IT/IM DIRECTIVE
PROCEDURE

System Life Cycle Management Procedure

Directive No: CIO 2121-P-03.1

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

System Life Cycle Management Procedure

1. PURPOSE

This System Life Cycle Management (SLCM) procedure establishes the Agency's approach for planning, developing and managing information technology (IT) systems, applications and solutions. This procedure assures the Agency's SLCM approach is consistent with EPA and federal IT planning, management and acquisition requirements (e.g., the Clinger-Cohen Act of 1996 and the Federal Information Technology Acquisition Reform Act (FITARA) of 2014), accessibility requirements, security requirements, enterprise architecture principles, enterprise shared services (ESS) approach, Capital Planning and Investment Control (CPIC) requirements and the Agency's Digital Strategy.

2. SCOPE

The Application Review Process cited in the Pre-Definition Phase of the SLCM applies to all new systems or applications that meet the criteria maintained on EPA's Application Review Process (ARP) site. This holds even if the application is not of sufficient size or scope to require strict compliance with the rest of this procedure.

Beyond compliance with the Application Review Process, this procedure applies to:

- EPA programs, acquisitions and solutions with an information technology component (includes interagency or government-wide initiatives). It outlines EPA's required SLCM phases, activities and responsibilities involved in the pre-definition, definition, acquisition, development, implementation, operations and maintenance and termination of EPA IT systems and applications.
- IT systems, applications, projects and general support systems (GSS).
- Custom-developed, commercial off-the-shelf (COTS), or government off-the-shelf (GOTS) and Software as a Service (SaaS) applications.
- Applications, solutions and systems developed on behalf of EPA by other federal agencies or contractors irrespective of where they are hosted, including cloud-based solutions.

Small internal facing applications using Agency-provided COTS/SaaS services where no custom code is being generated and there is no additional procurement outside of Agency provided services, are excluded from the requirements of this policy – with the exception of complying with the Application Review Process.

The processes and controls outlined in this procedure help to appropriately scope and implement IT systems and applications using effective management control practices. They also help to ensure that EPA conducts regular control gate reviews to determine whether to proceed to the next phase of the system life cycle.

This procedure does not mandate a specific system development methodology. However, EPA strongly encourages the use of Agile practices and alignment to the TechFAR, Digital Services Playbook and EPA's Interim Digital Strategy. For information regarding Agile practices, see EPA's Developer Central.

The specific SLCM artifacts and participants in the system life cycle process, reviews and approvals may vary and are dependent on the project scope, architectural decisions and the development methodology. System Owners and System Managers must tailor guidance and work products resulting from this procedure to the needs of their individual project as discussed in Section 6 – Procedure.

3. AUDIENCE

The audience for this procedure includes EPA and contractor personnel participating in the development and management of IT systems and applications, including but not limited to the following:

- Chief Information Officer (CIO)
- Chief Financial Officer (CFO)
- Chief Technology Officer (CTO)
- Senior Information Officials (SIOs)
- Chief Architect (CA)
- Information Management Officers (IMOs)
- Information Resource Management Branch Chiefs (IRM BCs)
- Information Security Officers (ISOs)
- Information System Security Officers (ISSOs)
- System Sponsors
- System Owners
- System Managers
- Project Managers (PMs)
- Senior Information Technology Leaders (SITLs)

4. BACKGROUND

The Clinger-Cohen Act of 1996, the Federal Information Security Management Act of 2002 (FISMA), and Office of Management and Budget (OMB) Circulars A-11 and A-130 require EPA to ensure that system life cycle management procedures are comprehensive, up-to date and follow a controlled, structured approach to managing IT projects.

In addition, FITARA builds upon these laws and directives that require federal Chief Information Officers (CIOs) to do the following:

- Play a significant role in IT decisions, including annual and multi-year planning, programming, budgeting, execution, reporting, management, governance and oversight functions. This includes the review and approval of IT acquisitions.
- Certify that IT investments adequately implement incremental development, as defined by OMB.
- Participate on Agency governance and investment review boards (IRBs) to ensure IT investments align with enterprise and program objectives.

- Monitor the performance of Agency IT investments and advise on the continuation, modification or termination of the investment.

These authorities help federal agencies reduce waste, increase transparency and accountability to taxpayers, and focus on modernizing and streamlining legacy systems and processes by enabling innovation.

This SLCM procedure serves as the mechanism to assure that Agency IT systems and applications support EPA mission goals, consider shared services, adhere to Agency policies and procedures, are controllable and cost-effective, reduce risk, and comply with federal regulations.

EPA's SLCM Procedure integrates system life cycle management with IT investment management requirements and practices, CPIC, enterprise architecture, quality, accessibility and information security requirements. Implementation of these procedures helps to ensure that the Agency delivers accessible, quality and secure IT systems and applications that:

- Meet federal and Agency requirements and mission goals and objectives,
- Promote re-use of applications and shared services,
- Are within budget, and
- Work effectively with the Agency's IT infrastructure.

5. AUTHORITY

Clinger-Cohen Act of 1996 (also known as the Information Technology Management Reform Act of 1996) (Pub. L. 104-106, Division E) https://www.govinfo.gov/content/pkg/USCODE-2011-title40/pdf/USCODE-2011-title40-subtitleIII.pdf

Digital Government: Building a 21st Century Platform to Better Serve the American People, May 21, 2012 https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf

EPA System Life Cycle Management Policy https://www.epa.gov/sites/production/files/2021-02/documents/system_life_cycle_management_policy.pdf

Interim E-Enterprise for the Environment Digital Strategy https://e-enterprisefortheenvironment.net/wp-content/uploads/2019/08/Interim-E-Enterprise-Digital-Strategy-V-2.0.pdf

Federal Cloud Computing Strategy, 2019 https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf

Federal Information Security Modernization Act (FISMA) of 2014, December 2014 https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

Federal Information Technology Acquisition Reform of the National Defense Appropriations Act of 2015 (Pub. L. 113-291), December 2014 https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf#page=148%5D

Government Performance and Results Act of 1993 https://www.congress.gov/bill/103rd-congress/senate-bill/00020

OMB Circular A-130 Revised, July 28, 2016 https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

Executive Order 13011, Federal Information Technology, FR 61-140, July 16, 1996 https://govinfo.library.unt.edu/npr/library/direct/orders/27aa.html

OMB Circular A-11, Preparation, Submission, and Execution of the Budget https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

OMB Memorandum 16-21, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software, August 8, 2016 https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf

OMB Memorandum 19-16, Centralized Mission Support Capabilities for the Federal Government, April 26, 2019 https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-16.pdf

OMB Memorandum 19-18, Federal Data Strategy - A Framework for Consistency, June 4, 2019 https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf

OMB Memorandum 19-21, Transition to Electronic Records, June 28, 2019 https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-21.pdf

Paperwork Reduction Act of 1995 https://www.govinfo.gov/content/pkg/PLAW-104publ13/html/PLAW-104publ13.htm

Privacy Act of 1974, as amended https://www.justice.gov/opcl/privacy-act-1974

Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. § 794 (d)), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998 https://www.govinfo.gov/content/pkg/USCODE-2011-title29/html/USCODE-2011-title29-chap16-subchapV-sec794d.htm

6. PROCEDURE

EPA’s SLCM Procedure provides a structured approach to managing IT projects and includes six phases – Pre-Definition, Definition, Acquisition/Development, Implementation, Operations and Maintenance and Termination. Although the phases are described sequentially, they can be conducted in parallel or combined to follow iterative and incremental models, such as Agile development. System Owners and System Managers must tailor SLCM activities to address the needs of their specific projects.

System Development Tailoring

When developing a tailoring plan, System Owners and System Managers must analyze all SLCM requirements to determine which are necessary for their system or application, which can be combined and consolidated with another requirement, and the level of detail needed for the requirements that are selected as part of the plan.

