Description of document:	United States Customs Service Systems Development Life Cycle Handbook (SDLC) (CIS-HB 5500-07A), 2001
Requested date:	2017
Release date:	13-February-2020
Posted date:	09-March-2020
Source of document:	FOIA Request FOIA Officer US Customs and Border Protection 90 K Street, NW 9th Floor, Mail Stop 1181 Washington, DC 20229 FOIA Online

02/13/2020

CBP-2017-024343

This is a final response to your Freedom of Information Act (FOIA) request to U.S. Customs and Border Protection (CBP).

CBP is granting your request under the FOIA, Title 5 U.S.C. §552. After carefully reviewing the responsive documents, CBP has determined that they are approved for release in their entirety, no deletions or exemptions have been applied.

If you have a FOIAonline account, you MUST log into your account to retrieve your responsive records. After logging in, click on "View My FOIA Requests". Requests that have new, unread correspondence have a mail icon next to the tracking number.

This completes the CBP response to your request.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. 552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You may contact CBP's FOIA Public Liaison, Charlyse Hoskins, by sending an email via your FOIAonline account, mailing a letter to 90 K St, NE MS 1181, Washington DC, 20229 or by calling 202-325-0150. The FOIA Public Liaison is able to assist in advising on the requirements for submitting a request, assist with narrowing the scope of a request, assist in reducing delays by advising the requester on the type of records to request, suggesting agency offices that may have responsive records and receive questions or concerns about the agency's FOIA process. Please notate file number CBP-2017-024343 on any future correspondence to CBP related to this request.

Sincerely,

U.S. Customs and Border Protection

Systems Development Life Cycle Handbook

February 2, 2001

Department of the Treasury
United States Customs Service

Office of Information and Technology
Planning Group

Foreword

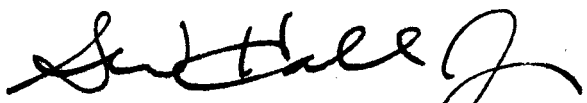
The Systems Development Life Cycle Handbook (SDLC) (CIS-HB 5500-07A) is official Customs policy, including approved development life cycles, processes, and documentation requirements. The SDLC describes a project's responsibilities for all aspects of systems development including Project Planning and Management, Risk Management, Quality Assurance, Requirements Management, IT Security, Contract Management, and Configuration Management.

This entire handbook is policy and applies to all Customs Information and Technology (IT) projects and systems regardless of sponsor, developer, project size, methodology, or technology used. It is mandatory that all IT projects, pilots, and prototypes comply with this handbook. This includes projects currently underway and systems already in operation. Because development projects vary in size and complexity, the SDLC contains guidelines on tailoring its requirements to fit the needs of the projects. Through approved tailoring, including Senior Management approval, even small projects that require less documentation can comply with this handbook.

This handbook supercedes the Systems Development Life Cycle Handbook (CIS HB 5500-07) dated October 1998. The templates, examples, and tutorial materials found in that previous version may be found in the OIT Process Asset Library (currently called the OIT Toolbox) on the Customs Intranet. The goal of this revision was to produce a Handbook that is easy to understand and use and that clearly addresses the systems development environment at Customs. A Process Action Team chartered by the OIT Software Engineering Process Group (SEPG) worked for six months to extract and craft policy statements for the Handbook. The SEPG and the Systems Life Cycle Team reviewed these policies, as well as the portions of the Handbook that contain information on life cycles, development activities, and standards. Comments received from public reviews on the Intranet were also incorporated.

The SDLC Handbook should be considered the first step of process improvement work that will continue in the years ahead. As Customs development practices improve and mature, policies and standards will be revised. Suggestions are welcome and will provide the basis for future revisions.

Comments or questions about this handbook may be addressed to the Systems Life Cycle Team by email to SDLCMAIL. Changes may be requested by using the SDLC Change Request process in Appendix D of this handbook.



Assistant Commissioner
Office of Information and Technology

February 2, 2001
Distribution: G-25

Record of Changes

Change Number	Date	Number of Figure, Table or Section	Type of Change[1]	Title or Brief Description	Change Request Number
1	2/2001	All		Original Issue	N/A

[1] A = Addition; M = Modification; or Change, D = Deletion

Table of Contents

Chapter 4: Customs Standard Life Cycle

Chapter 5: Waterfall-Based Development Models

Chapter 6: Alternative Development Models

Appendices

A Glossary

B Roles and Responsibilities

C Standard Life Cycle Requirements Summary

D SDLC Change Procedure

E Governing Directives

Index

Executive Summary

Who Does the SDLC Apply To?

This Systems Development Life Cycle (SDLC) Handbook contains the policies, life cycles, and standards that govern Information and Technology systems (including infrastructure) built by or for the U.S. Customs Service.

This entire handbook is policy and applies to all Customs Information and Technology (IT) projects and systems regardless of sponsor, developer, project size, methodology, or technology used. This version of the SDLC has been integrated with the Investment Management Process (IMP) to simplify the project's view of the process from concept to retirement.

The level of detail and format of deliverables for different size or types of projects will vary. However, all projects must have disciplined engineering techniques, such as defined requirements, adequate documentation, quality assurance, and approvals. The tailoring and approval process described in this handbook provides the method for any size project to meet SDLC requirements.

This handbook applies not only to new projects, but also to projects already underway, and to systems in operation. The tailoring and approval process described in this handbook provides the mechanism for underway projects and systems in operation and their Senior Management to account for and document SDLC compliance, along with rationale for the level of effort to be expended.

What is Included in the SDLC?

This handbook was developed under the sponsorship of the SEPG (Software Engineering Process Group) with participants from the development and support disciplines.

This version evolved in response to comments received about the usability and format of the October 1998 SDLC. The new SDLC revision process represents the view of the Enterprise Process Improvement Program: that improvement ideas flow upward as well as downward and that practitioners have keen insight into appropriate solutions.

The previous version of the SDLC Handbook (CIS HB 5500-07, October 1998), which is superceded, contained policy, life cycles, detailed procedures, templates, and examples. This version contains only policies, high-level processes, and life cycles. The remaining detailed information from the October 1998 version along with any newly created or improved procedures are contained in the Customs Process Asset Library (PAL).

How Will the SDLC be Used for Project Management?

The Customs Life Cycle Policies in Chapter 2 are management's expectations, at a high level, of what a project must do. These policies are further expanded/clarified later in this handbook for implementation with details of tasks, deliverables, reviews, and responsibilities for development. This handbook also incorporates best practices from the Software Engineering Institute's (SEI's) Capability Maturity Model® (CMM®).

After considering the Customs Life Cycle Policies defined in Chapter 2, projects will select an appropriate life cycle from either Chapter 5 or 6 based on the needs of the project. Projects will develop a Project Plan using the life cycle combined with the stages, tasks, and activities of the Customs Standard Life Cycle in Chapter 4.

Based on project size, complexity, visibility, and risk, the activities and deliverables listed in the SDLC may be combined or expanded. However, each must be specifically accounted for and maintained along with tailoring rationale as part of the tailoring documentation. The Customs Process Asset Library (PAL) contains templates, examples, and procedures that projects will consult in order to take advantage of existing good practices. When approved by Senior Management (including a written account of tailoring actions) and a Project Work Authorization is issued, the tailored Project Plan will become the project's SDLC-compliant road map. Figure ES-1 summarizes this process.

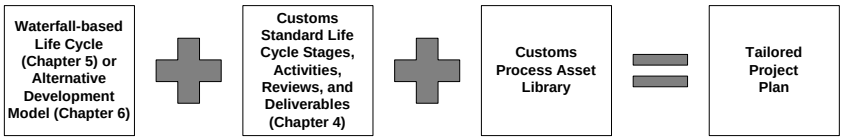


Figure ES-1, How to Develop a Project Plan

The Systems Life Cycle (SLC) Organization will assist projects in understanding the SDLC in order to create their tailored Project Plan. These SDLC Assist Visits may also include representatives from the Investment Organization and Evaluation Organization.

In addition, the definitions in the Glossary (Appendix A) have been specifically tailored and clarified for Customs unique requirements. These definitions are useful to clarify the intent of many portions of the Customs SDLC.

How Will the SDLC be Used for Process Improvement?

In addition to its role as the standard for project management, this SDLC supports the broader goal of Enterprise Process Improvement.

Process Groups (such as the Software Engineering Process Group [SEPG], the Software Acquisition Process Group [SAPG], and Infrastructure Services Process Group [ISPG]) and Process Action Teams will assist projects and individuals in creating project plans and identifying, developing, and documenting detailed processes, procedures, and examples to supplement this Handbook.

Suggestions for improved high level policies and life cycles will be reflected in this Handbook through periodic updates. Suggestions for improved detail-level processes and procedures will be implemented continuously in the Process Asset Library through the work of the Process Groups.

Chapter 1
SDLC Concepts

1.1 What is the Systems Development Life Cycle (SDLC) Handbook?

This handbook contains the policies, life cycles, and standards that govern Information and Technology systems (including infrastructure) built by or for the United States Customs Service. As such, it incorporates:

- Life Cycle Policies
- Approved Life Cycles
- Standard Life Cycle requirements
- Development activities
- Standards published by the Department of the Treasury and others as applicable (see Appendix E)
- Best practices and disciplined engineering methods from the Software Engineering Institute's (SEI) Capability Maturity Model® (CMM)[2] (throughout the document).

1.2 Who Does This Apply To?

This entire handbook is policy and applies to all Customs Information and Technology (IT) projects and systems regardless of sponsor, developer, project size, methodology, or technology used.

Everyone involved in developing, maintaining, or implementing systems or applications for the United States Customs Service shall be familiar with and follow the guidance in this handbook.

The policies and life cycle process in this handbook apply to large and small projects, including systems using commercial off-the-shelf solutions. The level of detail and format of deliverables for different size or types of projects will differ. However, all projects must have disciplined engineering techniques, such as defined requirements, adequate documentation, quality assurance, and approvals. The tailoring and approval process set forth in this Handbook provides a mechanism for any size project to meet SDLC requirements.

[2] Mark Paulk, et.al. *The Capability Maturity Model: Guidelines for Improving the Software Process*. New York: Addison-Wesley Publishing Company, 1995. ISBN: 0-201-54664-7.

1.3 How Does This Apply to Projects Already Underway and Systems in Operation?

This handbook applies not only to new projects, but also to projects already underway, and to systems in operation.

Senior Management shall weigh the costs and benefits, then determine and document the appropriate level of effort to be expended for each underway project and system in operation to bring them into compliance with this Handbook.

Managers of all underway projects and systems in operation shall determine in which stage of the Customs Standard Life Cycle they fall. Underway projects and systems in operation shall commence SDLC activities, reviews, and deliverables from that point forward. Deliverables and reviews from Life Cycle stages prior to that point, that are necessary precursors to future activities, shall be completed. Other deliverables must be completed to the maximum extent practicable.

The tailoring and approval process, described in this handbook in Chapter 4, Stage 2, provides the mechanism for underway projects, systems in operation, and their Senior Management to account for and document SDLC compliance, along with rationale for the level of effort to be expended.

1.4 How is This Handbook Organized?

This handbook was developed under the sponsorship of the SEPG (Software Engineering Process Group) with participants from the development and support disciplines.

This version evolved in response to comments received about the usability and format of the October 1998 SDLC. The new SDLC revision process represents the view of the Enterprise Process Improvement Program: that improvement ideas flow upward as well as downward and that practitioners have keen insight into appropriate solutions.

Each chapter presents a focused type of information:

- Chapter 1 describes to whom this handbook applies and how it supports process improvement.

- Chapter 2 contains the statements of policy that govern all IT systems built by or for the United States Customs Service. These are arranged by topic, with each policy statement having a unique item number.

- Chapter 3 defines a life cycle and contains information on the basic principles that govern the Customs development processes.

- Chapter 4 describes the stages, inputs/outputs, tasks/activities, roles, and reviews that constitute the Customs Standard Life Cycle.

- Chapters 5 and 6 contain all the development life cycles that are approved for use in the United States Customs Service.

- Appendix A defines the acronyms and terms used in this handbook. These Customs-specific definitions are useful to clarify the intent of many portions of the Customs SDLC.

- Appendix B lists roles and responsibilities for the activities identified in Chapter 4.

- Appendix C summarizes the standard life cycle requirements of the preceding chapters, but does not replace that more detailed guidance. Appendix C should not be used independently of Chapters 2 and 4.

- Appendix D provides the procedure for submitting changes to this handbook.

- Appendix E lists the standards and directives incorporated within this SDLC.

1.5 How Does This Handbook Differ From the Previous Version?

The previous version of the SDLC Handbook (CIS HB 5500-07, October 1998), which is hereby superceded, contained policy, life cycles, detailed procedures, templates, and examples. This version contains only policies, high-level processes, and life cycles. The remaining detailed information from the October 1998 version along with any newly created or improved procedures are contained in the Customs Process Asset Library (PAL).

In addition to its role as the standard for project management, this SDLC supports the broader goal of Enterprise Process Improvement.

Process Groups (such as the Software Engineering Process Group [SEPG], Software Acquisition Process Group [SAPG], and Infrastructure Services Process Group [ISPG]) and Process Action Teams will work as necessary to help projects and individuals to create project plans and to identify, develop, and document detailed processes, procedures, and examples to supplement this Handbook.

