-user and the system programmers. The Change Implementation Notice is a part of the larger change control process, documented in the Configuration Management Plan.

The Change Implementation Notice may include:

- Request Initiator
- System Name
- System Location
- Change Requested
- Urgency of Request
- Approval/Rejection
- Action and POC

Change Tracking Log

(Acquisition/Development Phase: Control Gate 4) The Change Tracking Log provides a continually updated list of proposed, approved, and rejected changes. Standard entry information includes a description of the proposed change, the status history, and the final disposition, noting dates and responsible parties. Every project will have different needs for the Change Tracking Log, therefore it is important to consider what information is important to track.

The Change Tracking Log may include:

- Item identifiers
- Dates, including opened, due, and closed
- Responsible parties

- Description of change
- Response/recommendation for implementation
- Actions proposed and taken
- Final disposition
- Notes and comments

Closeout Certification

(Termination Phase) A Closeout Certification documents and verifies the formal completion of all processes and steps involved in system termination. The System Owner and other relevant stakeholders must sign the Closeout Certification.

Concept of Operations

(Definition Phase: Control Gate 2) The Concept of Operations (CONOPS) is a high-level, user-oriented document that quantitatively and qualitatively describes the characteristics of the proposed system and the operational environment in which it will function. The CONOPS has the following objectives:

- Describe the envisioned solution (from a business and technical perspective).
- Clarify potentially vague and ambiguous requirements from users.
- Provide a foundation to support constructive dialogue among constituent users.
- Support the decision-making process that determines how to develop the system solution.

The target audience of the CONOPS document comprises users who either interact with the existing system or support the system operations from a business or technical perspective.

The Concept of Operations may include:

- Project Description and Overview
- Goals and Objectives of New System
- Rationale for New System
- Major Processes and Functions
- Process Flow of System
- High-Level Functional Requirements
- Requirements Traceability
- High-Level Operational Requirements
- Deployment and Support Requirements
- Configuration and Implementation
- System Environment Evaluation
- Classes/Categories of Users
- User Classes Mapped to Functional Features
- Sample Operational Scenarios
- Operational and Organizational Impacts
- Potential Risks and Issues

Conceptual Solution Architecture

(Definition Phase: Control Gate 2) The Conceptual Solution Architecture diagram depicts an IT system and its interfaces and information flows at a high level. The details of the system design will be planned and documented later in the SLC as part of the System and Software Design documents.

The conceptual solution architecture should show the high-level target ("to-be") information flows and interfaces among:

- Producers and consumers of data
- Systems to help users exchange, process, transform, and use data
- Data bases, data marts, and data warehouses used to store data

Template: Conceptual Solution Architecture template. This template's format may be either reused or modified to meet a segment/program's unique needs.

Configuration Management Plan

(Acquisition/Development Phase) Managing and controlling changes to a system's established configuration is critical to project success. System change requests should be evaluated for risk and impact to the project's business objective, schedule, and budget before accepting and implementing the change. The Configuration Management Plan describes the process for reviewing and approving proposed changes to the system configuration baseline, defining approval levels for authorizing changes, and providing a method to validate approved changes. A properly implemented configuration management system, including change control processes, accomplishes three main objectives:

1. Establishes an evolutionary method to consistently identify and request changes to established baselines, and to assess the value and effectiveness of those changes
2. Provides opportunities to continuously validate and improve the project by considering the impact of each change
3. Provides the mechanism for the project management team to consistently communicate all changes to stakeholders

The CM Plan may include:

- System Overview
- Configuration Items (CIs) within the CM Plan
- Baseline identification (technical characteristics of each CI)
- Roles, responsibilities, and relationships
- Request for change control and problem reports classification
- Change Control procedures and forms
- Problem resolution tracking
- Setup and operation of a Change Control Board
- Measurements (used to measure status of CM activities)
- Configuration status accounting
- Configuration Management Libraries
- Project release management
- Configuration audits
- Tools
- CM milestones
- Training approach

- Version Description Documentation
- Waivers

Contingency Plan/COOP

(Acquisition/Development Phase: Control Gate 4) The Contingency Plan is a part of the overall EPA Continuity of Operations Plan (COOP), which details EPA response to an incident that impacts agency business operations, personnel, and infrastructure. The critical business processes of EPA are heavily dependent upon its information technology (IT) resources. The Office of Environmental Information (OEI), which provides information management and IT infrastructure services throughout EPA, recognizes the potential financial and operational losses from service interruptions and the importance of preparedness for system contingency operations.

In addition, to achieve compliance with mandates from the Office of Management and Budget (OMB), the National Response Team (NRT), and guidance from the National Institute of Standards and Technology (NIST), an EPA COOP must be developed and implemented. Furthermore, it is essential that System Owners have, or conform to, a system Contingency Plan (CP) integrated with the overall EPA COOP. The Project and System Manager should use the CP to respond to any incident that renders IT systems partially or completely inoperable. The Contingency Plan is the repository for business continuity and disaster recovery information, tasks, and procedures to use when responding to interruptions of EPA normal business operations and services

The Contingency Plan may include:

- Purpose and scope of plan coverage:
    - Overview of system operations
    - Emergency response procedures
    - Backup arrangements, procedures, and responsibilities
    - Post-disaster recovery procedures and responsibilities
- General facility/System/Owner identification information
- Core plan
    - Discovery (problem/incident assessment and notification)
    - Initial response (procedures)
    - Sustained actions (covers transition from initial response)
    - Termination and follow-up (response close-out process)
- Detailed system design and operation information
- Appendices (detailed procedure, facility and system information)

Contract

Refer to the definition of Acquisition Package for more information.

Cost Benefit Analysis

(Acquisition/Development Phase: Control Gate 3) The Cost Benefit Analysis is a formal economic analysis and evaluation, from a cost and benefits perspective, of alternative solutions to meet the stated need. The OMB Circular A-94 details the technique, Benefit-Cost Analysis (BCA), for conducting formal economic analysis of government programs or projects. For projects or programs with the same benefits, use cost-effectiveness analysis to compare alternatives. A program or project is cost effective if, on the basis of life cycle cost analysis of competing alternatives, it is determined to have the lowest costs expressed in present value terms for a given amount of benefits.