EPA uses several factors to determine how to tailor a system's development. These include considering the following:

- Requirements for a new system or application versus modernization of an existing system or application
- Size and complexity of the investment
- Build-versus-buy-approach (custom development, COTS/GOTS, SaaS)
- Utilization of "open first," practices to develop or acquire custom-developed code
- Adoption or utilization of EPA ESS
- Agency risk and criticality to EPA's mission
- Whether problem solution and requirements are known/unknown (Agile or Waterfall)[1]
- Whether there is a DevSecOps environment that is available to the user

The following are examples of SLCM tailoring:

- Scheduling phases and activities in concurrent or sequential order
- Repeating or merging phases, activities or work products
- Including additional activities, tasks or work products in a phase
- Changing, combining or expanding activities, their sequencing or implementation timelines
- Changing the development schedule of work products

Senior IT Leaders (SITLs) and Senior Information Officials (SIOs), with the support of the Information Management Officer/Information Resource Management Branch Chief (IMO/IRM BC), are responsible for ensuring compliance with the SLCM procedure and oversight of IT development projects within their organization. IT system or application plans and tailoring must be documented in the Project Management Plan and FITARA request and approved by the SIO (or delegated authority) and/or CIO or CTO per Agency FITARA procedures. See EPA Acquisition Guide Chapter 39.

SLCM Process

The following sections describe the steps included in each phase of EPA's SLCM process. Control gates are also included where the Agency makes formal decisions regarding whether the system or application should proceed to the next life cycle phase. The sections also describe the work products produced during the phase and whether they are

[1] *Refer to Developer Central for information about decision criteria to determine whether Agile or Waterfall methodology should be used for a system.*

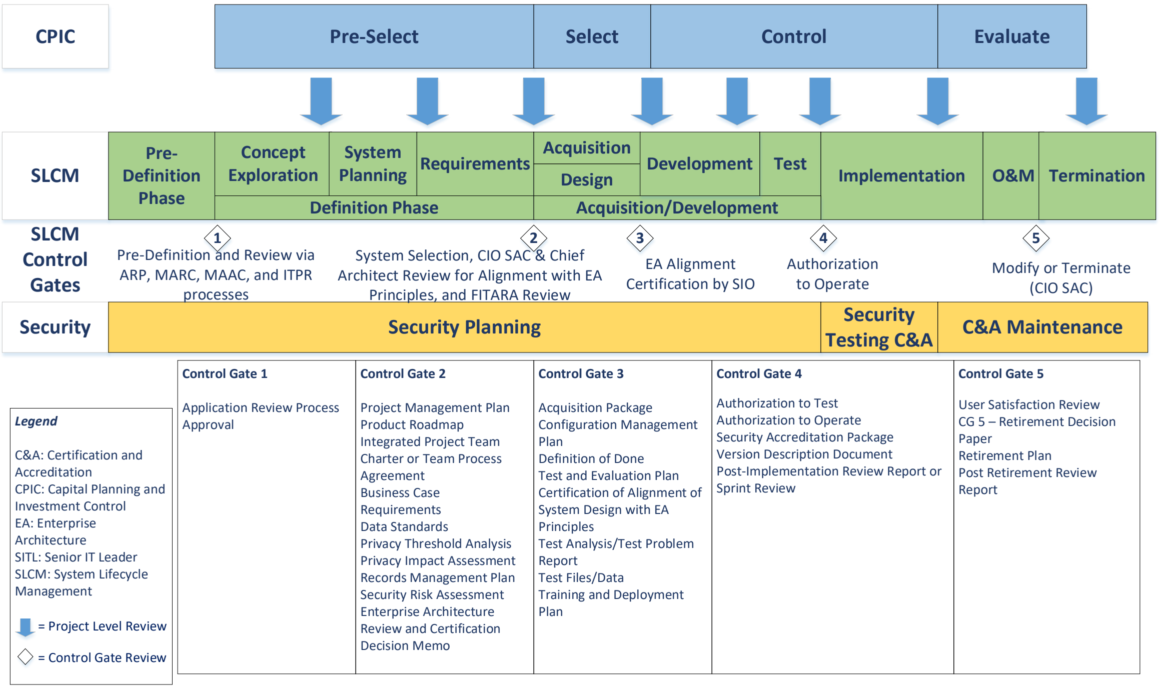
required or are optional per tailoring needs. Some work products may be optional based on the following:

- Project scope
- Instances where the project leverages an approved enterprise solution and is able to inherit work products (i.e., ATOs) from the enterprise service, or
- Architectural Review decisions.

An asterisk (*) in Tables 1-6 denotes these instances.

Work products are included in the SLCM phase in which they are initially developed. However, System Owners and System Managers should update their work products as needed throughout each life cycle phase to reflect system changes. For Agile development, System Owners and System Managers should re-evaluate and adjust their work products at the conclusion of each development sprint as part of the continuous improvement process. This includes evaluating costs to support work, which should align with the Integrated Project Team's (IPT) ability to balance project requirements and budget. Refer to Developer Central for information on Agile project planning and continuous improvement processes. Figure 1 provides a graphical depiction of the SLCM phases and integration with CPIC, FITARA and Security processes.

Figure 1 – Alignment of CPIC, SLCM and Security Procedures



Control Gate 1	Control Gate 2	Control Gate 3	Control Gate 4	Control Gate 5
Application Review Process Approval	Project Management Plan Product Roadmap Integrated Project Team Charter or Team Process Agreement Business Case Requirements Data Standards Privacy Threshold Analysis Privacy Impact Assessment Records Management Plan Security Risk Assessment Enterprise Architecture Review and Certification Decision Memo	Acquisition Package Configuration Management Plan Definition of Done Test and Evaluation Plan Certification of Alignment of System Design with EA Principles Test Analysis/Test Problem Report Test Files/Data Training and Deployment Plan	Authorization to Test Authorization to Operate Security Accreditation Package Version Description Document Post-Implementation Review Report or Sprint Review	User Satisfaction Review CG 5 – Retirement Decision Paper Retirement Plan Post Retirement Review Report

Legend

C&A: Certification and Accreditation
CPIC: Capital Planning and Investment Control
EA: Enterprise Architecture
SITL: Senior IT Leader
SLCM: System Lifecycle Management

⬇ = Project Level Review
◇ = Control Gate Review

Pre-Definition Phase

The Pre-Definition Phase is where business owners determine if the new IT system or application is required to fulfill a business need. This phase helps EPA to avoid duplication, promote the re-use of applications and functionality across the Agency, and increase the use of shared services and open source code.[2] This proposal must be approved by the SIO. The SLCM Procedure stops and no further action is needed if the concept proposal is not approved. The Pre-Definition phase is common to all types of investments regardless of the development methodology selected (Agile or Waterfall) or build versus buy approach or technology selection. Upon completion of this phase, the Agency has made the following decisions:

- There is a need for a new system/application or modernization of an existing system/application, and it should move forward to the Definition phase, or
- The system or application is not needed or could be fulfilled by another existing system or application.
- Whether the business need requires the use or development of a shared service.

The Pre-Definition Phase includes documenting the business need and approval decisions in compliance with the Agency's IT/IM Directive requirements.

The following steps are included in the Pre-Definition Phase:

Step 1 – Identify business need and check READ for similar systems

The SIO or delegated authority of the requesting program or regional office meets with business owners, per internal office governance processes, to discuss and document the need for a new system. This includes the following:

- Checking the Registry of EPA Applications, Models and Data Warehouses (READ), the availability of shared services, and Federal and EPA Code Repositories to identify any similar existing systems or applications instead of investing in a new system.
- Consulting with other SIOs to discuss and refine the business need and identify enterprise impacts.
- Identifying a Project Sponsor who understands the Agency's IT strategy, mission and program and funding/resource requirements.
- Documenting the vision for the application including the scope, timeframe and an assessment of the cost/resource requirements.
- Identifying security and privacy implications, other shared services and federal cooperation needed.