Suggestions for improved high level policies and life cycles will be reflected in this Handbook through periodic updates. Suggestions for improved detail-level processes and procedures will be implemented continuously in the Process Asset Library through the work of the Process Groups.

Figure 1.1, SDLC and Process Asset Library Structure, shows the relationship between the SDLC Handbook and the Process Asset Library and how suggestions will be incorporated into each.

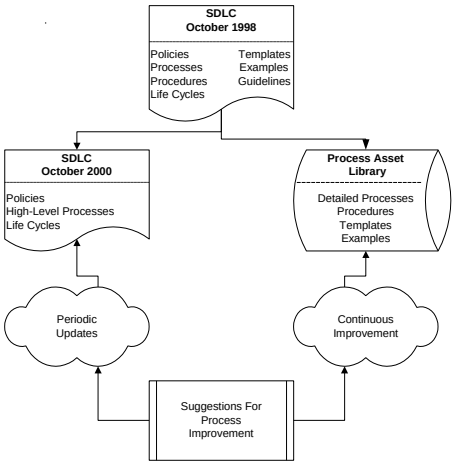


Figure 1.1, SDLC and Process Asset Library Structure

1.6 How Does This Handbook Support Improved Processes?

This handbook supports process improvement by defining Customs approved methods for disciplined development. These disciplined methods provide the structure for all Customs programs to conduct and measure process improvement activities. It allows for the hierarchy of process improvement documentation:

- Policies
- Processes
- Procedures
- Tasks/Activities
- Role Definitions

There are at least two major types of process improvement practitioners:

- Projects: Projects involved in system development will use this handbook by following the policies and life cycle stages. This guidance provides a standard life cycle process, activities, and rules with which to create tailored project plans.

- Process Improvement Organizations: This includes all organizations such as Process Groups, Process Action Teams, Projects, etc. which are engaged in documenting or improving their processes, procedures, or operations.

1.6.1 How Should Projects Use This Handbook?

- All projects will be governed by the Customs Life Cycle Policies in Chapter 2, which follow good engineering practices.

- Projects will choose one of the approved Life Cycles in Chapters 5 and 6.

- Projects will then utilize the Customs Standard Life Cycle in Chapter 4 to create their tailored Project Plan. The Systems Life Cycle (SLC) Organization, Investment Organization, and Evaluation Organization will actively assist projects in understanding the SDLC in order to create their tailored Project Plan.

- The Chapter 4 Standard Life Cycle incorporates all the activities, reviews, and deliverables for projects. While organized in a waterfall fashion for clarity, not all projects will be executed using the Waterfall Life Cycle. Appendix C also includes a summary of deliverables and activities to assist projects in defining work.

- Projects shall use the resources of the Process Asset Library (PAL) for details on processes, procedures, templates and examples.

1.6.2 How Should Process Improvement Organizations Use This Handbook?

Process Improvement Organizations (e.g., Process Groups and Projects that are conducting improvement work) will use the policies, life cycles, tasks/activities, and roles defined in this handbook as a roadmap to guide their improvement work. They will create, document, or improve processes, procedures, tasks/activities and roles, which support the high-level development concepts in this Handbook.

1.7 How Do I Submit Changes to This Handbook?

Suggested changes to the handbook shall be submitted using the change request shown in Appendix D.

Chapter 2
Customs Life Cycle Policies

2.1 Introduction

This entire handbook is policy and applies to all Customs Information and Technology (IT) projects regardless of sponsor, developer, project size, methodology or technology used. Everyone involved in developing, maintaining, or implementing systems for the United States Customs Service shall be familiar with and follow the guidance in this handbook.

The Customs Life Cycle Policies in this chapter are management's high-level expectations of what a project must do. These policies are further expanded/clarified elsewhere in this Handbook for implementation with details of tasks, deliverables, reviews, and responsibilities for development. This handbook also incorporates best practices from the Software Engineering Institute's (SEI's) Capability Maturity Model® (CMM).

The policies and life cycle process in this handbook apply to all projects. The level of detail and format of deliverables for different size or types of projects may vary. However there are certain specified minimums that all projects must have. (See Section 3.5.3 for details.)

The tailoring and approval process allows for variance among projects without excusing compliance with the required minimums. Section 2.3.3 contains the tailoring and approval policy. Chapter 4, Stage 2 – Initiation and Authorization, presents additional definition for the Project Tailoring Review tasks and activities.

The Customs Life Cycle Policies in this chapter are arranged by functional topics that were derived from a combination of CMM® concepts and Customs unique needs.. Each topic begins with a brief description and goals of the topic. The description is followed by tables containing an identifying number in the left column, the statement of the policy item in the middle column, and references/notes in the right column.

2.2 Requirements Management

Description: Requirements are the user and information and technology (IT) needs that determine the capabilities and the design of an IT system. Requirements Management is the process of capturing, tracing, and maintaining these requirements. The user and functional requirements are typically gathered in a requirements traceability matrix (RTM) to ensure that each requirement can be mapped through design, development, testing, and operations. Requirements are reflected in software, hardware, services, and documentation for both applications and infrastructure.

The overall goals of Requirements Management are to:

- Establish a common understanding of user and IT needs;
- Ensure that project plans, activities, and products are kept consistent with defined needs;
- Ensure that project plans, activities, and products are kept focused on defined needs; and
- Establish and control approved and certified requirements in order to facilitate engineering and management activities.

This section includes policies relating to:

- 2.2.1 The identification and definition of requirements including reviews and certification
- 2.2.2 Considerations for requirements documentation and traceability
- 2.2.3 Management of requirements changes and impact analysis
- 2.2.4 Ensuring that requirements management training is provided

Policies:

2.2.1 Requirements Identification and Definition		
Number	**Text**	**References**
2.2.1.1	All requirements must be clearly defined and uniquely identified.	
2.2.1.2	All requirements must be aligned with the goals, objectives, and strategies of the corresponding mission area as documented in the Customs Strategic Plan.	See the *Enterprise Architecture Blueprint*, Chapter 2, for information on the Business Alignment 2X2 Matrix.
2.2.1.3	All requirements must be thoroughly reviewed to ensure that everyone involved in the development, analysis, and implementation processes understands them.	
2.2.1.4	All requirements must be testable or verifiable.	
2.2.1.5	The Business Sponsor and the Project Manager shall document their mutual understanding of the business needs, requirements, and acceptance criteria for the system and shall certify their acceptance and approval.	

2.2.1 Requirements Identification and Definition		
Number	**Text**	**References**
2.2.1.6	Requirements Management processes must be reviewed in accordance with Project Monitoring and Quality Assurance policies.	See: • Section 2.4.1.1, Project Manager Reviews • Section 2.4.1.2, Senior Management Reviews • Section 2.5.1.1, Internal project QA Reviews.
2.2.1.7	All requirements must be incorporated in the design, testing, training, and implementation of the system.	

2.2.2 Documenting Requirements		
Number	**Text**	**References**
2.2.2.1	The requirements documentation shall include the following: • User Requirements • Functional Requirements (including System and Support Requirements)	"System and Support" Requirements include security, training, operational, performance, quality, automation readiness, and data requirements. Also see Sections 2.7.1.4 and 2.7.2, Security Policies.
2.2.2.2	All functional requirements must be traceable to one or more user requirements.	User Requirements in this context include the system and support needs of the user/system.

2.2.3 Requirements Change Control		
Number	**Text**	**References**
2.2.3.1	All projects must establish and follow a formal process to control project scope, assess impacts of changes, and incorporate approved changes in a controlled manner.	
2.2.3.2	All changes to certified requirements must be renegotiated, documented, and re-certified.	See Chapter 4, Stage 3 – Project Definition for certification activity.
2.2.3.3	Once requirements have been approved and certified, all requirements changes will fall under the Configuration Management (CM) change control policies.	See Section 2.6, Configuration Management.

2.2.3 Requirements Change Control		
Number	**Text**	**References**
2.2.3.4	Changes in requirements must be fully coordinated in accordance with Project Planning and Project Monitoring policies.	See: • Section 2.3.7.1, Negotiate Commitments • Section 2.3.7.2, Document Commitments • Section 2.3.7.3, Review/ Communicate Commitments • Section 2.4.2.2, Track Revisions • Section 2.4.2.3, Track Issues • Section 2.4.2.4, Corrective Actions.

2.2.4 Requirements Management Training		
Number	**Text**	**References**
2.2.4.1	Members of all affected organizations who are responsible for requirements management shall be trained in the objectives, procedures, and methods for performing their Requirements Management activities.	

2.3 Project Planning

Description: Project Planning involves developing estimates and descriptions for work to be performed, establishing necessary commitments, and defining the plan and schedule to do the work. It ensures that resources, capabilities, and constraints are accounted for and traceable; and that a documented plan is produced, agreed to, and used for tracking the project.

The goals of Project Planning are to:

- Develop and use plans for performing and managing all tasks associated with the project (for both management and engineering tasks);
- Document estimates (and their assumptions) for planning and tracking;
- Document project activities and commitments; and
- Obtain agreement from affected groups and individuals to their commitments.

This section includes policies concerning:

- 2.3.1 Investment Management Process (IMP) considerations
- 2.3.2 Obtaining waivers to policy if required.
- 2.3.3 Tailoring life cycles, processes, and documents
- 2.3.4 Planning the project concept, definition, life cycle and methodology to be used
- 2.3.5 Estimates required
- 2.3.6 Defining the required tasks, activities, and schedules
- 2.3.7 Commitments and negotiation between the project, its members, its customers, and external organizations
- 2.3.8 Replanning issues and plan approvals/reapprovals
- 2.3.9 Planning documentation and responsibilities
- 2.3.10 Establishing and maintaining process assets

Policies:

2.3.1 Investment Management Process Considerations		
Number	**Text**	**References**
2.3.1.1	All projects will follow the Investment Management Process.	See the *Investment Management Process System Description.*

2.3.1 Investment Management Process Considerations		
Number	**Text**	**References**
2.3.1.2	The Office of Information and Technology (OIT) shall support and maintain only those systems approved by the Investment Management Process.	See the *Investment Management Process System Description.*
2.3.1.3	Each project shall have a single Project Manager officially designated by Senior Management.	
2.3.1.4	The Project Manager and Business Sponsor are responsible for grouping project requirements into manageable, defined chunks of functionality for project funding and deployment.	See the *Investment Management Process System Description.*
2.3.1.5	The Business Sponsor, in conjunction with the Project Manager and OIT Senior Management, is responsible for approval of the Project Plan.	
2.3.1.6	Adequate resources and funding shall be provided for all project activities.	

2.3.2 Policy Waivers		
Number	**Text**	**References**
2.3.2.1	If waivers from any OIT policies are required, the project must gain approval from the Chief Information Officer (CIO) or the CIO's formal designee.	
2.3.2.2	If waivers of any policies from organizations outside of OIT are required, the project must • Gain approval from the CIO, and then • Follow the waiver procedures as defined by the organization outside of OIT.	

2.3.3 Tailoring		
Number	**Text**	**References**
2.3.3.1	Tailoring of approved life cycles and deliverables to meet project needs is allowed. The Project Manager must document the reasons for the tailoring. The tailoring must be approved by Senior Management.	**Note:** The Security Plan shall NOT be tailored. See Chapter 4, Stage 2 -- Initiation and Authorization.
2.3.3.2	Projects may develop documents and plans as needed in addition to those defined and required in the SDLC.	See Chapter 4, Customs Standard Life Cycle.

2.3.4 Project Planning Fundamentals		
Number	**Text**	**References**
2.3.4.1	Planning shall be based on identified requirements.	

2.3.4 Project Planning Fundamentals		
Number	**Text**	**References**
2.3.4.2	All projects must use one of the approved Customs life cycles.	See related guidance: • Section 2.3.2, Policy Waivers • Section 2.3.3, Tailoring • Chapter 5, Waterfall-Based Development Models • Chapter 6, Alternative Development Models.
2.3.4.3	Plans shall be created and reviewed as early in the life cycle as possible; they shall be modified as more detail is developed during the course of the project.	
2.3.4.4	All projects must be consistent with Customs information and technology architecture and software standards.	See Appendix E, Governing Directives, OIT Standards. For exceptions, see Section 2.3.2.1.
2.3.4.5	Projects shall plan to utilize the Customs technology infrastructure in lieu of building a project-specific solution.	See *Customs Enterprise Architecture Technical Reference Model*.
2.3.4.6	Business Sponsors and users requesting IT services are responsible for the initiation of projects under their business areas and for actively participating throughout the entire project life cycle.	
2.3.4.7	Senior Management shall provide sufficient, trained staff to perform required project planning, estimation, and project management activities.	
2.3.4.8	During planning, the Project Manager shall identify each task and activity to ensure that appropriate staff are identified.	See Chapter 4, Customs Standard Life Cycle.
2.3.4.9	The project planning results shall be reviewed and approved as specified in the IMP.	See the *Investment Management Process System Description*.
2.3.4.10	The Business Sponsor and Senior Management must approve the work product's readiness before it is turned over to Production.	See Chapter 4, • Stage 6 – Acceptance • Stage 7 – Operational Readiness.
2.3.4.11	Training for end-users shall be planned and provided in a timely fashion.	See Chapter 4, Customs Standard Life Cycle.