> **Note:** An urgent business need or external stakeholder pressure may dictate the use of an alternative development work pattern that may not identify, evaluate, or document alternative solutions. If no feasible alternatives are identified, tailor the BCA methodology to evaluate the costs and benefits of the proposed IT investment without extensive analysis of alternative solutions.

CROMERR

Acronym for Cross-Media Electronic Reporting Regulation. This regulation sets performance-based, technology-neutral standards for systems that states, tribes, and local governments use to receive electronic reports from facilities they regulate under EPA-authorized programs, and requires program modifications or revisions to incorporate electronic reporting. CROMERR also addresses electronic reporting directly to EPA.

Data Conversion Plan

(Acquisition/Development Phase) The Data Conversion Plan describes the strategies involved in moving data from its existing structure, storage type, or application into another environment prior to a system change. The plan includes a series of steps to design the conversion approach, plan the physical extraction of data, cleanse the data to prepare it for data load, load the data into the new environment, and verify the accuracy of data that has been loaded.

> **Note:** The original system's functional requirements need to be re-examined with respect to the condition of the system before conversion to determine if the original requirements are still valid.

The Data Conversion Plan may include:

- Purpose, Scope, Points of Contact
- System Overview
- Conversion Overview:
    - Description
    - Type
    - Strategy
- Conversion Planning:
    - Tasks and Procedures
    - Schedule
- Security
- Support
    - Hardware
    - Software
    - Facilities
    - Materials
    - Personnel

Data Standards

(Acquisition/Development Phase: Control Gate 3) Data standards define the technical specifications for the definition, naming, and use of data within the system. In a COTS scenario, they are vendor-specific. They are drafted during the System Planning step of the Definition phase and reach maturity in the Design step of the Acquisition/Development phase.

Deactivation Plan

(Termination Phase) During the Termination phase, the operation of the system ends in a planned, secure, orderly manner, including archiving system components and data or incorporating them into other systems as required. The Deactivation Plan captures the system's orderly shutdown process.

The Deactivation Plan provides instructions on how to disassemble, package, and ship the entire system to a designated site at the conclusion of operations, securely dispose of hardware and software as appropriate, and to restore the original system operations if needed.

Delivered System and Modified Software

Once testing of the system and application software is complete, organize the completed software and any hardware and media needed to store and support the application in preparation for implementation.

Development Decision Paper

(Acquisition/Development Phase) The EPA system life cycle requires the creation of decision papers to document project issues presented to management and the decisions and approvals needed to move a project through the life cycle phases. The Project Manager is responsible for maintaining Decision Papers with the set of documents as a record of decisions made during the course of a project. The level of detail contained in a decision paper should be appropriate to the system's categorization.

The Development Decision Paper, also known as the CG3 Decision Memo, documents the analysis that took place to support the decision to move the project into development, and details the process used to obtain project approval. Additionally, it identifies key stakeholders along with their roles in the decision process.

The Development Decision Paper may include:

- Overview of project concept:
    - Description/deliverables
- Assumptions and constraints
- Stakeholders
- Pre-assigned resources
- Schedule of events/milestones
- Decision to Proceed:
    - Decision process overview
    - Authorization memoranda (attach work product/deliverable approvals)

Feasibility Study

(Definition Phase: Control Gate 2) The Feasibility Study analyzes whether the information management need or opportunity is beyond the capabilities of existing systems and whether developing a new system offers a promising approach. It evaluates the degree to which the requirements, design, or plans for a system or component can be implemented under existing constraints. OMB Circular A-11 Capital Programming Guide defines the feasibility study as an evaluation of asset options. OMB notes that agencies should conduct market research to determine the feasibility of various capital asset alternatives that are available in the market to satisfy the requirements. The Feasibility Study should place emphasis on generating innovation and competition from private industry and on the use of commercial items and non-developmental items to meet the mission needs.

The Feasibility Study may include:

- Description of information management need
- Explanation of system requirements and design
- Evaluation criteria:
    - Availability
    - Affordability
    - Costs and benefits
    - Risks
- Alternative descriptions:
    - Alternative model (data modeling from current system to proposed)
    - Narrative description
- Recommendations

Functional Requirements Document

(Definition Phase: Control Gate 2) The Functional Requirements Document (FRD) specifies the functions that a system must be able to perform. System functional requirements typically form the basis for development of a statement of work used for acquiring products and services. Requirements represent conditions that a system or system component must meet for the customer/user to find the application satisfactory. Requirements provide a tool for measuring project success, describe the capabilities the application must provide in functional terms, provide a clear understanding among stakeholders, and enable the testing and verification of system development results.

The Functional Requirements Document may include:

- System Description
- Hardware Configuration
- Software Requirements:
    - Data Requirements (including an application data model)
    - Functional Process Requirements (processes performed by application)
    - Operational Requirements (non-business characteristics)
- Requirements for:
    - Security
    - Audit trail
    - Data currency
    - Reliability
    - Recoverability
    - System availability
    - Fault tolerance (operational ability during a failure)
    - Performance
    - Capacity
    - Data retention
- Requirements Traceability Matrix
- Project Reviews
- Test Requirements

Impact Assessment

(Acquisition/Development Phase: Control Gate 4) The introduction of a new IT system into an organization leads to a change in the way that organization does business. In some cases the change is very small, but in most cases the IT system changes the current operations, procedures, and daily activities of the business.

The Impact Assessment may include:

- A description of the proposed change
- The extent of the change
- Key differences between the current state and proposed state
- Potential impacts of the key differences
- Risks associated with the change

Implementation Decision Paper

(Implementation Phase) The EPA system life cycle requires the creation of decision papers to document project issues presented to management and the decisions and approvals needed to move a project through the life cycle phases. The Project Manager is responsible for maintaining decision papers as a record of decisions made during the course of a project. The level of detail contained in a decision paper should be appropriate to the system's categorization.