Step 2 – Submit the Application Review Form for review

If the SIO or delegated authority concur with the business need, the requesting organization completes the appropriate Application Review Form and submits it for Agency review/approval as follows:

- For new applications, including custom coded applications, COTS/GOTS tools, SaaS, and EPA public and intranet websites that deliver data dynamically or implement business logic, program/regional offices complete the Application Review Form per EPA's ARP.
- For new mobile applications, the program/regional office completes a Mobile Application Review Form per EPA's Mobile Application Review Committee (MARC) process.

[2] *Refer to Developer Central for additional information on open source code development at EPA.*

- For third-party mobile applications, the program/regional office completes a Mobile Application Review Form per EPA's Mobile Application Approval Committee (MAAC) process.

Step 3 – Approve or reject request (Control Gate 1)

The requested system or application is reviewed per ARP, MARC or MAAC review processes and is either approved or denied. This review is the first Control Gate of EPA's SLCM process. If approved, the application moves on to the Definition Phase. If denied, no further SLCM activities are required. Disputes related to the review process, including concerns about approval decisions, will be referred to the CIO for decision.

Table 1 Pre-Definition Work Products[3]

No.	Work Product	Description	Custom (Build)	COTS/GOTS (Buy) and SaaS (Rent)
1.	Application Review Process Approval	A description of the requested business case and assurance that there are no existing Agency applications that meet the need.	Required	Required

Definition Phase

The Definition Phase confirms the system or application's alignment with Agency architecture principles, establishes a plan for implementation of the MVP (Agile) or the full system (Waterfall) and acquisition of any hardware or software or services needed to complete the project as defined in the Vision/Concept. It also ensures the system/application meets CPIC and FITARA requirements. Essential IT security planning also begins in this phase to ensure that Agency information will be properly protected and available only for appropriate uses.

The phase begins with approval of the System or Application Vision/Concept as documented in the ARP, MARC, or MAAC process. Completion of this phase results in the following:

- Refinement of the system concept to enhance understanding of requirements.
- Understanding of alternatives, costs, and benefits and identification of recommended path forward.
- Documenting the platform for building the new application, if applicable. For Agile projects, this may include planning for a Minimum Viable Product (MVP) or proof of concept.
- Understanding of project risks and proposed mitigation strategies.
- Confirmation of the alignment of the proposed system or application with Agency architecture principles and EPA's Digital Strategy.
- Understanding of the acquisition approach and completion of related IT management and acquisition processes including:

[3] *Asterisk (*) indicates work products that may be optional based on project scope, instances where the project leverages an approved enterprise solution, inherited work products or Architectural Review decisions.*

  - Consideration of modular contracting approaches to support iterative customer-driven software development processes. Refer to EPA's Developer Central for additional information on Agile Acquisition and Modular Contracting.
  - Completion of CPIC processes per EPA CPIC Procedures.
  - Approval of funding to proceed with project as described in EPA's IT Portfolio Review Process.
- For system modernizations, describing the transition plan from the existing legacy system to the modernized application.

Table 2 provides a listing of Work Products produced during this phase. Work Products may be combined based on the project team's tailoring needs. The following steps are included in the Definition Phase:

Step 1 – Conduct concept exploration and system planning and identify requirements

During this step, the requesting office further develops the system or application concept to describe how the business will operate when it is approved and implemented. This step applies to both system modernizations and new system development. It includes verifying the project sponsorship/ownership, defining team members, determining staffing needs and developing the Project Management Plan. It also includes refining the acquisition strategy, assessing the feasibility of system alternatives and analyzing how the system affects privacy and hosting considerations.

To ensure the products and/or services provide the required capability on time and within budget, the requesting office reviews and defines project resources, activities, schedules and tools. Security certification and accreditation activities also begin with the identification of system security requirements and the completion of a high-level risk assessment.

The Definition Phase also includes definition of functional requirements, including but not limited to data requirements, system performance, security and privacy requirements, system integration and Section 508/accessibility. Requirements are defined to a level of detail sufficient for system design to proceed. In Agile development projects, requirements are often documented as Program and Portfolio Backlogs, Epics, Features and User Stories. Requirements need to be measurable and testable and relate to the business need or opportunity identified in the Pre-Definition Phase.

Step 2 – Conduct Enterprise Architecture Review (Control Gate 2)

System or application proposals must be reviewed by the Agency's CA and/or the requesting office's SIO (or delegated authority) to ensure the concept is sound and aligns with enterprise architecture principles, ESS approach, EPA's Digital Strategy and other federal and EPA requirements. Certification of the architecture constitutes the second Control Gate of EPA's SLCM process.

EPA's CA and the program/regional office's SIO review and certify all requests for IT systems or applications that are $250,000/year or more. The requesting office's SIO may review and certify investments that are less than $250,000/year, per CPIC criteria. The CA will also work with program/regional officers to offer guidance and ensure alignment between business needs and architectural considerations. Once the request is certified, an update is provided to the Chief Information Officer Strategic Advisory Committee (CIO SAC) to help identify potential Agency-wide impacts. The requesting office may then proceed with the Agency CPIC and/or FITARA review processes, if required, per Agency procedures.

Table 2 Definition Phase Work Products[4]

Number	Work Product	Description	Custom (Build)	COTS/GOTS (Buy) or SaaS (Rent)
1.	Project Management Plan	Provides the schedule, cost management, quality assurance, human resources, management structure, stakeholders, risk identification and mitigation, performance measurement, milestones, and contracting plans.	Required	Required
2.	Product Roadmap	Provides a forecasted view of long-term system epics and capabilities to be delivered incrementally as working pieces of functionality over time.	Optional*	Optional*
3.	Integrated Project Team Charter or Team Process Agreement	Defines the mission, leadership, membership and roles of the Integrated Project/Program Team. It is updated regularly as the team focuses on continuous improvement.	Optional*	Optional*
4.	Business Case	Documents the mission and budget justification to pursue new system development or modernization and may include the alternatives analysis.	Required	Required
5.	Requirements	Specifies the functions that a system must be able to perform. This includes Section 508 requirements. Refer to EPA's Section 508 Directives. May include the following artifacts if performing custom, Agile development: • Epic • Features • Backlog Refer to Developer Central for more information on Agile development and deliverables.	Required	Required

[4] *Asterisk (*) indicates work products that may be optional based on project scope, instances where the project leverages an approved enterprise solution, inherited work products or Architectural Review decisions.*

Number	Work Product	Description	Custom (Build)	COTS/GOTS (Buy) or SaaS (Rent)
6.	Data Standards	Defines the technical specifications for the definition, naming, and use of data within the system. In a COTS scenario, data standards are vendor specific. They are drafted during the Definition phase and are updated to reach maturity in the Acquisition/Development phase.	Required	Required
7.	Privacy Threshold Analysis (PTA)	Determines if the system will be collecting any personally identifiable information (PII) and if a full Privacy Impact Assessment (PIA) is required.	Required	Required
8.	Privacy Impact Assessment	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.	Required if indicated by PTA	Required if indicated by PTA
9.	Records Management Plan	Provides mandatory instructions on how long to keep records (retention) and when they can be destroyed and/or transferred to an agency-approved storage facility (disposition). The Records Management Plan should be updated throughout the iterative design/development process.	Required	Required
10.	Security Risk Assessment	Defines the security controls that must be implemented during the Development/Implementation Phases based on the Security Categorization of the system.	Required	Required
11.	Enterprise Architecture Review & Certification (CG 2 Decision Memo)	Includes a strategic review of the proposed architecture/technical approach to ensure it aligns with Agency standards, technology platforms, development languages, ESS, EPA's Digital Strategy, and other federal and EPA requirements.	Required	Required

Acquisition/Development Phase

The Acquisition/Development Phase results in the acquisition or development of the system that satisfies the mission need defined in the Definition Phase. Before embarking on this phase, the requesting program/regional office must complete and receive approval per the Agency's FITARA review process as described in EPA's FITARA Procedures.