2.3.5 Estimating		
Number	**Text**	**References**
2.3.5.1	The Project Manager shall use historical information from similar projects [when available] to do initial planning.	
2.3.5.2	The Project Manager will document the procedure used to develop estimates and schedules. Estimates shall include work product sizes, effort and cost.	

2.3.5 Estimating		
Number	**Text**	**References**
2.3.5.3	The Project Manager shall involve project team members, to the maximum extent possible, in creating, identifying, and documenting estimates, schedules, and risks.	

2.3.6 Defining Tasks/Activities/Schedules		
Number	**Text**	**References**
2.3.6.1	All activities shall be performed according to a documented process or procedure.	Also see Appendix E, Governing Directives, OIT Standards.
2.3.6.2	All project activities, including stakeholder and support organization activities, shall be defined and included in the Project Plan.	
2.3.6.4	The Project Manager shall develop a Work Breakdown Structure (WBS).	See Chapter 4, Customs Standard Life Cycle.
2.3.6.5	The Project Manager shall break the job down into tasks in order to allow effective progress monitoring and replanning.	
2.3.6.6	The Project Manager shall break near-term tasks into WBS increments that are defined in small enough units to track progress within each month.	

2.3.7 Negotiating and Approving Commitments		
Number	**Text**	**References**
2.3.7.1	The Project Manager must identify and negotiate commitments with representatives of all internal and external project stakeholders.	**Note:** Examples of internal and external project stakeholders include: system engineering, hardware engineering, system test, database engineering, security, training, other projects, users, and all project team members.
2.3.7.2	All project commitments must be documented.	
2.3.7.3	Project Managers shall plan for appropriate reviews with all internal and external project stakeholders.	
2.3.7.4	There must be a documented procedure for negotiating and changing commitments.	
2.3.7.5	A project Kickoff Meeting shall be held with all potential internal and external stakeholders to review specifications, requirements, and impacts.	
2.3.7.6	Senior Management shall review project commitments.	

2.3.8 Replanning

Number	Text	References
2.3.8.1	The Project Plan shall be revised, reviewed, and re-approved as changes are required and corrective actions taken.	
2.3.8.2	Rebaselining requires Senior Management approval.	
2.3.8.3	If a project's cost, schedule, or mission-related performance varies from approved plans by 10% or more, the project shall redo the formal Project Initiation Review and be re-authorized.	See Chapter 4, Stage 2 – Initiation and Authorization. Reference: Federal Acquisition Streamlining Act of 1994 (Title V).
2.3.8.4	The Project Manager has the authority to negotiate changes and revise the Project Plan accordingly for changes within the scope of the project.	Also see Policy line 2.3.1.5.

2.3.9 Planning Documentation and Responsibilities		
Number	**Text**	**References**
2.3.9.1	The Project Manager shall explicitly assign and document responsibility for specific activities and work products.	
2.3.9.2	The following project roles at minimum must be assigned by name in writing: • Project Manager (PM) • Project Quality Assurance • Project Configuration Management • Project Change Control Board • Planning • Risk Management	
2.3.9.3	If the Business Sponsor determines that major changes will occur to existing work processes or workforce as a result of the project, the Business Sponsor shall develop a plan in coordination with labor and employee relations organizations to mitigate workforce issues.	For additional information, contact the OIT Resource Management Group (RMG).
2.3.9.4	The Business Sponsor is responsible for determining the duration of parallel operations, if any, between the old and new systems.	
2.3.9.5	Projects shall comply with privacy policies throughout the life of the system.	See Appendix E, Governing Directives.
2.3.9.6	During project initiation and system retirement, notifications must be placed in the Federal Register for all systems covered by the Privacy Act of 1974 as amended.	For additional information and guidelines, contact the Office of the Chief Counsel.
2.3.9.7	Prior to implementation, all affected organizations and sites shall be notified with sufficient time to manage potential impact.	

2.3.10 Process Assets		
Number	**Text**	**References**
2.3.10.1	An OIT-wide Process Asset Library (PAL) of recommended processes, procedures, examples, and templates shall be established and used as a reference.	
2.3.10.2	Customs Process Groups (e.g., the SEPG) shall be responsible for the assets in the PAL.	

2.4 Project Monitoring

Description: Project monitoring ensures that all projects track and control their progress in an objective, proactive manner. It also ensures that the project's results, changes, and commitments are communicated to all interested groups, including senior management.

The goals of Project Monitoring are to:

- Track project results and performance against the project plans;
- Take and monitor corrective actions when project results deviate significantly from the project's plans; and
- Ensure that changes to commitments are agreed to by the affected groups or individuals and communicated to all interested parties.

This section includes policies relating to:

- 2.4.1 The required occurrence and documentation of status and oversight meetings
- 2.4.2 The tracking of the project's planned size, cost, schedule, and quality elements against actual results
- 2.4.3 Proactively anticipating and managing potential risks to project success
- 2.4.4 Analyzing objective results data collected to determine variances from estimates and corrective actions needed
- 2.4.5 Ensuring that project documentation is updated and accessible in a project repository
- 2.4.6 Ensuring project management training is provided

Policies:

2.4.1 All Meetings/Oversight		
Number	**Text**	**References**
2.4.1.1	Project Managers shall hold Project Status meetings to review project and process activities with project team members and other affected stakeholders on a regularly scheduled and event-driven basis.	
2.4.1.2	Senior Management shall review project and process activities on a regularly scheduled basis.	
2.4.1.3	All meetings shall be documented.	
2.4.1.4	Process Groups (e.g., the SEPG) shall review project activities and processes for the purpose of process improvement.	
2.4.1.5	Formal reviews shall be conducted by the Project Manager with representatives of stakeholders external to the project to address the accomplishments and results of the project at selected milestones, according to a documented procedure.	

2.4.2 Tracking		
Number	**Text**	**References**

2.4.2 Tracking		
Number	**Text**	**References**
2.4.2.1	The Work Breakdown Structure, project cost estimate, and Schedule shall be used for tracking project activities and communicating status.	
2.4.2.2	All project changes, issues, and problems must be identified, documented, and monitored.	
2.4.2.3	The Project Manager is responsible for taking corrective actions and making changes within the project to ensure that commitments are met.	
2.4.2.4	All contributing groups shall provide regular status reports to the Project Manager.	

2.4.3 Risk Management		
Number	**Text**	**References**
2.4.3.1	Each project shall identify, assess, prioritize, document, mitigate, communicate, and monitor both project and security risks on a regular basis.	
2.4.3.2	The Project Manager is responsible for risk assessment and risk mitigation. Everyone associated with the project is responsible for identifying and reporting to the Project Manager potential risks to allow for assessment and mitigation.	

2.4.4 Metrics		
Number	**Text**	**References**
2.4.4.1	Metrics on all project activities shall be gathered and reported to Senior Management. This includes Project Management Support activities as well as development activities.	See Chapter 4, Customs Standard Life Cycle.
2.4.4.2	Metrics shall be used to provide objective information on project schedule, resources, costs, requirements and work product sizes and changes, and product quality. Metrics shall NOT be used for motivation, punishment, nor for evaluation of individual or workgroup performance.	

2.4.5 Project Repository		
Number	**Text**	**References**
2.4.5.1	Projects must establish and maintain a repository for all project-related information in a centralized, known and accessible location. In the event that information from supporting and stakeholder organizations is maintained outside	

2.4.5 Project Repository		
Number	**Text**	**References**
	the project purview, the project may reference the required information rather than duplicate the information.	
2.4.5.2	The project repository shall contain or reference the most current project/release information using version control.	
2.4.5.3	All work products must be maintained or referenced in the project repository using version control. The tracking method for referenced products will need to be negotiated with the product owner. The project shall document the referenced product tracking method.	See Chapter 4, Customs Standard Life Cycle.
2.4.5.4	Information reported for all meetings (agendas, minutes, action item lists, etc.) must be maintained in the project repository.	
2.4.5.5	Project lessons learned meetings shall be planned and scheduled. Lessons Learned shall be documented, updated, and reported for use in future projects and releases.	
2.4.5.6	Before a system or an enhancement to a system can be moved into production, all system documentation must be completed/amended, verified, and approved. Final user documentation and training materials may be completed after implementation.	See Chapter 4, Customs Standard Life Cycle.

2.4.6 Project Management Training		
Number	**Text**	**References**
2.4.6.1	The members of all affected organizations who are responsible for project management activities shall be trained in the objectives, procedures, and methods for performing their project planning, estimating, tracking, and monitoring activities.	
2.4.6.2	Project Managers shall be trained in managing the technical and personnel aspects of the project.	
2.4.6.3	Project Team members shall be provided an orientation in the technical aspects of the project.	

2.5 Quality Assurance

Description: Quality Assurance (QA) is a planned and systematic approach to assessing, monitoring, and improving the quality of a project's work products. It includes a methodical process to independently review and audit work products and the procedures and processes used to produce them. It verifies that work products, procedures, and processes comply with

applicable documented standards, as well as provides project staff and senior managers with the results of these reviews and audits.

> **Note:** This section establishes the grounding for the mechanisms and procedures needed to ensure that Customs can produce quality products in a repeatable manner. Everyone on the project is responsible for the quality of project results. The specified QA Team's function is to review, advise, and verify plans, processes, activities, and products to help the project meet quality concerns.

The goals of Quality Assurance are to:

- Establish and implement quality assurance plans and procedures for both the project's work products and its processes at the project level;
- Objectively review work products and audit the project's processes/activities to ensure that they meet all applicable standards and requirements;
- Provide management with visibility into the development processes being used by the projects; and
- Ensure that the new system/changed system works with existing systems.

This section includes policies concerning:

- 2.5.1 Project QA responsibilities and activities within the Project Team
- 2.5.2 Organizational QA responsibilities and activities
- 2.5.3 Product testing activities by the developers within a project
- 2.5.4 Independent testing and validation of products
- 2.5.5 Ensuring that QA-related training and orientations are provided

Policies:

2.5.1 Project QA		
Number	**Text**	**References**
2.5.1.1	All projects shall plan, perform, document, track, and measure project quality assurance activities during the entire life cycle of the project. All QA activities shall be performed based on a documented and approved Project QA Plan.	
2.5.1.2	A Project QA Team within the project shall be identified and shall be responsible for coordinating, implementing and verifying project QA activities. They shall periodically report the results of their activities to the Project Team.	**Note:** A team may consist of one individual part-time up to multiple people full-time, as appropriate for the size and complexity of the project.
2.5.1.3	The results of quality assurance activities shall not be used to evaluate the performance of individuals.	

2.5.1 Project QA		
Number	**Text**	**References**
2.5.1.4	Peer reviews shall be planned and used to review work products as early in the development life cycle as possible.	
2.5.1.5	Formal reviews and signoffs shall be performed. At minimum, these shall occur: to certify requirements, to verify system design, before transition to acceptance testing, and before moving the system to production.	See mandatory minimum activities listed in Chapter 4, Customs Standard Life Cycle.
2.5.1.6	The Project QA Team shall identify and document processes and procedures in their QA Plan to account for deviations in project activities and work products.	

2.5.2 Organizational QA		
Number	**Text**	**References**
2.5.2.1	An OIT QA Organization with an independent reporting chain to senior management shall exist.	
2.5.2.2	The OIT QA Organization shall provide guidance to Project QA Teams for planning Project QA activities.	
2.5.2.3	The OIT QA Organization shall periodically monitor Project QA activities and documents. Deviations and compliance issues identified in project products or processes shall be documented and reported first to the Project Team and escalated if necessary to succeeding levels of Senior Management.	Also see Section 2.3.2, Policy Waivers.
2.5.2.4	Experts independent of the OIT QA Organization shall periodically review the activities and work products of the OIT QA Organization.	

2.5.3 Product Testing		
Number	**Text**	**References**
2.5.3.1	Testing shall be conducted to ensure that the delivered product meets the certified requirements and does not adversely affect existing software and systems.	
2.5.3.2	All development teams shall conduct and document unit and integration testing. Developers must include test cases and test results for all security features and requirements.	See Section 2.7.2.2 for restriction on test data.
2.5.3.3	The Project QA Team shall monitor unit, integration, and system level testing.	

2.5.4 Independent Testing		
Number	**Text**	**References**
2.5.4.1	Systems Acceptance Testing (SAT), Security Testing, and User Acceptance Testing must be performed independent of the development process. All independent testers shall document their test results.	
2.5.4.2	Documentation shall be provided to the independent testers that is clear, concise, and complete.	See Appendix E, Governing Directives, OIT Standards.
2.5.4.3	Testing shall be performed in accordance with documented Test Plans.	Also see Section 2.5.3.2.
2.5.4.4	The Business Sponsor must verify that the user documentation and training materials are acceptable and accurate.	

2.5.5 QA Training		
Number	**Text**	**References**
2.5.5.1	Members of the OIT QA Organization and Project QA Team shall be trained in the objectives, procedures, and methods for performing their Quality Assurance activities.	
2.5.5.2	Members of the Project Team shall receive orientation on the role, responsibilities, authority, and value of Project Quality Assurance and the OIT QA Organization activities.	
2.5.5.3	The members of all affected organizations who are responsible for testing shall be trained in the objectives, procedures and methods for performing their testing activities.	