The Implementation Decision Paper, also known as the CG4 Decision Memo, documents the analysis that took place to support the decision to move the project into implementation, and details the process used to obtain project approval. Additionally, it identifies key stakeholders along with their roles in the decision process.

The Implementation Decision Paper may include:

- Overview of Project Concept:
    - Description/deliverables
- Assumptions and Constraints
- Stakeholders
- Pre-Assigned Resources
- Schedule of Events/Milestones
- Decision to Proceed:
    - Decision process overview
    - Authorization memoranda (attach work product/deliverable approvals)

In-Process Review

(Operations and Maintenance Phase) The In-Process Review, also known as an Operational Analysis, involves collecting information about a system's performance and comparing it to the baseline performance measures (as defined in system planning and OMB Exhibit 300 documentation). This review formally evaluates how well an investment meets strategic and business objectives, customer needs, and system performance goals. Reviews should occur at pre-determined milestones or on a cyclical basis to ensure the investment continues to meet needs and performs effectively.

The In-Process Review should determine whether the asset is meeting program objectives and the needs of the owners and users, as well as performing within baseline cost, schedule, and performance goals. Such reviews provide data to enable system owners and resource managers to optimize performance of assets or acquire new assets, if necessary. Reviews should contain easy-to-understand information intended for non-technical audiences that managers can use to make sound decisions. Review reports

may include trend analysis, graphs, scorecards, or other ways of easily portraying information. They are very broad in scope and cover a wide range of performance criteria.

In-Process Review performance areas may include:

- Strategic goals
- Customer satisfaction
- Business results
- System operations
- System alignment with business processes
- System value
- System time, cost, service, quality

Information Preservation/Media Sanitization

Information preservation activities ensure that the retention of information conforms to current legal requirements and to accommodate future technology changes that may render the information retrieval method obsolete. Media sanitization ensures that data cleansing takes place before removing media from the system, through deletion, erasure, or writing over existing data, commensurate with the security level of data maintained on the media. The Project Manager is responsible for documenting specific procedures, rules, and regulations regarding information preservation and media sanitization in the System Security Plan. The Project Manager is also responsible for ensuring media sanitization is conducted during any phase when media is removed from the production system.

Initiation Decision Paper

(Definition Phase) The EPA system life cycle requires the creation of decision papers to document project issues presented to management and the decisions and approvals needed to move a project through the life cycle phases. The Project Manager is responsible for maintaining decision papers as a record of decisions made during the course of a project. The level of detail contained in a decision paper should be appropriate to the system's categorization.

The Initiation Decision Paper, also known as the CG1 Decision Memo, documents the analysis that took place to support the decision to initiate the system development project, and details the process used to obtain project approval. Additionally, it identifies key stakeholders along with their roles in the decision process.

The Initiation Decision Paper may include:

- Overview of Project Concept:
    - Description/deliverables
- Assumptions and Constraints
- Stakeholders
- Pre-assigned resources
- Schedule of events/milestones
- Decision to Proceed:
    - Decision process overview
    - Authorization memoranda (attach work product/deliverable approvals)

Integrated Project/Program Team (IPT) Charter

(Definition Phase: Control Gate 2) The Integrated Project/Program Team (IPT) is a multi-disciplinary team led by a project/program manager that is responsible and accountable for planning, budgeting, procurement and life-cycle management of the investment to achieve its cost, schedule, and performance goals. Team skills typically include: budgetary, financial, capital planning, procurement, user, program, architecture, earned value management, security, and other staff as appropriate.

The IPT Charter is a document that defines the mission, leadership, and membership of the Integrated Project/Program Team. The IPT Charter should address the following items:

- Need, Purpose, and Scope
- Outcome, Outputs, and Performance
- Authority
- Key Stakeholders
- Membership (names and specialties/functions)
- Decision Process/Team Governance
- Meeting Management
- Deliverables
- Charter Expiration Date
- Signatures/Approvals

IT Investment Business Case

(Definition Phase: Control Gate 2) The Capital Planning and Investment Control (CPIC) process is a structured, integrated approach to managing Information Technology (IT) investments mandated by the OMB under OMB Circular A-11. The intent of the EPA CPIC process is to ensure that all EPA IT investments align with the EPA mission and support business needs, while minimizing risks and maximizing returns throughout an IT investment's life cycle.

The IT Investment Business Case is the mission and budget justification document used by EPA to determine whether or not to incorporate a project into the Agency's IT investment portfolio.

The IT Investment Business Case is a critical product in the system selection review which occurs at Control Gate #2 as the system completes the Design phase. During Control Gate #4, reviewers consider an updated IT Investment Business Case when making the decision to terminate or modify a system.

Operations Manual

(Acquisition/Development Phase: Control Gate 3) The Operations Manual, or Systems Administration Manual, provides system administrators and system operators with a detailed operational description of the system and its associated environments (e.g., hardware operations, networking environment, host environment, and relevant procedures). This manual is an essential resource for administrators to operate a system, perform maintenance, shutdown or restart systems, closeout systems, etc.

The Operations Manual may include:

- System overview
- Detailed operational description of system
    - Associated environments
    - System functions/features

    - Operational procedures
- Roles and responsibilities
- POC information
- References to technical specifications documents

Post-Implementation Review Report

(Implementation Phase) The Post-Implementation Review (PIR) Report is an assessment of an IT project's implementation process. It also identifies lessons learned that will help to improve the understanding of an investment's business case and lead to process improvement. The PIR is a review of an IT investment or project that compares the actual cost, schedule, performance, and other results achieved against the conditions that existed prior to the implementation of the investment. The Clinger-Cohen Act mandates the planning and conducting of a PIR to satisfy the requirement of the "Evaluate" phase of the Capital Planning and Investment Control (CPIC) process after an investment or project is complete and fully operational.

The PIR usually occurs either after a system has been in operation for six months or immediately following investment termination. The review should provide a baseline to decide whether to continue the system without adjustment, to modify the system to improve performance or, if necessary, to consider alternatives to the implemented system. At a minimum, a PIR Report should address stakeholder and customer/user satisfaction, mission/program impact, technical capability, and lessons learned.