The Clinger-Cohen Act of 1996 suggests that agencies evaluate using COTS and GOTS products. However, systems based on COTS/GOTS or SaaS products may require some degree of modification, integration, and/or customization prior to implementation. Because work must be properly documented and controlled, it must adhere to the entire SLCM procedure and any additional applicable procedures and standards. If using COTS/GOTS or SaaS, the Project Manager and System Manager will document in the Project Management Plan how and if the vendor's documentation satisfies the requirements of the SLCM procedure.

Testing and certification of security also begins in this phase. System Managers must work with their Information Security Officers (ISOs) and Information System Security Officers (ISSOs) to ensure that the system, application or solution meets security requirements and controls, including NIST requirements. Cloud-hosted systems, applications and solutions must also adhere to the additional controls published by FedRAMP (https://www.fedramp.gov/documents/). Testing ensures the integrity of data and confidentiality mechanisms in COTS/GOTS and SaaS products or custom designed systems.

The following steps are included in the Acquisition/Development Phase.

Step 1 – Complete acquisition

If the project has been selected to conduct an acquisition, this step must be performed. If an acquisition is not required, omit this step. For Agile development projects, refer to Developers Central for guidance on Agile acquisition.

Upon receiving FITARA approval, the requesting program/regional office will perform the following activities in alignment with Agency and federal procurement policies and procedures:

- Prepare Request for Information (RFI)
- Prepare acquisition package and requests for proposals (RFPs) (if needed)
- Perform technical analysis and evaluation of vendor proposals
- Make a request for bid and conduct source selection
- Make contract award

Step 2 – Start design

This step includes designing the physical characteristics of the system or application, establishing the operating environment, defining major system/application components and their inputs and outputs, and allocating resources to life cycle processes. For Agile development, this step may include developing prototypes and MVPs that contains enough features to validate the application vision/concept and gather feedback for future development. See Developer Central for additional information on developing MVPs.

Step 3 – Coordinate with Hosting Provider

This step begins the process of planning for deployment of the system or application into the environment in which it will be hosted. Refer to the EPA National Computer Center's (NCC) ADC guidance for EPA-hosted applications.

Step 4 – Conduct Sprint Review and EA Alignment Certification (Control Gate 3)

The SIO or IMO, if delegated, will validate that the system or application design complies with the System or Application Concept/Vision as approved during the Definition Phase. This constitutes Control Gate 3 of EPA's SLCM process.

Step 5 – Perform development

This step includes translating the requirements and specifications defined during the design step into developed software. In Agile development, development is performed incrementally. Each iteration typically lasts from 1-2 weeks, but exact timeframes are determined by the project team. Each iteration results in tested, working and deployable system functionality that provides tangible value to the user. Product Roadmaps and other project documentation are updated at the conclusion of each development iteration/sprint. EPA strongly encourages following Agile development practices. For more information on Agile development, refer to Developer Central.

Step 6 – Conduct testing

This step includes completing testing in a development environment. Users also complete testing to ensure the system or application meets requirements and can perform required tasks in real-world scenarios. Testing activities must also include verifying Section 508 compliance and accessibility requirements. Refer to EPA's Section 508 Policy and Procedures for additional guidance. Testing will occur iteratively with each development sprint as new functionality is added to the system.

Step 7 – Obtain Authorization to Operate (ATO) (Control Gate 4)

Prior to operating in a production environment, the system or application must undergo certification and accreditation activities per EPA's Information Security and Privacy Directives to ensure the system is ready to move into an operational state. The SIO or delegated authority conducts the Authorization to Operate (ATO) review using the certification package. The Project Manager coordinates with key stakeholders, including the ISO and the ISSO, to ensure that the certification package is complete and there is an approved ATO as part of the Risk Management Framework. The IMO makes the recommendation and then forwards the certification package to the SIO for approval. For more information on the ATO process, refer to EPA's Information Security Assessment and Authorization Procedure. For more information on EPA's Privacy requirements, refer to EPA's Privacy Policy.

Table 3 Acquisition/Development Work Products[5]

Number	Work Product	Description	Custom (Build)	COTS/GOTS (Buy) and SaaS (Rent)
1.	Acquisition Package	Documents that are required to manage the process of acquiring products and/or services.	Required if performing an acquisition	Required if performing an acquisition
2.	Configuration Management Plan	Describes the process for reviewing and approving proposed changes to the system.	Required*	Required*
3.	Definition of Done	A checklist of the types of work the team is expected to successfully complete. The Definition of Done should be revisited and refined regularly as requirements change and the team focuses on continuous improvement. The Definition of Done may be included in another deliverable per the team's preferences.	Required*	Required*
4.	Test and Evaluation Plan	Describes how testing, including Section 508/accessibility testing, is being performed and the expected coverage of the tests. Automated testing scripts may also be used. Refer to EPA's Section 508 Directives for information on Section 508 and accessibility testing.	Required*	Required*
5.	Certification of Alignment of System Design with EA Principles	Control Gate 3 Decision Memo signed by the SIO or IMO (if delegated) certifying that the system or application design conforms to enterprise architecture principles, EPA's Digital Strategy and other federal and EPA requirements.	Required	Required
6.	Test Analysis/Test Problem Report	Documents the results of the testing process. This includes: • Accessibility and Section 508 Testing Results • User Acceptance Testing (UAT) • System Integration Testing (SIT)	Required	Required*
7.	Test Files/Data	Testing documentation, including actual test data and files.	Required	Required*
8.	Training and Deployment Plan	Outlines the objectives, needs, and strategy for training end-users on a new or enhanced system.	Optional	Optional

[5] *Asterisk (*) indicates work products that may be optional based on project scope, instances where the project leverages an approved enterprise solution, inherited work products or Architectural Review decisions.*

Number	Work Product	Description	Custom (Build)	COTS/GOTS (Buy) and SaaS (Rent)
9.	Authorization to Operate and Authorization to Test	Documents the official management decision given by a senior Agency official to authorize testing or operation of an information system.	Required	Required
10.	Security Accreditation Package	The Security Accreditation Package may include: • Security Categorization • 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 • Plan of Actions and Milestones (POA&Ms) • ATO Approval	Required	Required

Implementation Phase

Step 1 - Deploy to production

This step includes installation and operation of the application or system modifications in a production environment. The phase begins after the system completes testing and testers accept the modifications. Activities include notifying end users of the implementation, executing training plans, completing data entry or conversion and confirming of compliance with Section 508 requirements.

Step 2 – Complete deployment requirements

As part of the deployment process, applications and systems also complete security and accreditation activities as required by the hosting provider.

At the completion of the Implementation Phase, the system or application undergoes a post implementation evaluation to ensure that it functions as planned, costs are within the estimated budget and the system/application achieved intended benefits. For Agile development projects, these reviews take place at the end of each development sprint so that the development team can review overall sprint progress and accomplishments. This provides the System Owner with an opportunity to evaluate the current product and determine how to proceed. For Waterfall development, the review may be conducted as a Post Implementation Review as described in Table 4.

Table 4 Implementation Phase Work Products[6]

Number	Work Product	Description	Custom (Build)	COTS/GOTS (Buy) and SaaS (Rent)
1.	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.	Optional	Optional
2.	Post-Implementation Review Report or Sprint Review	An assessment of an IT project that identifies lessons learned, evaluates progress and accomplishments and determines next steps.	Optional	Optional

Operations and Maintenance Phase

This phase ensures that the system operates properly in the production environment and that routine maintenance takes place. During this phase, the Project Manager and System manager maintain schedules and periodically conduct reviews to ensure the health and security of the system and to validate its suitability for meeting the business requirements. The System Manager uses structured techniques to detect defects, capture user satisfaction, review the system requirements and evaluate shared services and the suitability of existing and emerging technologies to continue to meet the mission need. This phase also includes documentation, measurement and tracking of service level agreements (SLAs).