2.6 Configuration Management

Description: Configuration Management (CM) establishes and maintains configuration item (CI) integrity across the project. Configuration items are the hardware, software and documentation components related to a project. Work product integrity is achieved through the identification of the configuration items and the systematic control of changes to them. From the baseline, changes to CIs are managed via the change control and audit procedures.

The goals of Configuration Management are to ensure that:

- CM activities are planned;
- Selected work products are identified, tracked, controlled, and available from the CM repository;
- Changes to identified work products are controlled and documented; and
- Affected groups and individuals are informed of the status and content of the project's baselines.

This section includes policies on

- 2.6.1 General CM precepts
- 2.6.2 Migration to and from the SAT, Education, and Production environments
- 2.6.3 Baseline change control concerns
- 2.6.4 Configuration audits and status accounting reports
- 2.6.5 CM training and orientation
- 2.6.6 CM libraries and repositories for the project

Policies:

2.6.1 General CM Precepts		
Number	**Text**	**References**

2.6.1 General CM Precepts		
Number	**Text**	**References**
2.6.1.1	Configuration Management shall be planned and used throughout the entire life cycle. Project CM activities shall be performed based on a documented and approved Project CM Plan.	
2.6.1.2	All projects shall designate an internal Project Configuration Manager who is responsible for planning, performing, and verifying internal Project CM activities and for coordinating with the OIT CM Organization.	
2.6.1.3	All Configuration Management activities shall be conducted in accordance with the appropriate Customs Configuration Management (CM) Plans.	For software, see the Customs OIT Software Configuration Management (CM) Plan.
2.6.1.4	Work products to be placed under Configuration Management shall be identified, controlled, and baselined.	
2.6.1.5	Products shall be created from the project's baselined CIs as maintained in the CM repository. Their release shall be controlled by Project CM according to a documented procedure.	Also see Section 2.6.6.2, Libraries and Respositories.
2.6.1.6	Configuration Management shall be applied to identified work products, including all tools and components needed to recreate the previous version of the configuration item.	
2.6.1.7	The Project CM Team shall create, maintain, and implement a Project CM Plan that defines: • A set of internal Configuration Management procedures, • Configuration Management activities and specific project staff responsibilities, and • Designated configuration items for the project.	
2.6.1.8	The Project Manager, in consultation with the OIT CM Organization, is responsible for the Project CM Plan approval and for incorporation of the configuration management activities into the overall Project Plan.	
2.6.1.9	If a modeling tool is used, project CM procedures shall be developed and documented to handle versions of the same model.	

2.6.2 Migration		
Number	**Text**	**References**
2.6.2.1	Only properly authorized, tested, and approved hardware, system software, applications, and application changes shall be moved into the Production environment.	See mandatory minimum activities listed in Chapter 4, Customs Standard Life Cycle. Also see ISD's Standard

2.6.2 Migration		
Number	**Text**	**References**
		Operating Procedures for Operating System Support.
2.6.2.2	The Project CM Team is responsible for providing the OIT CM Organization with a change package that contains a complete list of all configuration items to be implemented.	
2.6.2.3	The OIT CM Organization is the only group authorized to migrate applications and application changes into Testing at the request of the Tester and then into the Production and the Education environments upon approval by the Business Sponsor.	
2.6.2.4	Projects which meet one or more of the emergency definition criteria are moved into Production upon the approval of the Testers outside of the regularly scheduled application migration periods.	
2.6.2.5	Emergency project moves shall follow currently established emergency procedures.	See ISD's Systems Operations Branch CM Team's Standard Operating Procedure *Change Control/Change Management Overview for Non-Emergency and Emergency Projects.*

2.6.3 Change Control		
Number	**Text**	**References**
2.6.3.1	A Project Change Control Board (CCB) shall be established having the authority for managing the project's baselines. The CCB shall record, review, approve/disapprove, prioritize, and track change requests and problem reports for all configuration items/units.	
2.6.3.2	If additional functionality needs to be added, a change request shall be initiated and tracked.	See Section 2.3.8.3, Variance for Re-reviews.
2.6.3.3	Changes to baselines shall be controlled according to a documented procedure.	

2.6.4 Audits and Status Reporting		
Number	**Text**	**References**
2.6.4.1	The Project CM Team shall record the status of project configuration items/units (CIs).	
2.6.4.2	Each project shall produce standard reports covering their configuration management activities and baseline contents. Copies of these reports shall be made available to all affected groups and individuals.	
2.6.4.3	The OIT CM Organization shall record and report status of the Production baselines and CIs.	

2.6.4 Audits and Status Reporting		
Number	**Text**	**References**
2.6.4.4	Project CM shall gather, collect, and report metrics to determine the status of its CM activities and CIs.	
2.6.4.5	A group external to the Project CM Team shall periodically audit configuration item baselines and verifies that they conform to the documentation that defines them.	
2.6.4.6	Configuration Management processes and activities shall be reviewed in accordance with Project Monitoring and Quality Assurance policies.	See: • Section 2.4.1.1, Project Manager Reviews. • Section 2.4.1.2, Senior Management Reviews. • Section 2.5.1.1, Internal Project QA Reviews.

2.6.5 CM Training		
Number	**Text**	**References**
2.6.5.1	The members of all affected organizations who are responsible for performing CM-related activities shall be trained in the objectives, procedures, and methods for performing their CM activities.	
2.6.5.2	Members of the OIT CM Organization and the Project CM Team shall be trained in the objectives, procedures, and methods for performing their configuration management activities.	
2.6.5.3	Members of the Project Team and other software-related groups shall be trained to perform their Configuration Management activities.	

2.6.6 Libraries and Repositories		
Number	**Text**	**References**
2.6.6.1	There shall be separate and distinct libraries for all environments (development, test, education, production, etc.).	
2.6.6.2	A Configuration Management library system shall be established as a repository for each project for software and documentation baselines.	

2.7 IT Security

Description: At the broadest levels, security policies are intended to protect assets from harm. These assets include the electronic data, software, hardware, networks, people, facilities, etc. needed to gather, store, process, and transport Customs information in electronic form. Some

physical, personnel, and administrative controls must be provided by the environment in which these electronic systems operate. However, technical controls must be built into the computer hardware and software systems, whether they are applications or infrastructure.

Security requirements cited in this document are explained in the *Information Systems Security Policy and Procedures Handbook*, CIS HB 1400-05A.

The overall goals of IT Security are to:

- Ensure appropriate security services are provided;
- Provide assurances that IT security features work as claimed and cannot be easily defeated; and
- Ensure the IT system has reasonable security controls to appropriately preserve the data's integrity, availability, and confidentiality.

This section provides the high-level policy mandates that directly affect the requirements for and the designs of Customs' electronic systems. These mandates are organized into the following subcategories:

- 2.7.1 Security documentation requirements
- 2.7.2 Security data and access requirements
- 2.7.3 Security Certification and Accreditation requirements
- 2.7.4 Security training requirements

Policies:

2.7.1 Security Documents		
Number	**Text**	**References**
2.7.1.1	Connectivity between internal Customs IT systems and all non-Customs systems or networks is prohibited without an approved Memorandum of Understanding and Interconnection Security Agreement (ISA).	See Appendix E of the *Information Systems Security Policy and Procedures Handbook*, CIS HB 1400-05A, for a complete description.
2.7.1.2	The Security Plan as defined in Customs guidelines may NOT be tailored.	**Note:** This is an exception to Section 2.3.3, Tailoring.
2.7.1.3	An annual Security Plan shall be competed/updated for each system or subsystem, regardless of its life cycle stage. Each plan is subject to a no-notice review by the Office of Management and Budget (OMB).	For additional information, contact OIT's Information Systems Security Branch (ISSB). Reference: Computer Security Act of 1987.

<table>
<tr><th colspan="4">2.7.1 Security Documents</th></tr>
<tr><th>Number</th><th colspan="2">Text</th><th>References</th></tr>
<tr><td rowspan="4">2.7.1.4</td><td colspan="2">The following Security-related documents must be created/updated, submitted, and resubmitted on a regular basis:</td><td rowspan="4">See Chapter 4, Customs Standard Life Cycle, for timeline, responsibilities, and approval authorities.</td></tr>
<tr><td>Document</td><td>Resubmission Schedule</td></tr>
<tr><td>Security Plan
Disaster Recovery Plan
Contingency Plan
Contingency Plan Test Report</td><td>Annually</td></tr>
<tr><td>Security Requirements
Security Design
Security Test Plan
Security Test Results Report
Security Features User's Guide
Trusted Facility Manual
Disaster Recovery Test Report</td><td>As required for major system changes</td></tr>
<tr><td>Security Risk Assessment
Security Certification
Security Accreditation
Interconnection Security Agreement (if applicable)</td><td>• Upon major system changes
• Upon major environment changes
• Upon significant security vulnerability changes
• At least every three years</td></tr>
</table>

2.7.2 Security Requirements		
Number	**Text**	**References**
2.7.2.1	All Customs data, applications, and systems are considered sensitive and must employ appropriate safeguards, according to guidelines.	See Treasury TD P 71-10, Chapter VI, Section 2A, paragraph 4b.
2.7.2.2	Production data must NOT be used for development, testing, or training.	
2.7.2.3	The Business Sponsor is responsible for informing OIT of all changes to the business area's Business Impact Analysis (BIA) and Continuity of Operations Plan (COOP).	See Appendix A, Glossary, for definitions of these business area documents.

2.7.2 Security Requirements		
Number	**Text**	**References**
2.7.2.4	All Customs systems must uniquely identify and authenticate each user.	Also see: • Section 2.2, Requirements Management. • *Information Systems Security Policy and Procedures Handbook*, for access and separation policies and procedures.
2.7.2.5	All Customs Systems must track each user's activities throughout all subsequent processes.	
2.7.2.6	Everyone shall receive only the set of security access privileges needed to perform their authorized tasks and no more.	Also see Appendix A of the Information Systems Security Policy and Procedures Handbook for separation procedures
2.7.2.7	Every application and infrastructure system shall follow the generic security rules (Security Standards of Use) listed in Appendix A of the Information Systems Security Policy and Procedures Handbook (CIS HB 1400-05A). Any additional system-specific security rules must be listed in the Security Plan.	Also see Section 2.2, Requirements Management.
2.7.2.8	All systems must be designed to allow for audits of all security-relevant events.	
2.7.2.9	The Business Sponsor/BITR is responsible for designating a Computer Security Officer (CSO) for every IT system whether infrastructure or individual application.	This assignment is documented in the system's Security Plan. Also see the *Information Systems Security Policy and Procedures Handbook*.

2.7.3 Security Certification and Accreditation		
Number	**Text**	**References**
2.7.3.1	Security Certification and Security Accreditation must be completed for each IT system in the USCS before it is moved into Production.	See the *Information Systems Security Policy and Procedures Handbook*

2.7.4 Security Training		
Number	**Text**	**References**
2.7.4.1	All employees and contractors involved with the management, use, design, development, maintenance, or operation of computer systems (both applications and infrastructure) shall receive training in: • Their security duties and responsibilities • The penalties imposed for non-conformance	

2.7.4 Security Training		
Number	**Text**	**References**
2.7.4.2	IT security orientation and technical training shall occur prior to carrying out security duties or using any security features. IT security refresher training must occur at least annually.	**Note:** This is required by Office of Personnel Management and Office of Management and Budget (OMB), per the Computer Security Act.
2.7.4.3	All affected organizations shall train members of their groups in the objectives, procedures, and methods for performing their security-related activities.	

2.8 Contract Management

Description: Contract Management involves selecting an IT contractor/subcontractor, establishing commitments, and monitoring the contractor/subcontractor's performance and results. These practices cover the management of a software (only) contract as well as the management of all the components of a contract that includes software, hardware, and possibly system components.

The goals of Contract Management are to:

- Select qualified contractors and/or subcontractors;
- Ensure the contractor and subcontractors agree to their commitments to each other;
- Maintain ongoing communications; and
- Track the contractor/subcontractor's actual results and performance against its commitments.

This section includes policies concerning:

- 2.8.1 Requirements for the evaluation, selection, and acquisition of IT products and services on projects
- 2.8.2 How a project manager shall plan and control the work performed
- 2.8.3 How the contractor/subcontractor activities and results shall be tracked and reviewed
- 2.8.4 Requirements for quality assurance and configuration management
- 2.8.5 Training in contract management responsibilities

Policies:

2.8.1 Product and Service Procurement		
Number	**Text**	**References**
2.8.1.1	The Statement of Work (SOW) shall be written with particular attention paid to defining the critical success factors and measures of performance.	Contact the Acquisition Organization for advice and assistance.
2.8.1.2	Any changes to the SOW must be approved according to the procedure defined by the Procurement Division, Office of Finance.	
2.8.1.3	The contractors'/subcontractors' qualifications shall be evaluated during the selection process. This shall be done according to the procedures established by the Procurement Division, Office of Finance (OFPD).	