The PIR Report may address:

- Mission alignment
- IT architecture including security and internal controls
- Performance measures
- Project management
- Customer acceptance
- Business process support
- Financial performance
- Return on investment
- Risk management
- Select and control phase performance ensuring initiative success
- Gaps or deficiencies in the process used to develop and implement the initiative
- Best practices applicable to other IT initiatives or the CPIC process

Post-Retirement Review Report

(Termination Phase) The Post-Retirement Review is conducted at the end of the project's life cycle after the system has been terminated. This phase-end review should be conducted within six months after retirement of the system to notify all parties that the final shutdown of the system has occurred. The Post-Retirement Review Report also documents the lessons learned from the retirement and archiving of the terminated system.

Privacy Impact Assessment (PIA)

(Definition Phase: Control Gate 2) EPA requires that Privacy Impact Assessments (PIAs) be conducted on all new or modified internal systems that collect, maintain, or disseminate personally identifiable information (PII). The PIA is a reporting requirement of the Federal Information Security Management Act (FISMA) and ensures that handling of PII conforms to all applicable privacy laws, regulations, and policy requirements.

In general, a PIA assesses the privacy impacts of the data contained in the information system, the individuals who will have access to the data, other IT systems that interface with or use the data, how the data is

organized and retrieved, and the maintenance and administrative controls necessary to secure the data.

The Project Manager is responsible for ensuring the PIA is updated whenever a change to the system that impacts privacy information occurs.

The Privacy Impact Assessment identifies:

- The nature and source of the information being collected
- The purpose of collecting the information
- The intended use of the information
- With whom the information will be shared
- How the information will be stored and secured
- Opportunities for consent
- Whether a System of Records Notice (SORN) will be created

Project Management Plan (PMP)

(Definition Phase: Control Gate 1) Prepare the Project Plan, also referred to as the Project Management Plan, for all projects, regardless of size and scope. The Project Management Plan is the primary source of information on how to plan, execute, monitor, control, and close a project.

Several other work products that provide the foundation for project planning support the Project Plan. Those work products include the Project Schedule, Responsibilities, and Work Breakdown Structure (WBS). The Project Plan integrates these individual work products into a comprehensive view of the project, including details on the scope definition, work breakdown, activity sequence and schedule, duration estimates, cost estimates, quality assurance, human resources, management structure, stakeholders, risk identification and mitigation, performance measurement, milestones, and contracting plans.

The Project Plan is a critical work product for all Control Gate reviews.

The Project Plan may address:

- Description of Project
- Project Team Organization and Responsibilities
- Scope Definition
- Project Work Breakdown Structure
- Schedule
- Project Deliverables
- Cost estimates
- Quality Assurance
- Acquisition
- Communication
- Project Standards and Procedures
- Risk Management
- Project Closure

Project Risk Management Plan

(Definition Phase: Control Gate 1) The Project Risk Management Plan describes how to identify, evaluate, mitigate, control, and track project risks throughout the life of the project. It identifies individuals or groups responsible for risk management, and describes how to communicate risks to various project stakeholders.

The Project Risk Management Plan may include:

- Methodology (approaches, tools and data for performing risk management)
- Risk identification procedures
- Roles and responsibilities
- Budgeting
- Timing
- Risk categories
- Risk definitions and probabilities
- Probability and impact matrix
- Stakeholder tolerances
- Reporting formats/requirements
- Tracking

Quality Assurance Plan (QAP)

(Acquisition/Development: Control Gate 4) The Quality Assurance Plan (QAP) details how an organization will evaluate performance on work throughout the life cycle of a system development project. The QAP defines the Quality Assurance (QA) and Quality Control (QC) processes for project work. Quality Assurance is a planned and systematic process necessary to provide adequate confidence that a project is following organizational processes and that an item or product conforms to established technical requirements. Quality Control comprises a set of activities designed to evaluate the quality of developed or manufactured products.

The QAP defines the QA performance measures and roles and responsibilities. It documents how the project will determine that the delivered products satisfy contractual agreements, meet or exceed quality standards, and comply with SLCM processes. Quality assurance activities typically include validation and verification activities to confirm the correctness of the software, and also process audits of the various groups involved in software development.

The Quality Assurance Plan may include:

- Roles and Responsibilities (responsibilities, scheduling, notification, and conduct)
- Quality Assurance Processes
- Audits:
    - Process audit schedule
    - Product audit schedule
- Verification:
    - Peer reviews
    - Subject Matter Expert (SME)/Technical reviews
    - Editorial reviews
    - Quality reviews
- Verification:
    - Code reviews
    - Testing
- Performance-Based Measures

Re-Authorization to Operate

The Re-Authorization to Operate is an official management decision (sign-off) granted by a senior Agency official to authorize the operation of a system. By re-authorizing the system to operate, the approver

explicitly accepts any risk to Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals that may occur in the implementation of an agreed-upon set of security controls.

A system must receive an Authorization to Operate during the Control Gate #4 review in order to move into the Implementation phase. The system must have changes that may occur in the Implementation phase reviewed, and re-authorization of the system must take place before the system can move into the Operations and Maintenance phase.

The Re-Authorization to Operate includes:

- Date of issuance, effective date close
- Senior Agency official signature and date

Records Management Plan

(Definition Phase) The Records Management Plan is also referred to as a "records schedule."

Records management is a critical activity mandated by the Clinger-Cohen Act, Freedom of Information Act (FOIA), and various Federal Records Acts. EPA has over 400 Agency records schedules that provide mandatory instructions on how long to keep records (retention) and when they can be destroyed and/or transferred to alternate storage facilities (disposition).

In most cases, EPA System Managers select an existing records schedule that applies to the types of records stored in and associated with the system. The System Manager does not need to develop a new records schedule if an appropriate EPA records schedule exists. However, an existing records schedule may require modification or the system may need a new records schedule created. In this case, System Managers should contact their Records Liaison Officer for assistance.