Step 1 – Perform operations and routine maintenance

During this phase, activities include performing routine maintenance in accordance with manufacturer’s guidelines, installing patches and/or updates to system components and making enhancements consistent with user needs/desires and the mission need. Any routine maintenance activity, including patches or updates that impact the user interface, must be manually tested for accessibility. Major new requirements or significant technology refreshment may cause maintenance that requires the system to return to the Definition Phase or Acquisition/Development Phase. For enhancements to existing EPA-developed mobile apps, contact the MARC to determine whether a new concept proposal is required.

Step 2 – Perform Annual System Assessments (Control Gate 5)

This step includes annual assessments of the operational system or application through in-process reviews and post implementation reviews to determine how to make the system

[6] *Asterisk (*) indicates work products that may be optional based on project scope, instances where the project leverages an approved enterprise solution, inherited work products or Architectural Review decisions.*

more efficient and effective or to determine if the system/application is still an Agency need. For CPIC Major and Non-Major Systems, the Modify or Terminate Review will coincide with the annual Information Technology Portfolio Review (ITPR) process.

For most Non-Major systems, the System Manager coordinates completion of this control gate annually or at a frequency that is appropriate for the scope and size of the system. The Project Management Plan should specify the frequency of review. The system manager and IMO provide a recommendation to the SIO for approval to maintain, modify or terminate the system. System Managers must notify the SITLs, SIOs CIO SAC, and CA to ensure awareness of termination decisions.

Table 5 Operations and Maintenance Phase Work Products[7]

Number	Work Product	Description	Custom (Build)	COTS/GOTS (Buy) and SaaS (Rent)
1.	User Satisfaction Review	Measures how well an investment meets customer needs.	Optional	Optional
2.	Control Gate 5 Memo - Retirement Decision Paper	Documents the decision to retire the system. The retirement decision must be documented as part of the ITPR process.	Required	Required

Termination Phase

This phase results in removing an existing system from the product environment at the end of the life cycle process. During this phase, the System Managers retire and close down systems that are redundant or obsolete. Occasionally, a System Manager will use this phase to shut down a major subsystem while the main system remains in operation. The emphasis in this phase is to ensure the packaging and archiving of data, procedures and documentation in an orderly fashion to make it possible to reinstall the system and bring it back to operational status, if necessary, and to retain all data in accordance with EPA policies regarding retention of electronic records. The system retirement activities preserve information not only about the current production system, but also about the evolution of the system through its life cycle.

The System Owner and System Manager ensure performance of the following activities:

- Prepare retirement and disposition plans
- Archive or transfer data
- Archive or transfer system components

[7] *Asterisk (*) indicates work products that may be optional based on project scope, instances where the project leverages an approved enterprise solution, inherited work products or Architectural Review decisions.*

- Sanitize and dispose of equipment/hardware and software media (including system backup and other media)
- Prepare the post-termination review report

The System manager performs the Post-Retirement Review within six months after retirement of the system to notify all parties of the final shutdown of the system. The Post-Retirement Review Report also documents the lessons learned from the shutdown and archiving of the terminated system.

Table 6 Termination Phase Work Products[8]

Number	Work Product	Description	Custom (Build)	COTS/GOTS (Buy) and SaaS (Rent)
1.	Retirement Plan	Plans for an orderly closeout of the project and ensures the proper archiving of system components and data or their incorporation into other systems.	Required	Required
2.	Post-Retirement Review Report	Notifies all parties that the final shutdown of the system has occurred and documents the lessons learned from the retirement and archiving of the terminated system.	Required	Required

7. ROLES AND RESPONSIBILITIES

In support of the SLCM Policy, this procedure includes roles and responsibilities related to the SLCM phases.

Roles with significant responsibilities necessary for implementing the SLCM Procedure include the following:

Chief Information Officer (CIO), who is also the Deputy Assistant Administrator for the Office of Mission Support Environmental Information (OMS-EI), is responsible for the following:

- Approving the SLCM Policy and Procedure
- Reviewing and approving EPA information systems/investments acquisitions that are $1M or greater or that meet other needs for CIO attention
- Ensuring Agency compliance with the SLCM Policy and Procedure by providing guidance and tools to senior level managers for program oversight
- Deciding on requests to waive requirements of the SLCM Policy
- Delegating review and approval of any waivers to the SLCM Procedure to the CTO
- Participating in and providing oversight into Agency annual and multi-year IT planning, programming, budgeting, execution, reporting, management and governance

[8] *Asterisk (*) indicates work products that may be optional based on project scope, instances where the project leverages an approved enterprise solution, inherited work products or Architectural Review decisions.*

- Conducting reviews of Agency’s IT portfolio (PortfolioStat/TechStat sessions) to ensure effective IT and risk management processes
- Certifying that information technology investments adequately implement incremental development, as defined by OMB
- Overseeing Agency governance and investment review boards (IRBs) to ensure IT investments align with program objectives
- Monitoring the performance of Agency IT investments and advising on the continuation, modification or termination of the investment
- Establishing and promoting effective approaches to developing, procuring, deploying and sharing new Agency applications
- Ensuring custom-developed code that EPA develops or procures is shared for broad use across the federal government, subject to limited exceptions
- Resolving disputes identified during the ARP
- Assign responsibility for maintaining and enhancing the ARP workflow tool to support the ARP

Assistant Administrators, Chief Financial Officer (CFO), General Counsel (GC), Inspector General (IG), Deputy Chief of Staff to the Administrator, Associate Administrators, Regional Administrators and Laboratory Directors are responsible for the following:

- Ensuring compliance with SLCM requirements for IT systems within their organizations
- Ensuring the CFO obtains CIO approval to reprogram or move funds for IT resources [as they pertain to congressional notifications]

Chief Technology Officer (CTO), who is also the Director of OMS’s Office of Digital Services and Technical Architecture (ODSTA), is responsible for the following:

- Establishing and publishing procedures, technical operating procedures and standards (TOPS) and guidance supporting the Agency’s SLCM Policy
- Reviewing and approving waivers to the SLCM Procedure
- Reviewing and approving EPA information systems acquisitions less than $1M/year
- Promote adoption of Agile development
- Promote the adoption of EPA enterprise digital and shared service strategies

Chief Information Security Officer (CISO) is responsible for:

- Providing oversight to the Agency’s security assessment and authorization process and status
- Reviewing authorization packages and making authority to operate (ATO) decision recommendations to the CIO

Chief Information Officer – Senior Advisory Committee (CIO SAC) is responsible for:

- Reviewing and recommending enterprise IT strategic direction and criteria for making IT investment decisions
- Advising on IT annual budget as it relates to IT strategic direction
- Advising CIO on requests for new IT solutions, system modernizations and terminations

Information Review Board (IRB), advises and assists the CIO on all matters pertaining to information investment management. The IRB supports the CIO in making recommendations on the appropriateness of information investments and monitors the Agency's IT investments from inception to completion throughout the pre-select, select, control, and evaluate phases of the CPIC program.