2.8.2 Planning and Control		
Number	**Text**	**References**
2.8.2.1	Each contract shall have a contract administrator, a contracting officer, and a Contracting Officer's Technical Representative (COTR). All are appointed by the Office of Finance.	
2.8.2.2	During the project, technical work performed by the contractor/subcontractor shall be planned, documented, and approved before the activities are begun.	Also see Acquisition Policies as defined by the System Acquisition Process Group (SAPG).

2.8.3 Contract Monitoring		
Number	**Text**	**References**
2.8.3.1	Regular meetings with the contractor/subcontractor management shall be scheduled in the project plan. Results shall be documented and distributed.	
2.8.3.2	Technical work to be performed by the contractor/subcontractor shall be tracked and formally reviewed on a regular basis.	

2.8.4 Quality Assurance		
Number	**Text**	**References**
2.8.4.1	Quality assurance and configuration management activities shall be performed, monitored, and documented.	
2.8.4.2	Periodic quality assurance reviews of contractor/subcontractor technical activities shall be defined within the SOW and performed as indicated.	

2.8.5 Contract Management Training		
Number	**Text**	**References**
2.8.5.1	All affected organizations shall train members of their groups in the objectives, procedures and methods for performing their Contract Management activities.	

Chapter 3
Customs Life Cycle Concepts

3.1 What is a Life Cycle?

A life cycle is a series of ordered, repeatable activities used to develop, maintain, and retire an information and technology (IT) system, product, or hardware configuration. It defines when activities will occur during the life of the system.

3.2 Benefits

Use of a clear, well-defined life cycle increases the probability that:

- Cost, schedule, and functionality will be predictable
- The system's performance will meet the user's needs
- High quality products will be developed and maintained within budget and on time
- Resources will be efficiently controlled and applied
- Systems will comply with relevant standards and regulations
- Systems will be produced in a disciplined, repeatable, engineered manner
- Risk will be accurately assessed and mitigated
- Management control is consistently applied
- The development process will produce a complete set of deliverables

3.3 What is the Difference Between "SDLC" and "Customs Standard Life Cycle"?

The SDLC is this entire handbook and is the all-encompassing term for the collection of policies, approved life cycles, and high-level processes. The entire SDLC defines management expectations for developing and maintaining Customs IT systems.

The Customs Standard Life Cycle is the framework that describes the activities, reviews, and deliverables that occur during a development life cycle. These are organized into conceptual stages (e.g., Design) which are high-level processes. The model provides expected entry criteria, inputs, outputs, exit criteria, activities, and responsibilities for each of these high-level processes.[3]

The Customs Standard Life Cycle model must be **tailored** to create a project plan and work breakdown structure that meets the specific needs of each project based on project size, complexity, visibility, and project risk.

[3] In CMM terms, the Customs Standard Life Cycle defines the "organization's standard software process". The approved Project Plan documents the "project's defined software process" which is tailored and approved based on the standard software process, approved life cycles, and project needs.

The terms "project plan", "work breakdown structure (WBS)", and "schedule" are discussed below:

- A **Project Plan** is a management document describing the approach to be taken for a project. It describes the work to be done, resources required, development methods and management strategies to be used, constraints and assumptions, project organization, assigned roles and responsibilities, as well as milestones to be met. The WBS and Schedule are essential parts of this plan as well.

- A **WBS** is a family-tree division of all tasks for the project, consisting of hierarchical levels of detail, including phases and steps at intermediate levels. It organizes, defines, and graphically displays the work to be done to achieve the specified product. At the lowest level, it subdivides the project into individual tasks that are defined, estimated, and tracked.

- A **Schedule** is the WBS tasks organized along a timeline. The Schedule is created when tasks, estimates of required effort (as modified based on assigned staff), staff availability, and critical dependencies are interwoven to create the most efficient plan of action over time. It is often depicted graphically and completion of project activities and milestones is tracked against this timeline.

- A **task** is a defined unit of work for one or more persons which has a measurable end. The level of effort required to complete the task is estimated and tracked.

3.4 How Do We Use the Customs Standard Life Cycle?

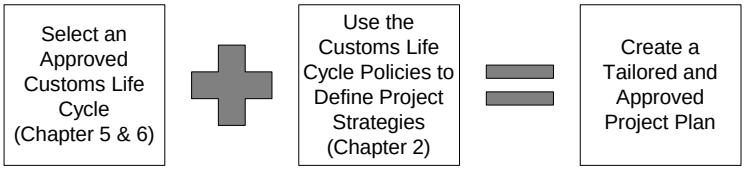


Figure 3.1, Evolution of a Project Plan

Figure 3.1 shows the high-level evolution of a project plan. After collecting requirements and evaluating constraints, the Project Team:

- Selects an approved Customs Life Cycle based on the advantages and disadvantages of the life cycles.

- Defines project strategies in keeping with Customs Life Cycle Policies

- Using all of the above, the project
  - Tailors the Customs Standard Life Cycle activities and deliverables to create a Tailored Project Plan (including WBS and schedule)
  - Performs Project Tailoring Reviews with all affected organizations
  - Has its Tailored Project Plan reviewed and approved by Senior Management

- A Project Work Authorization is issued to begin development after the Project Initiation Review is completed

The Systems Life Cycle (SLC) Organization is available to assist projects in understanding the SDLC in order to create their tailored Project Plan. These SDLC Assist Visits may also include representatives from the Investment Organization and Evaluation Organization.

3.5 What are the Basic Principles of the Customs SDLC?

The following principles form the foundation of the Customs development processes.

3.5.1 User Primacy

Every system development project begins and ends with the user. Systems development focuses on satisfying user requirements through defined, documented, mission-related performance goals for that system. Business Sponsors and users continue this involvement until the system is retired.

3.5.2 Disciplined Project Management Goals

- Every system development project shall be managed as a valuable taxpayer investment using a disciplined engineering process with effective management controls.

- Disciplined Projects:
  - Repeat successes by following a framework of processes, such as the SDLC;
  - Mitigate the risks associated with complex programs by re-using structured activities and artifacts.

- Well-engineered projects:
  - Document their plans;
  - Follow those plans; and
  - Retain evidence of their work.

- Projects require effective management and oversight to ensure that the system is developed on schedule, within budget, and produces the expected results. This includes providing:
  - The right people on the project team with clearly defined roles, objectives, and responsibilities;
  - Adequate resources to accomplish the tasks; and

- A solid, effective communication mechanism for reporting progress, identifying issues, and sharing lessons learned.

3.5.3 All Projects Shall…

- Perform project planning and monitoring activities governed by a Project Plan which is tailored to fit the project, including mandatory reviews;
- Have mission-related performance goals and acceptance criteria for the system;
- Have clear user requirements that are testable and traceable to the work products produced;
- Meet Security requirements;
- Perform Quality Assurance throughout the project's life cycle;
- Perform Configuration Management;
- Establish mechanisms to capture, prioritize, and track:
  - Work and change requests;
  - Intra-project issues;
  - Inter-project issues.

3.5.4 Projects shall be subject to management reviews and approvals.

Management reviews and approvals are defined in the Customs Standard Life Cycle in Chapter 4. They are consistent with the Customs Enterprise Life Cycle Methodology. Under the umbrella of the Enterprise Life Cycle Methodology, the IMP and SDLC, along with the Customs strategic planning process, the budget process, and the Enterprise Architecture process provide executive direction, control and management of Customs IT investments.

3.6 How Does the Customs Standard Life Cycle Fit With the Investment Management Process (IMP)?

This version of the SDLC has been integrated with the IMP to simplify the project's view of the process from concept through retirement. The stages of the Customs Standard Life Cycle incorporate the required IMP deliverables, reviews, and approvals.

In addition to the reviews/audits that are conducted within the development life cycle, there are a series of reviews that are performed by groups outside the project to give Customs, Treasury, and OMB executives objective decision criteria and status for each project. These reviews are included in the Customs Standard Life Cycle.

Figure 3.2 shows the relationship between the Customs Standard Life Cycle stages and the Investment Management Process phases. While these stages are depicted conceptually in a waterfall fashion, actual projects may use iterative, parallel, or spiral time lines.

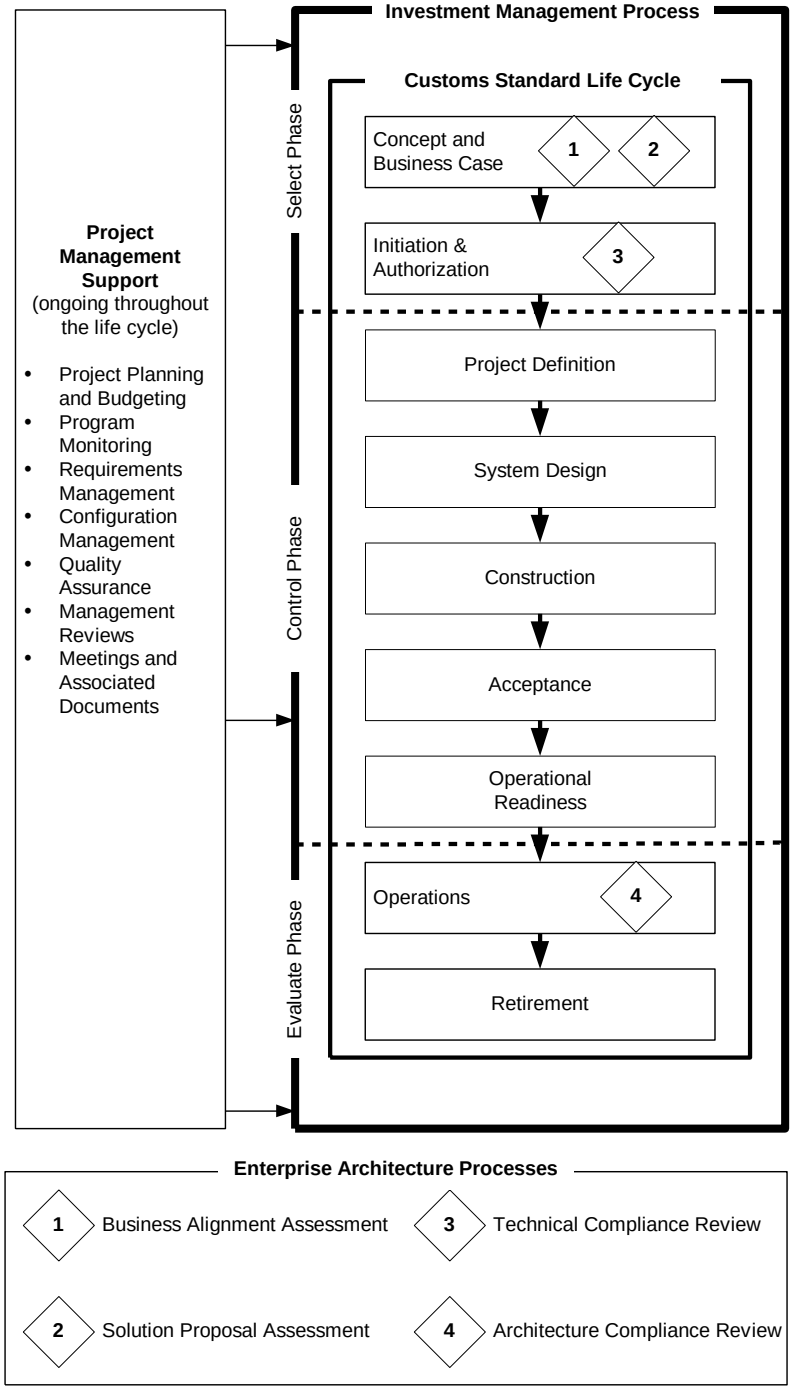


Figure 3.2, Customs Standard Life Cycle, the Investment Management Process, and the Enterprise Architecture Processes

3.7 How Does the Customs Standard Life Cycle Fit With the Enterprise Architecture?

An effective Enterprise Architecture enables Customs to make more informed IT investment decisions that align with the business mission and to control the evolution of the technology environment.

The Customs Standard Life Cycle includes architecture-related processes that provide checkpoints to ensure that the project complies with all applicable technical standards and align with the business mission. These checkpoints are:

- A Business Alignment assessment and a Solution Proposal assessment which are performed as part of the Concept and Business Case Stage
- Technical Compliance Reviews which occur during Project Initiation and Authorization
- Architecture and SDLC Compliance Reviews which occur during the project's life cycle and after the system is in Operation.

An Enterprise Architecture Repository has been established with baseline and target information including:

- Business process profiles;
- Application system profiles;
- Infrastructure platform views; and
- The Technical Reference Model (TRM).

For more details, see the *Customs Enterprise Architecture Blueprint*.

Chapter 4
Customs Standard Life Cycle

4.1 Introduction

The Customs Standard Life Cycle includes the stages, task/activities, reviews, and deliverables which must be accounted for by all projects. It is the foundation upon which other life cycles are built and against which specific projects are measured.

Regardless of the development life cycle model chosen, all projects that develop or maintain IT products built by or for the United States Customs Service shall use the policy in this chapter.

4.2 How to Use this Chapter

4.2.1 How to Use the Customs Standard Life Cycle

After considering the Customs Life Cycle Policies defined in Chapter 2, projects will select an appropriate life cycle from either Chapter 5 or 6 based on the needs of the project. Projects will develop a Project Plan using the life cycle combined with the stages, tasks, and activities of the Customs Standard Life Cycle in this chapter.