Request for Proposal

Refer to the definition for Acquisition Package for more information.

Requirements Specifications (Hardware, Software, and Interface)

(Definition Phase) The Requirements Specifications state the requirements for a system or component. Requirements specifications typically include functional requirements, performance requirements, interface requirements, design requirements, and development standards. Measures of complete requirements include the degree to which they are specific, measurable, and testable. For the purposes of these work products, hardware, software, and interface requirements are typically identified as system constraints.

The Project Manager is responsible for ensuring the Requirements Specifications are finalized at the end of the Requirements phase. Executive Management should also formally approve it at the end of the phase. If changes are necessary during subsequent phases, the Project Manager is responsible for ensuring updating, documenting, and approving the reasons for the needed change as part of the change control process.

The Requirements Specifications may include:

- Data Requirements
- Functional Requirements
- Interface Requirements

- Design Requirements
- System Performance Requirements
- Security Requirements
- Maintainability Requirements
- User Interface Requirements
- Development Standards
- User Documentation Requirements

Requirements Traceability Matrix

(Definition Phase) The Requirements Traceability Matrix is a table that documents the links (relationships) among the requirements under development and the related process (i.e., requirements as they relate to design, code, and testing). The use of a traceability matrix allows for the tracking of completed tasks, what systems they interact with, and the impact of changes on all other components under development (For example, changing a design element may require new code specific to that design, as will testing of the new design, new code, etc.).

The Requirements Traceability Matrix may include:

- Requirements identification
- Requirements specification
- Design specification
- Function specification
- Source code/code files
- Test cases

Retirement Decision Paper

(Termination Phase) The EPA system life cycle requires the creation of decision papers to document project issues presented to management and the decisions and approvals needed to move a project through the life cycle phases. The Project Manager is responsible for maintaining decision papers as a record of decisions made during the course of a project. The level of detail contained in a decision paper should be appropriate to the system's categorization.

The Retirement Decision Paper documents the analysis that took place to support the decision to retire the system, and the process used to obtain retirement approval. Additionally, it identifies key stakeholders along with their roles in the decision process.

The Retirement Decision Paper may include:

- Overview of Project Concept:
    - Description/deliverables
- Assumptions and constraints
- Stakeholders
- Pre-assigned resources
- Schedule of events/milestones
- Decision to Proceed:
    - Decision process overview
    - Authorization memoranda (attach work product/deliverable approvals)

Retirement Plan

(Termination Phase) Retirement refers to permanent removal of a system or component from its operational environment along with product support. The Retirement Plan includes the plans necessary for an orderly closeout of the project. The plan ensures the proper archiving of system components and data or their incorporation into other systems. This may include shutting down the active support for the system provided by the operations and maintenance organizations.

The Retirement Plan may include:

- Project information
- Project goals
- Preparation of a final report
- Why project is being closed
- Post-project tasks
- Project closure recommendations
- Project approvals

Security Accreditation Package

(Acquisition/Development Phase: Control Gate 4) The Security Accreditation Package contains certification results in a security assessment report that results in findings and recommendations. To the package contents are the basis for revising and approving the Security Plan and for developing Plans of Action and Milestones (POA&Ms) to correct deficiencies. The approving authority will develop the "Accreditation", which contains their decision to accredit, decision rationale, and any terms and conditions. Until identified deficiencies are corrected and until the system moves into production/implementation, the term "No accreditation" is used. Full accreditation allows for implementation into the production environment.

It is essential for the Certification and Accreditation (C&A) of an information system before it becomes operational.

The Security Accreditation Package may include:

- Approved Security Plan
- Approved C&A memoranda
- Rules of Behavior
- Designation of security responsibilities
- Configuration Management Plan
- Risk Assessment
- Security Test & Evaluation
- Contingency Plan
- Security Assessment Report
- POA&Ms
- Privacy Impact Assessments
- Certifier's Statement

Security Categorization

Refer to the definition for System Categorization for information.

Security Certification and Accreditation

Refer to consult the definition for Security Accreditation Package for more information.

Security Configuration Management

(Operations and Maintenance Phase) Security Configuration Management and control activities identify and evaluate potential security impacts due to changes made to an operational information system or its surrounding environment. During a system's Operations and Maintenance life cycle phase, changes made to the system's configuration can create a need to update security controls, processes, and documentation to avoid any potential risk caused by the change. The Configuration Management Plan should detail the change control processes in place to ensure the identification of changes, their impact evaluation, and the approval process required before implementation. Security considerations should be integrated into the project's change control processes.

Security Plan

The Security Plan describes the plan to meet security and privacy protection requirements for a given project or system. It addresses what is known to date about the impact levels, conceptual information, system architecture, risks, required controls, contingency or continuity of support needs, laws, and penalties that may apply to breach of confidentiality, etc. The Project Manager is responsible for ensuring Security Plans are developed in accordance with the Agency Network Security Policy and relevant authorities, such as the Federal Information Security Management Act (FISMA).

A Security Plan is mandatory for every system, and establishes the security requirements and formalizes the security process for the system.

The Security Plan may include:

- Knowledge of potential impact levels
- Conceptual information system architecture
- Risks
- Required controls
- Contingency or continuity of support needs
- Laws and penalties that apply to breach of confidentiality, etc.
- Hardware and software disposal procedures

Security Risk Assessment

(Definition Phase: Control Gate 2) The Security Risk Assessment determines the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to system security requirements. The certification agent or an independent party prepares the Security Risk Assessment and provides the results of assessing the security controls in the information system listed in NIST SP 800-53 Recommended Security Controls for Federal Information Systems. The security assessment report can also contain a list of corrective actions recommended by the certification agent that will assist the agency with bringing their information systems into full compliance with Federal NIST standards.

Segment Architecture

(Pre-Definition Phase: Control Gate 1) The Segment Architecture is a set of documents that describe the baseline and target states of a Segment, as well as the transition between those states. The Segment Architecture is developed according to the goals and scope defined in the Segment Architecture Charter. The target recommendations that result from a Segment Architecture may lead to either the development of new IT systems and processes or the modification of existing systems and processes.