Office of Digital Services and Technical Architecture (ODSTA), is responsible for:

- Maintaining the SLCM Policy, the SLCM Procedure and supporting documents and tools
- Monitoring compliance with the SLCM Policy and Procedure through EA, IT Investment Portfolio Reviews and security processes

Office of Information Technology Operations (OITO) Director is responsible for the following:

- Monitoring compliance with the SLCM Policy and Procedure through Agency FITARA and security processes
- Ensuring Agency development processes, including software development, deployment and related information-technology operations comply with the SLCM Policy and Procedure

Chief Architect (CA) is responsible for the following:

- Serving as the technology and business leader for Agency development efforts
- Ensuring development processes align with enterprise architecture principles and the SLCM Policy and Procedure
- Formulating recommendations for system life cycle activities that are informed by technology planning, accessibility planning, mission/business planning, capital planning, security planning, infrastructure planning, human capital planning, performance planning and records planning best practices and requirements
- Ensuring systems development efforts are properly aligned with business requirements, Agency architecture principles, EPA's Digital Strategy and other Agency and federal IT management requirements
- Promoting communication between EPA offices to assess whether they have similar needs and identifying opportunities for collaboration to use shared services and avoid system duplication
- Reviewing and approving Control Gate 2 for Major Systems and Non-Major Systems, as appropriate

Chief Data Officer is responsible for the following:

- Developing and aligning the Agency Data Strategy within IT portfolios
- Identifying priority data assessments for Agency Open Data Plans
- Managing and improving the ability to leverage data as a strategic asset and improve access to data assets

Director of the Office of Mission Support -Office of Acquisitions Solutions (OAS) is responsible for the following:

- Ensuring the incorporation of EPA's SLCM requirements in requests for proposals and contracts, as appropriate
- Initiating contract actions that include IT that are reviewed and approved by the CIO and are consistent with the acquisition strategy and acquisition plans, as appropriate

- Managing and maintaining FAC-P/PM, FAC-P/PM with IT Core-Plus Specialization, FAC-COR certification is awarded and maintained through continuous learning
- Ensuring EPA IT acquisition policies and processes are updated to support an open source software approach to enable sharing of custom-developed code

Senior Information Officials (SIOs) are responsible for the following:

- Ensuring compliance with the SLCM Policy and Procedure for systems within their offices
- Ensuring that the IT used and managed by their organizations supports their business needs and missions and helps to achieve strategic goals
- Reviewing and approving Control Gate 2 for systems/applications that are less than $250,000/year, including ensuring that systems development efforts are properly aligned with business requirements, Agency architecture principles, EPA's Digital Strategy and other Agency and federal IT management requirements
- Reviewing, concurring on, advising on and/or submitting requests to waive SLCM Policy and Procedure requirements, as applicable
- Approving a project to continue through control gates (this may be delegated for smaller systems)
- Meeting with business owners and System Owners to ensure development and management activities are completed in compliance with Agency policy
- Providing feedback and input on implementing the SLCM Policy and Procedure and related review processes

Information Management Officers (IMOs) and Information Resources Management Branch Chiefs (IRM BCs) are responsible for the following:

- Supporting the SIO or delegated authority in ensuring compliance with the SLCM Policy and Procedure for systems within their offices
- Reviewing SLCM documentation
- Reviewing and concurring on requests to waive SLCM Procedure requirements, as applicable
- Reviewing, approving and supporting the development of accessibility documentation, as appropriate
- Reviewing requests for exceptions to sharing custom-developed code

Information Security Officers (ISOs) are responsible for the following:

- Reviewing and supporting the development of SLCM security documentation, as appropriate
- Assigning security responsibilities throughout the system life cycle

Information System Security Officers (ISSOs) are responsible for:

- Maintaining the operational security of the information system
- Assisting in the planning and execution of security-related SLCM documentation

Records Liaison Officers (RLOs) are responsible for:

- Reviewing system documentation to ensure Agency records requirements are properly integrated.

System Sponsors are responsible for the following:

- Authorizing, approving and ensuring adequate funding and resources during the system life cycle of their information systems
- Appointing System Owners and authorizing those individuals to initiate system development
- Reviewing waiver requests, as applicable

System Owners are responsible for the following:

- Monitoring compliance to the SLCM Policy and Procedure and approving tailoring plans
- Appointing Project Managers and System Managers
- Coordinating SLCM development activities with those of the EA, Agency IT Investment Management, including FITARA and CPIC procedures, and information security processes
- Serving as the information owner of the system
- Ensuring compliance with Section 508 requirements during the SLCM process
- Concurring on waiver requests to the SLCM Policy and/or Procedure, as applicable
- Approving completed Control Gate and Project Level Reviews
- Ensuring submission of System or Application Concept Proposals as described in this procedure
- Working with the reviewers of the System or Application Concept Proposal and others to explain the proposed applications and, as necessary, consider alternate approaches
- Sharing custom IT solutions developed within their offices with the Agency Enterprise Code Repository

System Managers are responsible for the following:

- In coordination with the System Owner, ensuring submission of System or Application Concept Proposals as described in this procedure
- In coordination with the System Owner, working with the reviewers of the System or Application Concept Proposal and others to explain the proposed applications and, as necessary, consider alternate approaches
- Providing day-to-day management of the system life cycle process and products within their programs
- Ensuring that systems properly advance through the SLCM phases and activities
- Creating the SLCM Tailoring plan and submitting it for approval by the System Owner
- Recommending and preparing written justification for waivers and documenting them as part of the Project Management Plan
- Preparing Control Gate and Project Level Reviews

Senior Information Technology Leaders (SITLs) are responsible for the following:

Within own organization:

- Providing day-to-day management of system life cycle process and products within their programs

- Ensuring that their systems advance through the SLCM phases and activities
- Recommending and preparing written justification for waiver requests and documenting them as part of the Project Management Plan
- Preparing Control Gate and Project Level Reviews
- Implementing internal policies or procedures to review proposed systems or applications
- Reviewing proposed system applications and either denying the proposal internally or forwarding the proposal to the larger SITL group for review

As part of larger SITL group per the ARP:

- Reviewing proposed applications and discussing compliance with the procedures as documented at the ARP SharePoint Site
- Escalating proposals with unresolved issues to the CIO for resolution
- Providing feedback and input on the implementation of the SLCM Policy and Procedure and related review processes

Project Managers (PMs) are responsible for the following:

- In coordination with the System Owner, ensuring submission of System or Application Concept Proposals as described in this procedure
- In coordination with the System Owner, working with the reviewers of the System or Application Concept Proposal and others to explain the proposed applications and, as necessary, consider alternate approaches
- Managing the defined system through its life cycle
- Incorporating the SLCM documents and work products in the system project schedule
- Assigning resources on the system project team to complete SLCM documents
- Working with the System Manager to prepare Control Gate and Project Level Reviews
- Applying open development practices when developing custom-developed code
- Sharing custom IT solutions developed within their offices with the Agency Enterprise Code Repository

Code Repository Owners are responsible for:

- Requesting a code repository for their team's source code
- Selecting the appropriate open source license for broad reuse across the federal government, subject to limited exceptions
- Selecting the appropriate rights license to provide the government's rights to share custom-developed code with other agencies where EPA is not seeking or able to obtain the rights to publicly release the code
- Managing their team's code repository
- Releasing public code that leverages existing communities in order to:

  (1) foster solutions for shared challenges,

  (2) improve the ability of the OSS community to provide feedback on, and make contributions to, the source code, and

  (3) encourage federal employees and contractors to participate in the OSS community by making contributions to existing OSS projects.

- Fostering open development practices when developing custom-developed code
- Sharing custom IT solutions developed within their offices with the Agency Enterprise Code Repository

Integrated Project Teams are responsible for the following:

- Supporting the Project Manager in the planning, execution, delivery and implementation of life cycle decisions for the project.

Privacy Act Officer is responsible for:

- Reviewing and supporting system development and management as it relates to privacy and personally identifiable information

Mobile Access Approval Committee (MAAC), comprised of members from EPA offices, Office of General Counsel, Office of Information Security and Privacy and, as needed, subject matter experts, is responsible for the following:

- Reviewing and prioritizing third party mobile app requests
- Approving or denying third-party mobile app requests based on legal and security review
- Assisting in the deployment of third-party mobile apps to the EPA's App Catalog for installation on EPA mobile devices.