Based on project size, complexity, visibility, and risk, the tasks/activities and deliverables listed in the SDLC may be combined or expanded. However, each must be specifically accounted for and maintained along with tailoring rationale as part of the tailoring documentation. The Customs Process Asset Library (PAL) contains templates, examples, and procedures that projects will consult in order to take advantage of existing good practices. When approved by Senior Management (including a written record of tailoring actions) and a Project Work Authorization is issued, the tailored Project Plan will become the project's SDLC-compliant road map. Figure 4.1 summarizes this process.

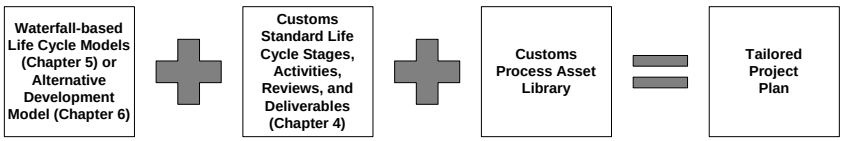


Figure 4.1, How to Develop a Project Plan

The SLC Organization is available to assist projects in understanding the SDLC in order to create their tailored Project Plan. These SDLC Assist Visits may also include representatives from the Investment Organization and Evaluation Organization.

4.2.2 Thresholds

The thresholds shown in Table 4-1 below combine the Investment Management Process and the Systems Development Life Cycle thresholds for approvals. These apply to all IT projects regardless of sponsor, developer, project size, methodology, or technology used. As guided by this table, projects must account for all reviews, approvals, and criteria of the Customs Standard Life Cycle.

Additional details concerning the investment review and selection process and its deliverables can be found in the *Investment Management Process System Description* and by contacting the Planning Group.

Table 4-1 -- Project Process Thresholds

Projected Total Life Cycle Cost	Funded?	High Risk?	Business Case Required?	Approval Authority	Follow Customs Standard Life Cycle?
$100,000 or less	Yes	Yes	Yes	IRB	Yes
		No	No	TRC	
	No	Yes	Yes	IRB	
		No	Yes	IRB	
$100,001 - $1 million	Yes	Yes	Yes	IRB	
		No	Yes	ITC	
	No	Yes	Yes	IRB	
		No	Yes	IRB	
Over $1 million	Yes	Yes	Yes	IRB	
		No	Yes	IRB	
	No	Yes	Yes	IRB	
		No	Yes	IRB	

4.2.3 What Information Will This Chapter Give Me?

A short description of each stage is presented in Section 4.3, with graphical representations of the Customs Standard Life Cycle in Figures 4.2 and 4.3. In addition, the following information is presented:

For Each Stage

- The stage's generic order within the life cycle
- The name of the stage
- Entry criteria for the stage
- Inputs to the stage
- Exit criteria for the stage
- Outputs from the stage
- The tasks and activities within each stage

For Each Task/Activity

- Task name
- Deliverables/outputs for each task
- The functional role having primary responsibility (see Appendix B for role summary)
- The functional role having a support responsibility or input
- Notes and references

Definitions of these items follow:

Entry Criteria: Indicates the conditions which must exist when the stage begins.

Inputs: Identifies the work products that must be present before the activities of a specific stage can be performed.

Outputs: Identifies the work products that are generated or produced within a specific stage.

Exit Criteria: Indicates the conditions under which the stage can be declared complete.

Tasks/Activities: Indicates the steps involved in implementing a stage/activity.

- An activity is the action, steps, or process taken to create or achieve a specific product, service, or result. Activities may identify either the "What" or the "How".

- A task is a defined unit of work for one or more people with a measurable endpoint. Multiple tasks may be defined to complete one activity.

Primary Responsibility: Identifies those who perform hands-on activities or who have specific approval authority. The roles listed are functional roles rather than titles; see Appendix B for role definitions and a summary of the role's responsibilities.

Support Responsibility: Includes those who provide assistance, reviews, and concurrence with results/outputs. Support responsibilities also include sources that the project can tap for expert advice. The roles listed are functional roles rather than titles. See Appendix B for role definitions and a summary of the role's responsibilities.

4.3 Customs Standard Life Cycle Stages

Stage 1 -- Concept and Business Case: This life cycle stage begins with the business need for a particular automated solution and ends with the release of funds to begin development. Included in this stage are Enterprise Architecture reviews by the Technology and Architecture Group (TAG), and reviews by the Technology Review Committee (TRC), the Information Technology Committee (ITC), and the Investment Review Board (IRB), depending on the project size, life cycle cost, risk, and funding availability.

Stage 2 -- Initiation and Authorization: This stage begins when funding is released to begin detailed project planning. This includes developing a draft of user requirements and infrastructure planning, a technical compliance review, an initial project plan, and appropriate life cycle tailoring. This stage ends with a review process (i.e., the Project Tailoring Reviews and Project Initiation Review) that authorizes the project to continue with development.

Stage 3 -- Project Definition: During Project Definition, information created in the previous stage is further refined until a clear set of functional requirements can be produced and certified by the Business Sponsor. On the basis of these requirements, the technical planning and support area documentation are created.

Stage 4 -- System Design: During System Design, the development team uses the requirements to create the technical design of the system under development. This stage ends with a Critical Design Review, in which the Business Sponsor reviews the work products and certifies that the system design meets the business need.

Stage 5 -- Construction: During this stage, the requirements and design developed during the previous stages are translated into operational work products (e.g., infrastructure, source code, and databases). These work products and code then undergo unit and integration testing by the development team and supporting organizations until the system is ready for acceptance testing. Also, equipment is received and checked to ensure proper operation and integration.

Stage 6 -- Acceptance: There are two types of acceptance testing that occur in this stage. First the system is tested to ensure that it interfaces properly with other automated systems within the Customs environment. Secondly, independent testers and the users test the system to ensure that the developers have delivered a system that meets the needs stated in the user and functional requirements. Security Certification and Accreditation are obtained during this stage.

Stage 7 -- Operational Readiness: At this point, the new system is moved into the Customs Production environment in preparation for operational processing. While the system is now in the Production environment, it has not yet been transitioned to full operation. Activities during this transition stage include:

- Implementing the system, including site preparations, infrastructure installation/deployment, data conversions, and scheduling as necessary to make the new system available to the general users
- Database and system code installation into the Production environment
- Field testing and parallel operations as required
- Finalizing User Documentation and Training Materials
- Documenting project experiences and lessons learned.

For some projects, particularly legacy mainframe systems and very small projects, this stage may take less than a day to complete because there will be few, if any, changes to documentation and/or infrastructure.

Stage 8 -- Operations: The system is in general use throughout the U.S. Customs Service. This stage consists of activating and rolling out the system plus the activities to monitor performance of the system in production and ensure continuity of operations. This includes:

- Performance monitoring and management feedback
- Tracking of system performance statistics, costs, and resource allocations
- Detecting defects in the application, operation, and local systems
- Assessing the system's efficiency and effectiveness to determine if the investment was cost beneficial and achieved the planned functionality
- Managing system and infrastructure problems
- Recovering from system and infrastructure problems
- Implementing system and infrastructure changes

The system is reviewed while in production to ensure that it continues to meet user needs and accreditation requirements. Independent evaluations may also be performed during this and other stages of the life cycle to validate that project standards, processes, and requirements are being complied with.

Stage 9 -- Retirement: When a system no longer meets Customs needs, its existence is terminated and any data or modules not needed by replacement systems are archived and stored in a secure off-site location. Affected stakeholders are notified of the intent to retire the system and upon completion of this project.

Project Management Support: Project management support encompasses many of the disciplined activities which lead to higher levels of capability maturity. While not a formal "stage", these mandatory tasks/activities occur during more than one life cycle stage throughout the duration of the project. These engineering activities include project planning and budgeting activities, program monitoring activities, requirements management, configuration management, quality assurance, and miscellaneous project support activities.

Figures 4.2 and 4.3 depict the Customs Standard Life Cycle stages in a summary fashion. These summaries are provided in order to be easily extracted and distributed for training and briefings. The specific details are provided in the individual stage descriptions which follow.