The Federal Segment Architecture Methodology (FSAM) provides detailed guidance for developing a segment architecture: http://www.fsam.gov/federal-segment-architecture-methodology-toolkit/. In particular, EPA recommends the steps and templates that encompass Business Process and Data Flow Analysis, as described below:

Business Process and Data Flow Analysis
The Business Process and Data Flow Analysis are key to determining the high-level business and information needs of an EPA segment or program area. These processes identify how activities are currently being performed, how information flows throughout these activities, and what are the opportunities for improvement. The improvement opportunities are documented and added to the target.

The following activities and corresponding templates will help in the completion of the Business Process and Data Flow Analysis:

1) Identify and document, in a "swim lane" diagram, all existing ("as-is") high-level business process steps and data flows for the segment/solution.

Depict the flows between the following elements, using a separate swim lane for each:

- Roles (i.e. people, Program Offices)
- IT systems
- Data and information sources.

2) Identify and document strategic improvement opportunities for the business and data architecture. Describe the current state and target state of each improvement opportunity, as well as security/system/infrastructure considerations, relationships and dependencies, and risks/other issues.

3) Identify and document all target ("to-be") high-level business process steps and data flows that reflect the business and data architecture improvement opportunities identified above.

Depict the flows between the following elements, using a separate "swim lane" for each:

- Roles (i.e. people, Program Offices)
- IT systems
- Data and information sources.

Templates:

- As-Is Business Process and Data Flow Swim Lane Diagram
- Business and Data Architecture Improvement Opportunities
- Target Business Process and Data Flow Swim Lane Diagram

Segment Architecture Charter

(Pre-Definition Phase: Control Gate 1) The first artifact that should be created or updated in the Pre-Definition Phase is the Segment Architecture Charter. This artifact, created by the core Segment Team of IT and business subject matter experts, establishes the:

- Purpose, goals and objectives of the project,
- Preliminary scope of the segment,

- Legitimacy of the project,
- Role of each team member,
- Operational ground rules of the core team, and
- Decision-making structure of the core team.

The Segment Architecture Charter establishes the foundation required to effectively identify the business and IT needs that can potentially result in the revision of business processes, or revision of the data architecture, and/or creation of a new system.

Segment Performance Measures (CG 1)

(Pre-Definition Phase: Control Gate 1) The Segment Architecture Performance Measurement Indicators are the key to documenting how the Segment and associated solutions will achieve the target business outcomes. The performance measures are updated revisited throughout the SLC as additional information and requirements become available. The purpose of the performance measures is to identify and track quantifiable metrics that show how the Segment/Solution activities and systems are supporting the targeted business outcomes. Performance Measurement Indicators may cover a wide range of systems, technologies, processes, activities and outcomes within a segment. For segments with CPIC Major investments, performance measurement indicators may be leveraged from the Exhibit 300s.

Listed below are the components of the EPA Segment Performance Measurement Indicators template:

Field name	Description of field
Investment name	Name of the IT investment corresponding to the Measurement Indicator.
Fiscal Year	Fiscal year for the target measurement indicator
Measurement Indicator	Quantifiable performance measurement that reflects the critical success factors of the segment architecture development process
Target	Target value of the measurement indicator
Actual Results	Actual results achieved during the fiscal year
Comments	Further description of the metric or link to relevant information

Template: Segment Performance Measurement Indicators template

Sequencing Plan

(Acquisition/Development Phase: Control Gate 3) The Sequencing Plan provides a roadmap for tracking the development and implementation of an IT system's modules and interfaces. It helps business and system owners plan and manage the implementation of their own systems, as well as understand scheduling impacts due to interfaces with other systems.

The sequencing plan captures the following information:

Significant System Components and/or Modules

- ☐ Start Date: Date when work on this Module began.
- ☐ Target Completion Date: Date when this Module is expected to be completed.
- ☐ Actual Completion Date: Date when this Module was actually completed.

Interfaces between the system and other systems and/or information resources

- ☐ Start Date: Date when work on this interface began
- ☐ Target Completion Date: Date when this interface is expected to be completed.
- ☐ Actual Completion Date: Date when this interface was actually completed.

Template: Sequencing Plan template

Software Requirements Specification

Refer to the definition of Requirements Specifications for information.

Solution Architecture

A Solution Architecture describes how an individual information system will address a business need. It also defines a technical solution to that need that complies with the requirements of the Target Architecture, which is the set of products that portrays the future state of the Agency.

A Solution Architecture is a comprehensive architectural response to a business problem and must address all layers of the Enterprise Architecture, i.e., business and strategy, data, applications and technology, and security.

All systems must create a Solution Architecture, and it is a critical element of compliance for Control Gates #1 and #2.

The Solution Architecture includes:

- Identification of current business processes, data classes, security, applications, and technology currently in use
- Identification of future business processes, data classes, security, applications, and technology required to provide a solution to the business need
- Measures needed to get from current state to the future state, including sequence of activities and identification of gaps

System Design Document

Refer to the definition for System and Software Design Documents for more information.

System and Security Test Plan

(Acquisition/Development Phase: Control Gate 4) The System and Security Test Plan, also referred to as the System Test Plan, describes the specific tests and test cases used to evaluate the system at appropriate points in the system's life cycle. The System Test Plan provides specific details on testing activities that will achieve the testing strategy outlined in the Test and Evaluation Master Plan (TEMP). The security testing portion of the System Test Plan addresses the verification and evaluation of the specific security controls and security requirements outlined in the System Security Plan.

The purpose of the System and Security Test Plan is to establish a test plan for the activities that will verify the system as a high quality product that meets the needs of the business community. System testing verifies that the functional requirements are met; Security testing verifies that security controls are properly implemented and operating correctly according to Agency and NIST SP 800-53 security requirements.