Mobile Access Review Committee (MARC), comprised of members from Office of Web Communications, Office of Digital Services and Technical Architecture, Office of General Counsel, and the OEI Lead Region and, as needed, subject matter experts, is responsible for:

- Reviewing and approving mobile app concept proposals
- Providing guidance for mobile app development
- Assistant in the deployment of native mobile apps to third-party app stores

8. RELATED INFORMATION

CIO 2130-P/S/G-01.0 Accessible Electronic and Information Technology Standards, Procedures, and Guidance: https://www.epa.gov/irmpoli8/policy-standards-procedures-and-guidelines-accessible-electronic-and-information-technology

CIO Policy 2120.2, Interim Capital Planning and Investment Control Program Policy: https://www.epa.gov/sites/production/files/2021-01/documents/interim_capital_planning_and_investment_control_program_policy.pdf

CIO Policy 2120-P-02.2, Interim Capital Planning and Investment Control Procedures: https://www.epa.gov/sites/production/files/2021-01/documents/interim_capital_planning_and_investment_control_procedures.pdf

CIO 2155.4, Interim Records Management Policy: https://www.epa.gov/irmpoli8/interim-records-management-policy-define-epas-records-management-responsibilities

CIO Policy 2130.1, Section 508: Accessible Electronic and Information Technology (EIT): https://www.epa.gov/irmpoli8/policy-standards-procedures-and-guidelines-accessible-electronic-and-information-technology

CIO Policy 2150.5, Information Security Policy: https://www.epa.gov/irmpoli8/information-security-policy

CIO Policy 2151.1, Privacy Policy: https://www.epa.gov/irmpoli8/epas-privacy-policy-personally-identifiable-information-and-privacy-act-information

Code.gov website: https://www.code.gov

Digital Government Strategy, Digital Government: Building a 21st Century Platform to Better Serve the American People, May 23, 2012: https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html

U.S. Digital Services Playbook: https://playbook.cio.gov/

E-Government Act of 2002, Public Law 107-347: https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Federal Acquisition Regulation (FAR) Part 27 – Patents, Data, and Copyrights: https://www.acquisition.gov/content/part-27-patents-data-and-copyrights

FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

GAO Cost Estimating and Assessment Guide March 2020: https://www.gao.gov/assets/710/705312.pdf

Information and Communication Technology (ICT) Final Standards and Guidelines (36CFR Part 1193 and 1194, January 18, 2017): https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule

NIST Cybersecurity Whitepaper: Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SFDF), April 23, 2020: https://csrc.nist.gov/publications/detail/white-paper/2020/04/23/mitigating-risk-of-software-vulnerabilities-with-ssdf/final

Office of Management and Budget, Federal Cloud Computing Strategy, February 8, 2011: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

Office of Management and Budget Memorandum M-16-21, Federal Source Code Policy, Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software, August 8, 2016: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf

Office of Management and Budget Memorandum M-15-14, Management and Oversight of Federal Information Technology: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf

Office of Management and Budget Strategic Plan for Improving Management of Section 508 of the Rehabilitation Act, January 24, 2013: https://obamawhitehouse.archives.gov/sites/default/files/omb/procurement/memo/strategic-plan-508-compliance.pdf

Open Source Initiative website: https://opensource.org

Recommended Security Controls for Federal Information Systems and Organizations – NIST 800-53: https://nvd.nist.gov/800-53

Section 255 (of the Communications Act of 1934, as amended by the Telecommunications Act of 1996 – 36 C.F.R. Part 1193: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-telecommunications-act-guidelines

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

TechFAR Handbook: https://techfarhub.cio.gov/handbook/

U.S. Environmental Protection Agency Acquisition Guide (EPAAG) Chapter 39 – Acquisition of Information Technology, Section 39.1, Subsection 39.1.1 –Information Technology Acquisition Approval Procedures, April 2018: https://contracts.epa.gov/EPAAG

U.S. Environmental Protection Agency Application Governance SharePoint Site: https://usepa.sharepoint.com/sites/oei_Work/ODSTA/AppGov/SitePages/Process%20Overview.aspx

U.S. Environmental Protection Agency FITARA SharePoint Site: https://usepa.sharepoint.com/sites/oei/OCAPPM/FITARA/SitePages/Community%20Home.aspx

9. DEFINITIONS

Acquisition – The step of the SLCM Acquisition/Development Phase for planning and acquiring the software, hardware and services necessary to construct a planned system.

Acquisition/Development Phase – The SLCM phase where the system is acquired through the purchase of software and services to yield a system that satisfies the mission need established in the Definition Phase.

Agile Development – An adaptable, iterative way to manage development projects. The use of the word Agile in this context derives from the Agile Manifesto.

Application – A system for collecting, saving, processing and presenting data by means of a computer. The term application is generally used when referring to a component of software that can be executed. The terms application and software application are often used synonymously. [NIST Interagency Report 7695]

Assistive Technology – Any item, piece of equipment or system, whether acquired commercially, modified or customized, that is commonly used to increase, maintain or improve the functional capabilities of individuals with disabilities.

Authorization to Operate (ATO) – The official management decision given by a senior Agency official to authorize operation of an information system and to explicitly accept the risk to Agency operations (including mission, functions, image or reputation), Agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Business Case – Describes current business processes, possibly using activity and data models, associates current costs and performance with the models, and identifies gaps between current and desired outcomes. The Business Case develops and evaluates alternatives for improving the business based on readily available information.

Business Justification – Describes the compelling business rationale for developing or modernizing a system.

Capital Planning and Investment Control (CPIC) Process – The decision-making process for ensuring information technology investments. The process integrates strategic planning, budgeting, procurement and the management of IT in support of Agency missions and business needs, as defined in the Clinger-Cohen Act (CCA) of 1996.

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

Commercial Off-the-Shelf (COTS) – A commercial product or information system available to the general public. COTS products contain pre-established functionality, although some degree of customization is possible.

Concept Exploration – The step of the SLCM Definition Phase that establishes the preliminary definitions of the business needs of the system sponsor. It explains the concept in sufficient detail for decision makers to determine whether and how to proceed.

Control Gate – Phase-driven “go/no-go” decision points with reviews of SLCM activities to ensure compliance with appropriate OMB and EPA requirements. A system cannot proceed without a “go” decision by the appropriate senior manager for the specific control gate.

Custom-Developed Code – Code that is first produced in the performance of a federal contract or is otherwise fully funded by the federal government. It includes code, or segregable portions of code, for which the government could obtain unlimited rights under Federal Acquisition Regulations (FAR) Pt. 27 and relevant agency FAR Supplements. Custom-developed code also includes code developed by agency employees as part of their official duties. For the purposes of this policy, custom-developed code may include, but is not limited to, code written for software projects, modules, plugins, scripts, middleware and application programming interfaces (APIs); it does not, however, include code that is truly exploratory or disposable in nature, such as that written by a developer experimenting with a new language or library.

Decision Papers – The result of a phase review that culminates with a decision memo approving the system to progress to the next phase or halting system development until requirements are met.

Definition Phase – The SLCM phase that results in a defined business justification for the system and a plan for implementation or acquisition. Upon completion of this phase, the project will have approval and funding to proceed.

Design – The step of the SLCM Acquisition/Development Phase that involves creating detailed designs for system components, products and interfaces and where initial test planning begins. The objective is to transform detailed, defined requirements into complete, detailed system specifications to guide the work of the Development step.

Developer Central – EPA Website (https://developer.epa.gov/) that provides resources for developers looking to interface with EPA’s Data and Application Programming Interfaces (APIs).

Development – The step of the SLCM Acquisition/Development Phase where production and assembly of all of the system components needed to complete the design and meet the mission needs takes place. The objective is to convert the work products of the Design step into a complete information system.

DevSecOps – The philosophy that security is continuously incorporated throughout development and operations.

Enterprise Architecture (EA) – A strategic information asset base which defines business mission needs, the information content necessary to operate the business, the information technologies necessary to support business operations and the transitional processes necessary for implementing new technologies in response to changing business mission needs.

Enterprise Shared IT Service (ESS) – A centrally provided IT service with defined service levels, costs, and methods of integration that is designed to be used or consumed by any part of the enterprise with a business requirement or need. EPA's centrally provided shared technical infrastructure services include email and collaboration tools, data center hosting, and network management. EPA shared applications services include access to payroll and other enterprise applications. EPA plans to expand its SS portfolio into software delivery services and shared data services in the future.