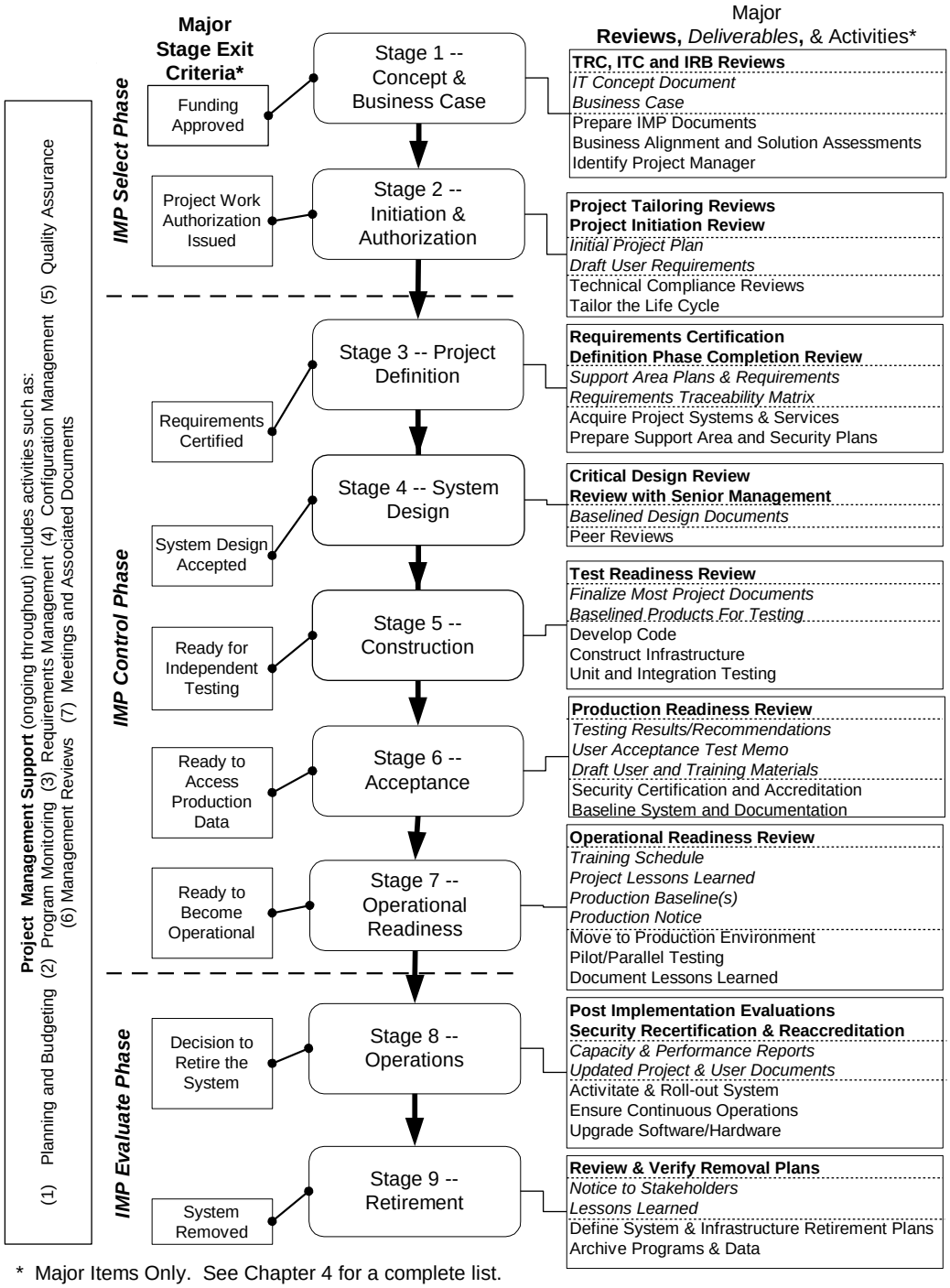


Figure 4.2, Customs Standard Life Cycle – Overview

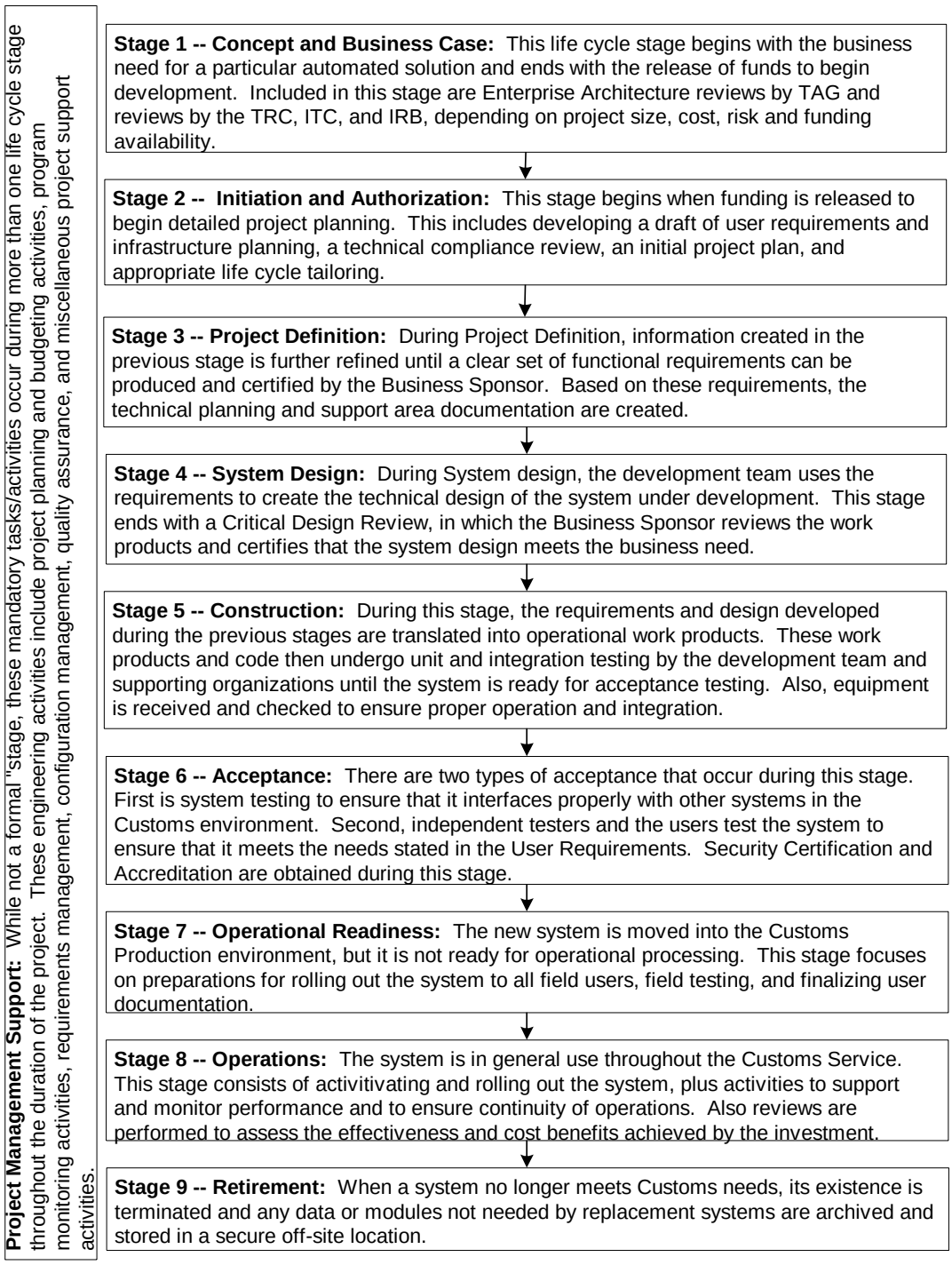


Figure 4.3, Customs Standard Life Cycle – Stage Descriptions

Stage 1 -- Concept and Business Case

Stage 1 -- Concept and Business Case Entry Criteria

- General need for an IT system is expressed by the Business Sponsor

Stage 1 -- Concept and Business Case Inputs

- Business Need
- Business Sponsor's/User Ideas/Concepts

Stage 1 -- Concept and Business Case Exit Criteria

- Business Sponsor (and BITR) receives notification of funding amount approved

OR

- Project is under $100K, already funded, and has received approval from either the TRC, ITC, or IRB as appropriate

OR

- Project was not approved by either the TRC, ITC, or IRB (Therefore, Project may not continue)

Stage 1 -- Concept and Business Case Outputs

- IT Concept Document (ITCD)
- ITCD Decision Memo
- Architectural Waiver Justification, if applicable
- Business Alignment 2X2 Matrix
- Business Case, including
- Business Case Worksheet
- Operational Concept
- Evaluation of Alternatives (COTS, GOTS, etc.)
- Timeline
- High Level Costs
- Preliminary Cost Benefit Analysis, if applicable
- Notification of Funding Approval, if applicable

Stage 1-- Concept and Business Case Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities[4]**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Create Project Concept	IT Concept Document (ITCD)	Business Sponsor	Business Information Technology Representative (BITR), Business Interface Representative (BIR), Architecture Organization, Acquisition Organization, ISD Support Teams	**This deliverable is mandatory for all projects.** **Reference:** *Investment Management Process System Description*
Identify COTS/GOTS, etc. for further Application Product Evaluations	Preliminary COTS/GOTS, etc. Evaluation Results	Business Sponsor, Product Evaluation Team	Support Organizations, Architecture Organization	If applicable. **Note:** Existing systems with similar functionality should be investigated as a first resort. Depending on cost and complexity, this task itself may need to be approved and authorized through Stages 1 and 2.
Review High-level Business Alignment and Architecture	• Updated ITCD with TAG Recommendation • Business Alignment 2X2 Matrix	Architecture Organization, Evaluation Organization	Business Sponsor, Senior Management, ISD Support Teams	**Note:** This includes performing a Business Alignment Assessment and a Solution Proposal Assessment.

[4] Primary responsibilities include those who perform hands-on activities or who have specific approval authority; support responsibilities include assistance, reviews, and concurrence with results/outputs. Support responsibilities also include sources that the project can tap for expert advice.

Stage 1-- Concept and Business Case Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities[4]**		**References, Resources, Notes and Comments**
		Primary	**Support**	
TRC Approval Process	• ITCD Decision Memo, • Architectural Waiver Justification, if applicable	Technology Review Committee (TRC)	Business Sponsor, Technology and Architecture Group (TAG)	**Reference:** *Investment Management Process System Description* **Note:** See Thresholds in Table 4-1. ITC must review and approve all architectural waivers.
Identify Project Manager		Senior Management		**Note:** Project Manager refers to the technical manager responsible for the day-to-day success of the project.
Create Business Case	Business Case, including: • Worksheet, • Operational Concept (including definition of environment), • Evaluation of System Alternatives, • Timeline, • High Level Costs, • Preliminary CBA	Business Sponsor, BITR, Project Initiation Team	Investment Organization, BIR, Acquisition Organization, Evaluation Organization, Training Organization, Infrastructure Services Division	**Reference:** *Investment Management Process System Description* **Note:** See Thresholds in Table 4-1.
ITC Approval Process	Project Authorization Documents	Information Technology Committee (ITC)	Investment Organization	If applicable. **Note:** See Thresholds in Table 4-1.
IRB Approval Process	Cover page for Authorization Package	Investment Review Board (IRB)	Investment Organization	If applicable. **Note:** See Thresholds in Table 4-1.
Release Funding	Notification of Funding Approval	Planning Group	IRB	If applicable.

Stage 2 – Initiation and Authorization

Stage 2 -- Initiation and Authorization Entry Criteria

- Business Sponsor (and BITR) receives notification of funding amount approved

OR

- Project is under $100K, already funded, and has received approval from either the TRC, ITC, or IRB as appropriate

Stage 2 -- Initiation and Authorization Inputs

- IT Concept Document (ITCD)
- ITCD Decision Memo
- Architectural Waiver Justification, if applicable
- Business Alignment 2X2 Matrix
- Business Case, including
- Business Case Worksheet
- Operational Concept
- Evaluation of Alternatives (COTS, GOTS, etc.)
- Timeline
- High Level Costs
- Preliminary Cost Benefit Analysis, if applicable
- Notification of Funding Approval, if applicable

Stage 2 -- Initiation and Authorization Exit Criteria

- All action items from the Project Tailoring Review have been resolved

AND

- Senior Management approval of the project has been received

AND

- Project Work Authorization has been issued

Stage 2-- Initiation and Authorization Outputs

- Tailored Life Cycle and Deliverables Set
- Technical Compliance Review Results
- Initial Project Plan
- Release Plan, if applicable
- Project Initiation Package, including
- Project Initiation Worksheet
- Detailed Cost Estimates
- Detailed Cost Benefit Analysis, if applicable
- Draft
  - User Requirements Document
  - Acquisition Plan, if applicable
  - Infrastructure Plan
- Project Work Authorization

Stage 2 -- Initiation and Authorization Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Identify Initial Members of the Project Team		Project Manager, Senior Management		**Note:** This includes, at a minimum, identification of initial members of Project QA and Requirements Analysis staff. Additional Project Team members may be added in later stages.
Document User Requirements	• Draft of User Requirements Document, • Minutes of review with the User	Business Sponsor, Users	Development Team, BIR, BITR	**This deliverable is mandatory for all projects.** **Note:** The Requirements document must have enough detail for project estimation.
Select Appropriate Life Cycle and Identify Tasks/Deliverables	• Tailored Life Cycle and Deliverables Set • Results of Technical Compliance Review	Project Manager	Support Organizations, SLC Organization, Evaluation Organization, Architecture Organization	**This deliverable is mandatory for all projects.**
Create Initial Project Plan	• Initial Project Plan, • Release Plan, if applicable	• Business Sponsor, • Project Manager	Acquisition Organization, Evaluation Organization, Support Organizations, Process Groups, SLC Organization, TAG	**This deliverable is mandatory for all projects.** **Note:** The Project Plan must be developed in consultation with all stakeholders.
Create Infrastructure Plan	Infrastructure Plan	Project Manager, Infrastructure Services Division		**Note:** This may be combined with the Project Plan.

Stage 2 -- Initiation and Authorization Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Develop Acquisition Plan	Acquisition Plan	Business Sponsor, Acquisition Organization, Project Manager	Project Planner, Contracting Officer	If applicable **Note**: The Acquisition Organization may also contact the Office of Finance, Procurement Division (OFPD) for assistance.
Create Initiation Documentation	Project Initiation Package, including • Worksheet, • Detailed Cost Estimates, • Detailed CBA	Business Sponsor, Project Team	Project Manager, Investment Organization	**Reference:** *Investment Management Process System Description*
Conduct Project Tailoring Reviews	• Project Tailoring Review Package, • Agenda, Minutes and Action Items, • Senior Management Approval	Project Manager, Senior Management	Business Sponsor, SLC Organization, Program Monitoring Group (PMG), Evaluation Organization, BIR, Support Organizations, OIT QA Organization, Infrastructure Services Division, Investment Organization	**This review is mandatory for all projects.**

Stage 2 -- Initiation and Authorization Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Perform Project Initiation Review	Project Work Authorization Memo	Investment Organization	Division Director, TAG, PMG, BIR, SLC Organization	**This review is mandatory for all projects.** **Reference:** *Investment Management Process System Description* **Note:** Project engineering, development, and detailed definition work may not begin without a Project Work Authorization. Signatory for the Project Work Authorization Memo is the Director, Planning Group

Stage 3 – Project Definition

Stage 3 -- Project Definition Entry Criteria

- All action items from the Project Tailoring Review have been resolved

AND

- Senior Management approval of the project has been received

AND

- Project Work Authorization has been issued

Stage 3 -- Project Definition Inputs

- Tailored Life Cycle and Deliverables Set
- Technical Compliance Review Results
- Initial Project Plan
- Release Plan, if applicable
- Project Initiation Package, including
- Project Initiation Worksheet
- Detailed Cost Estimates
- Detailed Cost Benefit Analysis, if applicable
- Draft
  - User Requirements Document
  - Acquisition Plan, if applicable
  - Infrastructure Plan
- Project Work Authorization

Stage 3 -- Project Definition Exit Criteria

- Requirements Certification is completed

AND

- Project Manager signs-off on Definition Phase Completion

Stage 3 -- Project Definition Outputs

- User and Functional Requirements Documents
- Requirements Certification Form
- Initial Requirements Traceability Matrix (RTM)
- Finalized Acquisition Plan(s)
- Contract Award, if applicable
  - Training Requirements Document
- Final Configuration Management (CM) Plan
- Final Quality Assurance (QA) Plan
- Security Documents
- Security Plan
- Security Risk Assessment
- Draft Disaster Recovery Plan
- Draft Contingency Plan
- Draft Security Test Plan
- Draft Trusted Facility Manual
- Interconnection Security Agreements, if applicable
- Other Draft Support Plans
  - System Test Plan
  - Data Management Plan
  - Implementation Plan
  - Deployment Plan
  - Project Risk Management Plan and Project Risks Database

Stage 3 -- Project Definition Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Update User Requirements	User Requirements document	BITR, BIR, Business Sponsor	Users, Development Team	**This is mandatory for all projects.** Note: User Requirements at this stage must have enough detail to support the development of Functional Requirements.
Prepare Functional Requirements	Functional Requirements Document	Development Team	Support Organizations	**This deliverable is mandatory for all projects**. Note: Functional Requirements includes security, Automation Readiness, quality assurance, and data requirements.
Walkthrough Functional Requirements	Meeting Minutes	Development Team, Support Organizations	Business Sponsor, Infrastructure Services Division, Project QA Team	**This is mandatory for all projects**.
Certify User and Functional Requirements	Requirements Certification Form with signature of Business Sponsor and Project Manager	Project Manager, Business Sponsor	Developers, Project CM Team, Support Organizations	**This is mandatory for all projects**.
Create Requirements Traceability Matrix (RTM)	Initial Requirements Traceability Matrix (RTM)	Development Team		**This deliverable is mandatory for all projects**.
Acquire Project Systems/Services	• Finalized Acquisition Plan(s), • Contract Award	Business Sponsor, Project Manager, Acquisition Organization, Infrastructure Services Division	Resource Management Group (RMG), Contracting Officer and Procurement Group, OFPD	If applicable.
Define Test Requirements	System Test Plan	Development Team, Testing Organization, Project QA Team	Business Sponsor	**This is mandatory for all projects**.