The System and Security Test Plan may include:

- Test activities
    - Scope
    - Content
    - Methodology
    - Sequence
    - Management
    - Responsibilities
- Testing types
    - Unit/module
    - Subsystem integration
    - Independent security
    - Functional qualification
    - User acceptance
    - Beta

System and Software Design Documents (SDD)

(Acquisition/Development Phase: Control Gate 4) The System and Software Design Documents sometimes referred to as the System Design Document (SDD), detail how the system and software requirements will be designed. All requirements should be traceable to the design documents and all design elements should be traceable to specific requirements. The System and Software Design Documents describe the operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interface, detailed design, processing logic, and external interfaces. In conjunction with the Functional Requirements Document, they provide a complete software and system specification of all user requirements and reflect the architect's perspective of the design.

These documents serve as a representation of the system and software, created to facilitate analysis, planning, implementation, and decision-making. Design documents serve as a medium for communicating software design information, and serve as a model or blueprint of the software or system.

The System and Software Design Documents may include:

- System Overview
- System Architecture:

  - Hardware
  - Software
  - Internal communications
- Data Design:
  - Physical data design
- Human-Machine Interface:
  - Inputs
  - Outputs
- Detailed Design:
  - Include sections for each major system or software component
  - Data entry screens
  - Internal communications
- Interfaces with other systems
- System Integrity Controls:
  - Security architecture
  - Security model

System Categorization

(Acquisition/Development Phase: Control Gate 2) System Categorization, also referred to as Security Categorization, is not a standalone work product. It is part of the Security Risk Assessment or the Security Concept Document. A system development project must be categorized according to this framework as part of the system's reporting requirements under the Federal Information Security Management Act (FISMA).

System Categorization is determined using a set of standards for information and information systems that provide a common framework and promote effective management and oversight of information. The basis for system categorization is the potential impact on an organization should certain events occur. These events are ones that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. In conjunction with vulnerability and threat information, use the system categorization to assess the risk to an organization.

System Engineering Management Plan (SEMP)

The System Engineering Management Plan (SEMP) articulates the planning activities and strategy for executing the technical management aspects of the project. It combines features of the Project Management Plan and the SDD; however, the SEMP has a more technical focus and is developed for large systems facing complex technical issues.

The SEMP focuses on the overall plan for the system engineering management of the project by identifying and describing the project organization, roles and responsibilities, overall tasks, and engineering management planning required to control the design, development, fabrication, and tests associated with the project. The SEMP describes technical planning and control, systems engineering processes, and engineering specialty integration. The SEMP should not cover operational aspects of the project.

The System Engineering Management Plan may include:

- Project Organization

- Responsibility and Authority
- Work Breakdown Structures
- Testing and Verification
- Change Control Procedures
- Project Schedule and Milestones
- Functional Analysis
- Requirement Allocation
- Design Optimization/Effectiveness Compatibility
- Logistics Support and Development Standards
- Development Process:
    - Standards
    - Languages
    - Methodologies
- Engineering Environment
- Systems Engineering Tools
- Information Technology Systems Security
- Specialty Engineering
- Integration Design
- Computer Resources Life cycle Management Plan
- Integrated Validation Plan

System Implementation Plan

(Acquisition/Development Phase) The System Implementation Plan describes how to deploy, install, and transition the information system into an operational system. The plan contains an overview of the system, a brief description of the major tasks involved in the implementation, the overall resources needed to support the implementation effort (e.g., hardware, software, facilities, materials, and personnel), and any site-specific implementation requirements.

The System Implementation Plan may include:

- System Description
- System Organization
- Management Overview:
    - Description of implementation
    - Major tasks
    - Implementation schedule
    - Security:
        - System security features
        - Security during implementation
- Implementation Support:
    - Hardware, software, facilities, and materials
    - Personnel:
        - Personnel requirements and staffing
        - Training of implementation staff
    - Performance Monitoring Configuration Management Interface

- Implementation Requirements by Site (multiple sites possible):
    - Site name or identification:
        - Site requirements
        - Site implementation details
        - Rollback plan
        - Post-implementation verification

System Operations and Maintenance Concept

Refer to the definition for System Concept Document for information.

Test Plan and Test Results

(Acquisition/Development Phase: Control Gate 4) The Test Analysis and Test Problem Report documents the results of the testing process and any event that occurs during the testing process that requires investigation. The purpose of this report is to summarize the results of designated testing activities and provide evaluations based on those results.

The Test Plan and Test Results may include:

- Test summary report identifier
- Test Files/Data
- Summary
- Variances
- Comprehensive assessment
- Summary of results
- Evaluation
- Summary of activities
- Reference material (appended, if applicable)

Test and Evaluation Master Plan (TEMP)

(Definition Phase: Control Gate 2) The Test and Evaluation Master Plan (TEMP) defines the overall strategy for ensuring the developed and implemented system conforms to all documented requirements. The TEMP describes the types of testing that will be acceptable for use at various points in the system's life cycle and what constitutes "successful" testing. The System and Security Test Plan defines the specific testing procedures and plans necessary to carry out the strategy outlined in the TEMP.

Test Files/Data

(Acquisition/Development Phase: Control Gate 4) The Test Files and Data consist of the actual test data and files used for system testing and should be part of Test Anal. This may include identifying test items including version/revision level. The work product may specify characteristics of transmittal media, including those that impact hardware requirements or indicate the need for logical/physical transformations before testing can begin.

The Test Files/Data may include:

- Test data and related files
- Preconditions required
- References to:
    - Requirements Specification

  - Design Specification
  - User Guide
  - Operations Guide
  - Incident reports (if applicable)
- Items to be specifically excluded from testing

Test Problem Report

Refer to the definition for Test Analysis and Test Problem Report for more information.

Training Plan

(Acquisition/Development Phase: Control Gate 3) The Training Plan outlines the objectives, needs, and strategy for training end-users on a new or enhanced system. The plan describes activities needed to support development of training materials, schedules, needs, and other tasks.