Federal Information Technology Acquisition Reform Act (FITARA) Review – Agency processes for reviewing and approving information technology acquisitions in accordance with FITARA, which states that agencies "may not enter into a contract or other agreement for information technology or information technology services, unless the contract or other agreement has been reviewed and approved by the Chief Information Officer."

Government Off-the-Shelf (GOTS) – A product developed by or for a government agency that can be used by another agency with the product's pre-established functionality and little or no customization.

Implementation Phase – The SLCM phase that involves moving a completed system (or system modifications) into the production environment and completing the necessary processes to allow users to access the system to perform the work identified in the mission.

Information and Communication Technology (ICT) – Information technology and other equipment, systems, technologies or processes for which the principal function is the creation, manipulation, storage, display, receipt or transmission of electronic data and information, as well as any associated content. Examples of ICT include but are not limited to: computers and peripheral equipment, information kiosks and transaction machines, telecommunications equipment, customer premises equipment, multifunction office machines, software, applications, websites, videos and electronic documents.

Information Technology Portfolio Review (ITPR) – The CIO's annual review of the Agency's IT portfolio

Major IT Investment – EPA uses OMB's definition of a Major IT Investment, which can be found in the CPIC Procedures document. For OMB budget reporting, EPA must report all Major IT Investments the Exhibit 53 and submit a Capital Asset Plan and Business Case (Exhibit 300).

Mobile App or Application – Any native or web application (app) specifically designed to be accessed and utilized on a handheld mobile device, such as a cell phone, smart phone, tablet or portable digital assistant (PDA).

Native Mobile Apps – Native apps can come preinstalled on a mobile device, such as a smart phone, but can also be downloaded from app stores and other websites. Native apps can be programmed to leverage many smart phone capabilities, such as the camera and geo-location.

Mobile Web Apps – Mobile web Apps reside on a server and are accessed using a mobile browser. Mobile web apps are distinct from mobile websites that only provide simple content. Mobile web apps use server-side or client-side processing (e.g., JavaScript) to provide a level of interactivity akin to many downloadable native apps.

Mobile Websites – A mobile website is a set of interconnected web pages designed specifically to be accessed by mobile web browsers.

Non-Major IT Investment – EPA uses the OMB's definition of a Non-Major investment, which can be found in CPIC Procedures. For OMB budget reporting, EPA must report all Non-Major IT Investments in Exhibit 53.

Open Source Software (OSS) – Software that can be accessed, used, modified and shared by anyone. OSS is often distributed under licenses that comply with the definition of "Open Source" provided by the Open Source Initiative4 and/or that meet the definition of "Free Software" provided by the Free Software Foundation.

Operations and Maintenance (O&M) Phase – The SLCM phase where users have a working system to support the mission need. More than half of a typical system's life cycle costs are attributable to O&M, making the management of this phase of equal importance to the other phases that deliver the functionality. During this time, the Project Manager maintains schedules and periodically conducts reviews to ensure the health of the system and to validate the suitability of the system for meeting SLCM requirements.

Pre-Definition Phase – The first phase in the life cycle where business owners determine if an IT System or Application is needed to fulfill a business need and/or performance gap.

Project Level Reviews – Reviews conducted at the project level to determine system readiness to proceed to the next phase of the IT life cycle. Key project stakeholders review and agree that the system under development is the system that needs to be built and that it is being built correctly. The System Manager and System Owner approve the completed review.

Quality Management – Ensures the quantity and quality of the data's intended use. Under the EPA Quality System, Agency organizations develop and implement supporting quality systems. Similar specifications may also apply to contractors, grantees, and other recipients of financial assistance from EPA.

Security Testing and Evaluation (ST&E) – An examination or analysis of the protective measures placed on fully integrated and operational information system. ST&E objectives are to uncover design, implementation and operational flaws that could allow the violation of security policy; determine the adequacy of security mechanisms, assurances and other properties to enforce the security policy; and assess the degree of consistency between the system documentation and its implementation. The scope of an ST&E Plan typically addresses computer security, communications security, emanations security, physical security, personnel security, administrative security and operations security.

Small Desktop Applications – End-user programs or applications that reside solely on a desktop or laptop which, while they may interconnect with other applications, do not control integrate, or manage components of a system.

Software as a Service (SaaS) – Software as a service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted rather than installed on individual computers.

Sprint Review – Agile development efforts are broken into sprints or short, time-boxed periods when a development team works to complete a set amount of work. Sprint reviews are conducted at the completion of a sprint to evaluate project priorities and confirm the intended product functionality was successfully designed, built, integrated, tested and documented; and it delivered value to the customer.

System (Information System) – NIST defines an information system as “A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information” (NIST SP 800-18 Rev. 1). Federal guidance gives agencies flexibility in constituting an information system and system managers must establish system boundaries to define the information resources allocated to the system. A single system may consist of several subsystems (a component of a system that performs specific functions). These subsystems fall under the governance of the overall system and should be included in the system documentation, but they do not require separate documentation. A system or subsystem may include information resources (e.g., applications, web pages, databases or spreadsheets). On their own these resources are not considered an information system, but once combined with other resources to perform a specific function or process they become a system or subsystem.

System Life Cycle Management (SLCM) –System Life Cycle Management is the Agency's approach and practices in the definition, acquisition, development, implementation, operations and maintenance, and termination of EPA IT systems and applications. System Owners and Project Managers must maintain required documentation for each phase, step and activity during the life cycle of an IT system or application. Each system must fit within the overarching Agency EA, and thus, the SLC includes control gates where management can review and approve alignment with EA principles, security and system requirements before the system may proceed to the next phase of its life cycle.

System Planning – The step of the SLCM Definition Phase where creation of the necessary management structure to properly manage and control the system occurs and the Project Manager and System Manager create many of the plans essential to the success of the project. Reviewing and updating the plans takes place throughout the remaining SDLC phases. The System Manager further develops the plan for how the business will operate after implementation of the approved system occurs and an assessment of how the implemented system will impact employee and customer privacy takes place.

Termination Phase – The phase of the SLCM process where system shutdown occurs. The purpose is to arrange for the retirement of a system and orderly disposition of system assets. During this end-of-life cycle phase, a system designated as excess or obsolete is retired and closed down. The emphasis of this phase is to ensure the orderly packaging and archiving of data, procedures and documentation to ensure the retention of all records and make it possible to reinstall the system and bring it back to operational status if necessary.

Waiver – Written justification for deviating from the SLCM process or for omitting sections or documents of the SLCM process. The consideration of waivers depends on the requirements of the system and the needs of the developing office. Waivers for major applications and general support systems and systems considered to be major investments in the CPIC process must receive concurrence from the System Owner and applicable IMO and approval from the Director of the Office of Environmental Information's Office of Technology Operations and Planning (OTOP). Waivers for any other applications and/or systems must receive concurrence from the System Owner and approval from the applicable IMO. Waivers should be documented in the Project Management Plan.

10. WAIVERS

Waivers to the requirements of this procedure may be considered based on the requirements of the system or application and the needs of the developing office. All waivers must be justified and documented (including all approvals and concurrences), by the information system Project Manager.

Any waiver requests must include signed concurrence by the System Owner and the SIO or IMO (if delegated). While the CIO will approve SLCM Policy Waivers, the CTO will approve waivers to the SLCM Procedure or applicable standards.

11. MATERIAL SUPERSEDED

System Life Cycle Management Procedure; CIO Transmittal 12-004; CIO Directive CIO 2121-P-03.0.

12. CONTACTS

For more information on this procedure, contact your Information Management Officer. You may also contact the Office of Mission Support, Environmental Information, Office of Digital Services & Technical Architecture.

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2021.02.26 15:20:31 -05'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information
and Chief Information Officer
U.S. Environmental Protection Agency