The Training Plan may include:

- Training strategy
- Scope of training to be provided
- Training topics to be addressed
- Format of training program
- Training materials
- Space requirements
- Proposed training schedule

User Manual

(Acquisition/Development Phase: Control Gate 3) The User Manual contains all essential information for the user to make full use of the system. The manual acts as a central reference point for end users to effectively familiarize themselves with the system's core and specific functions.

The User Manual is a useful resource to familiarize end-users with the system's functions and capabilities through simplified language. It can also be an effective means of communication between developers and users throughout the development of the system.

The User Manual may include:

- Description of system functions and capabilities
- Contingencies and alternate modes of operation
- Step-by-step procedures for system access and use

User Satisfaction Review

(Operations & Maintenance Phase) The User Satisfaction Review is a tool to measure how well an investment meets customer needs. The Reviews often use customer satisfaction surveys to gather and analyze data to help determine an investment's accuracy and reliability.

The User Satisfaction Review not only provides a routine avenue for investment managers to gauge system performance, but also provides users the opportunity to suggest changes or identify problems. The Review results should be used to guide future investment decisions and to inform the In-Process and Post-Implementation Reviews.

User Satisfaction Review components may include:

- User profile (i.e., who uses the system and for what purpose)

- Customer satisfaction survey results
- Customer satisfaction trends
- User satisfaction performance measures
- Qualitative feedback from users
- Recommendations and next steps

Version Description Document

(Implementation Phase) Describe every unique release of a software application (i.e., initial, interim, and final) in a Version Description Document. The Version Description Document tracks the various versions of a software application released into the operational environment. Typical contents include an inventory of system or component parts, identification of changes incorporated into the version, and installation and operating information unique to the version described.

The Version Description Document may include:

- Chart of Revisions and Previous Versions
- Version Description:
    - Inventory of materials
    - Inventory of software content
    - Inventory of incorporated changes
    - Version specific installation and operation instructions

Waivers

(Acquisition/Development Phase: Control Gate 4) In some cases, IT system owners may apply for and be granted an IT Policy Waiver for certain IT policy requirements. Each EPA IT policy and procedure document outlines specific waiver requirements and conditions.

Work Breakdown Structure

(Acquisition/Development Phase: Control Gate 4) The Work Breakdown Structure (WBS) defines and organizes the scope of a project into manageable units, also called work packages. A well-designed WBS includes the appropriate level of detail to accurately manage and track project progress without adding burden to the project team. Many projects use a detailed WBS to assist in performing earned value management (EVM) calculations to assess project performance against planned schedules and costs.

The Project and System Manager is responsible for identifying work packages and assigning duration estimates and dependencies to each work package. This allows Project Managers to determine the critical tasks and dependencies necessary to keep the project on schedule. Assigning resources to work packages provides an organized view of resource scheduling and availability over the life of the project.

The Work Breakdown Structure may include:

- Task activities (work packages)
- Task durations
- Task dependencies and constraints
- Task start and finish dates
- Task assigned resources

Earned Value Management metrics and associated cost data

5. RELATED DOCUMENTS

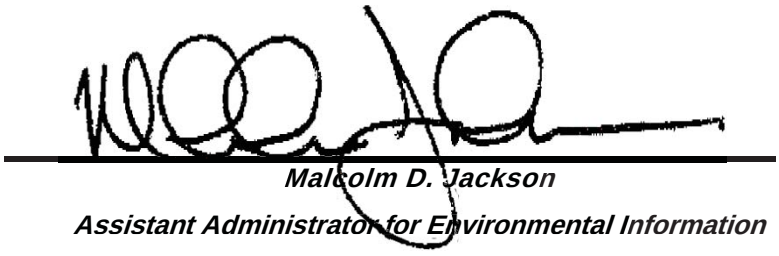
- Capital Planning and Investment Control (CPIC) Policy: http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/2120.pdf
- Capital Planning and Investment Control (CPIC) Procedures for the Office of Management and Budget (OMB) Exhibit 300: *http://intranet.epa.gov/cpic/fy2008/cpic-procedures-sept05.pdf*
- Data Exchange and Collection Procedure: http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/CIO_2122-P-04.0.pdf
- Data Standards Policy: http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/2133.0.pdf
- Enterprise Architecture Procedure: *http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/ea-procedure-final040406.pdf*
- EPA Acquisition Regulation (EPAAR): *http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?sid=52c48b59c02b4481b8576a658c6e69ab&c=ecfr&tpl=/ecfrbrowse/Title48/48cfrv6_02.tpl*
- EPA's Earned Value Management Procedures: http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/2120-p-01.1.pdf
- Federal Cloud Computing Strategy: http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf
- FedRAMP: http://www.gsa.gov/portal/category/102371
- GAO Cost Estimating and Assessment Guide March 2009: http://www.gao.gov/new.items/d093sp.pdf
- Interim Agency Information Security Policy: http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/ansp_interim_policy.pdf
- ISO Standard 27002: http://www.27000.org/iso-27002.htm
- Mobile Access Review Committee (MARC) Resource Page (URL add)
- PMBOK Project Management Institute Guide and Standards: http://www.pmi.org/PMBOK-Guide-and-Standards.aspx
- Privacy Policy: http://intranet.epa.gov/oei/imitpolicy/qic/pdfs/cio2151.0.pdf
- Procedures for Preparing and Publishing Privacy Act System of Records Notices: http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO2151-P-03.1.pdf
- Project Management Templates developed by Deloitte for EPA: http://intranet.epa.gov/otopintr/slcm
- Quality Policy: http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/2106-0.pdf
- Recommended Security Controls for Federal Information Systems and Organizations – NIST 800-53 Rev. 3: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
- Security Considerations in the System Development Life Cycle – NIST 800-64 Rev. 2: http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf

6. ROLES AND RESPONSIBILITIES

See the SLCM Procedures for detailed information on roles and responsibilities during the System Life Cycle.

7. RELATED PROCEDURES, STANDARDS AND GUIDANCE

System Life Cycle Policy
System Life Cycle Procedure
System Life Cycle Web Site



Malcolm D. Jackson
Assistant Administrator for Environmental Information
and Chief Information Officer
U.S. Environmental Protection Agency