Stage 3 -- Project Definition Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Define Training Requirements	Training Requirements	Training Organization, Business Sponsor	Development Team	
Conduct Support Organization Interface Meeting(s)	Meeting Minutes	Project Manager	Support Organizations, ISD Support Teams	**Note:** Include all potential supporting and affected organizations.
Prepare Required Security Deliverables	• Security Plan, • Security Risk Assessment, • Security Test Plan, • Disaster Recovery Plan, • Contingency Plan, • Trusted Facilities Manual	Development Team, Project Security Team	System Design Security Officer (SDSO)	**These deliverables are mandatory for all projects.**
Prepare Support Area Plans	• Data Management Plan, • Quality Assurance Plan, • Configuration Management Plan, • Implementation Plan, • Deployment Plan, • Project Risk Management Plan and Project Risks Database	Development Team, Project QA Team, Project CM Team, Project Implementation Team, Project Management Team	Data Management Organization, Training Organization, OIT CM Organization, Support Organizations, Testing Organization, OIT QA Organization	**These deliverables are mandatory for all projects.**

Stage 3 -- Project Definition Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Negotiate and Document ISAs	Interconnection Security Agreement(s) (ISA)	Project Manager, Senior Management, External Stakeholders	OIT Security Organization	If applicable. Each ISA must have a previously approved MOU. Signatories for final ISA are the CIO and equivalent level in the non-Customs organization(s).
Perform Definition Phase Completion Review	• Definition Phase Completion Review Package, • Meeting Minutes, Agenda, Action Items, • Project Manager Sign-off	Project Manager, Senior Management, Business Sponsor	Development Team, Support Organizations, Project QA Team	This may be accomplished by an informal or formal review as appropriate to the project

Stage 4 – System Design

Stage 4 -- System Design Entry Criteria

- Requirements Certification is completed

AND

- Project Manager signs-off on Definition Phase Completion

Stage 4 -- System Design Inputs

- User and Functional Requirements Documents
- Requirements Certification Form
- Initial Requirements Traceability Matrix (RTM)
  - Training Requirements Document
- Final Configuration Management (CM) Plan
- Final Quality Assurance (QA) Plan
- Security Documents
- Security Plan
- Security Risk Assessment
- Draft Disaster Recovery Plan
- Draft Contingency Plan
- Draft Security Test Plan
- Draft Trusted Facility Manual
- Interconnection Security Agreements, if applicable
  - Other Draft Support Plans
    - System Test Plan
    - Data Management Plan
    - Implementation Plan
    - Deployment Plan
    - Project Risk Management Plan and Project Risks Database

Stage 4 -- System Design Exit Criteria

- Critical Design Review is completed. The System Design is accepted by the Business Sponsor and all affected stakeholders.

AND

- All Design documents are baselined

Stage 4 -- System Design Outputs

- Draft Training Plan
- Memo of User Acceptance of Design
- Baselined
  - Project Plan, CM Plan, QA Plan
  - Data Management Plan (including Data Model and DDL)
  - System Design Documents
  - Security Design Document

Stage 4 -- System Design Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Create Preliminary System Design	System and Security Design Documents	Development Team, Project Security Team	BITR and/or BIR, Users, ISD Support Teams	**Reference:** *Customs Data Object Definition and Naming Standards*
Conduct Peer Reviews and Preliminary Design Reviews	Minutes and memos documenting the reviews	Development Team	Project Manager, Project QA Team, Support Organizations	**This is mandatory for all projects.**
Create Detailed System Design	System and Security Design Documents	Development Team, Project Security Team, Data Management Organization	BITR, BIR, Users, ISD Support Teams	**This deliverable is mandatory for all projects.** **Notes:** • This task includes developing the logical and physical database designs. • Also see the *Automation Standards Definition Document*.

Stage 4 -- System Design Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Conduct Peer Reviews and Detailed Design Reviews	Minutes and memos documenting the reviews	Development Team, Data Management Organization	Project Manager, Project QA Team, Support Organizations	**This is mandatory for all projects.**
Create Training Plan	Draft Training Plan	Training Organization	Business Sponsor, Project Manager	
Conduct Critical Design Review (CDR)	• Critical Design Review (CDR) Package, • Agenda, Meeting Minutes, Action Items, • Memo of User Acceptance of Design	Project Manager, Development Team, Business Sponsor	Support Organizations, Project QA Team, BIR, BITR	**This review is mandatory for all projects.** **Note:** Critical Design Review package includes updated RTM and Automation Readiness information.
Baseline Design	Baselined • System Design Documents, • Security Design Document, • Data Management Plan, • Project CM Plan, • Project QA Plan	Project Manager, Development Team, Project CM Team, Business Sponsor	Support Organizations, Data Management Organization, Project QA Team	**This is mandatory for all projects.** **Note:** The Data Management Plan at this stage includes Data Model(s), Logical and Physical Database Design(s), and the required Data Definition Language [DDL] references
Conduct Project Review with Senior Management/DD	• Meeting Agenda and Minutes, • Baselined Project Plan	Project Manager, Business Sponsor	Senior Management, Division Director	

Stage 5 – Construction

Stage 5 -- Construction Entry Criteria

- Critical Design Review is completed. The System Design is accepted by the Business Sponsor and all affected stakeholders.

AND

- All Design documents are baselined

Stage 5 -- Construction Inputs

- Draft Training Plan
- Memo of User Acceptance of Design
- Baselined
  - Project Plan, CM Plan, QA Plan
  - Data Management Plan (including Data Model and DDL)
  - System and Security Design Documents

Stage 5 -- Construction Exit Criteria

- The Test Readiness Review is completed, signifying that the Work Products are ready for independent testing.

AND

- Work Products turned over for testing are baselined

Stage 5 -- Construction Outputs

- Source Code
- Source Code documentation (e.g., flowcharts, comments)
- Infrastructure
- Infrastructure documentation
- Databases
- Machine Executable Code
- Developers' Test Cases/Scenarios and Results
- Draft Documents
  - User Documentation and Training Materials Outlines
  - Security Features User's Guide
  - System Acceptance Test Plan
  - Operations Manuals
- Final Documents
  - Project Plan
  - Infrastructure Plan
  - Data Management Plan
  - Requirements Traceability Matrix (RTM)
  - Training Plan
  - System Test Plan
  - Security Test Plan
  - Disaster Recovery Plan
  - Contingency Plan
  - Trusted Facility Manual
  - Project Risk Management Plan
  - System and Security Design Documents

Stage 5 -- Construction Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Establish Working Environments	Appropriate Development, Test, and Education Environments	Infrastructure Services Division, Development Team	Training Organization	
Develop/Code Software Package	Source Code	Development Team		**Note:** Includes Data Conversion Programs if required.
Construct Infrastructure	• Infrastructure • Databases	Project Manager, Infrastructure Services Division, Data Management Organization	Project Implementation Team, Development Team	**Note:** Infrastructure construction must account for projections made by capacity planning.
Create System Acceptance Plan	System Acceptance Test Plan	Testing Organization, Infrastructure Services Division	System Design Security Officer (SDSO)	**Note:** Includes Security Testing and initial Test Cases/Scenarios.
Document Work Products	Documentation for • Source Code (e.g., flow charts, comments), • Infrastructure	Development Team	Support Organizations	**This is mandatory for all projects.** Program documentation may include flowcharts, modification log updates, and inline comments in the source code.
Conduct Unit/ Integration Testing	• Updated System and Security Test Plans, • Developer's Test Cases/Scenarios, • Test Results	Development Team	Project Security Team, System Design Security Officer (SDSO), Training Organization	**This is mandatory for all projects.** **Note:** Test Cases/Scenarios include those for Security testing. Training is involved in integration testing for online Help, CBT, and training materials when available from within the application.

Stage 5 -- Construction Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Prepare Draft User Documentation and Training Material Outlines	• User Documentation and Training Material Outlines, • Security Features User's Guide	Training Organization, Project Security Team	Development Team	**This is mandatory for all projects.** **Note:** For some enhancements/ updates, it may not be necessary to produce these as new materials.
Prepare Operations Manual(s)	• Data Center Operations Manual, • Site Operations Manual, • System Administrator's Guide	Development Team	Infrastructure Services Division	**This is mandatory for all projects.** **Note:** For some enhancements/ updates, it may not be necessary to produce these as new materials. This also includes drafting updates to the Operations Run Manual System.
Conduct Work Product Walkthroughs	Minutes/Results of Reviews/Walkthroughs	Development Team	Project QA Team	
Conduct Peer Reviews	• Minutes of Reviews • Peer Review Results	Development Team	Project QA Team	**This is mandatory for all projects.**
Finalize Project Deliverables	• Project Plan, • Business Case, • RTM, • Project Risks Database, • Other documents as needed	Project Manager, Development Team, Project Management Team	Support Organizations, Project CM Team	See list of specific documents to be finalized in the Outputs above.
Prepare Turnover Package	Turnover Package (including all work products to date, whether draft or final)	Development Team	Testing Organization	This includes updated Implementation and Deployment Plans, if appropriate.

Stage 5 -- Construction Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Conduct Test Readiness Review (TRR)	• Meeting Agenda and Minutes, • Approved Turnover Package	Project Manager, Testing Organization, Data Management Organization, OIT Security Organization	Senior Management, Project QA Team, Infrastructure Services Division, OIT CM Organization	**This review is mandatory for all projects.**

Stage 6 – Acceptance

Stage 6 -- Acceptance Entry Criteria

- The Test Readiness Review is completed, signifying that the Work Products are ready for independent testing.

AND

- Work Products turned over for testing are baselined

Stage 6 -- Acceptance Inputs

- Source Code
- Source Code documentation (e.g., flowcharts, comments)
- Infrastructure
- Infrastructure documentation
- Databases
- Machine Executable Code
- Developers' Test Cases/Scenarios and Results
- Draft Documents
  - User Documentation and Training Materials Outlines
  - Security Features User's Guide
  - System Acceptance Test Plan
  - Operations Manuals
- Final Documents
  - Project Plan
  - Infrastructure Plan
  - Data Management Plan
  - Requirements Traceability Matrix (RTM)
  - Training Plan
  - System Test Plan
  - Security Test Plan
  - Disaster Recovery Plan
  - Contingency Plan
  - Trusted Facility Manual
  - Project Risk Management Plan
  - System and Security Design Documents

Stage 6 -- Acceptance Exit Criteria

- Production Readiness Review (PRR) is completed.
  OIT certifies that the system is tested and ready to access production data.

AND

- System is baselined

Stage 6 -- Acceptance Outputs

- System Acceptance
  - System Acceptance Test Plan
  - System Acceptance Test Cases/Scenarios and Results
  - System Acceptance Test Problem Reports
  - Testing Organization Recommendation
- User Acceptance
  - User Acceptance Test Cases/Scenarios and Results
  - User Acceptance Test Problem Reports
  - User Acceptance Test Sign-off memo
- Approved User Documentation and Training Materials
- Security Certification Package
- Security Accreditation Package
- Production-Ready Code
- Production-Ready Infrastructure
- Final Documents
  - Implementation Plan
  - Deployment Plan
  - Operations Manuals
  - Security Plan
  - Security Risk Assessment
  - Security Features User's Guide
- Baselined System and Documentation
- Production Readiness Review Sign-off Form
- SAT to Production Move Request
- Draft Production Notice

Stage 6 -- Acceptance Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Prepare/Update Test Cases	Updated Test Cases/ Scenarios	Testing Organization, Infrastructure Services Division		
Migrate Software to Test Environment	Software Moved to Test Environment	OIT CM Organization	Project CM Team, Testing Organization	
Finalize System Acceptance Test Plan	System Acceptance Test Plan	Testing Organization, Infrastructure Services Division	System Design Security Officer (SDSO)	**Note:** Includes Security Acceptance Test information and Automation Readiness test information.
Conduct System Acceptance Test (SAT)	System Acceptance Test Problem Reports	Testing Organization, Infrastructure Services Division		**This is mandatory for all systems.**
Resolve Test Problems	Production-Ready Code and Infrastructure	Development Team, Project CM Team	Testing Organization, OIT CM Organization	
Prepare Production-Ready Environment	Production-Ready Infrastructure	Infrastructure Services Division, Development Team	Project Implementation Team	
Prepare Testing Organization's SAT Reports	• SAT Test Results, • Testing Organization Recommendation	Testing Organization, Infrastructure Services Division		
Security Certification	Security Certification Package	Computer Security Officer (CSO)	Project Security Team, OIT Security Organization	**This is mandatory for all systems.** **Note:** Security Certification is signed by the Information Systems Security Manager (ISSM).
Develop/Update Initial User Documentation and Training Materials	• User Documentation, • Training Materials	Training Organization	Development Team, Testing Organization	

Stage 6 -- Acceptance Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
User Acceptance Testing	• User Acceptance Test Cases/Scenarios and Results, • Test Problem Reports, • Approved User Documentation and Training Materials, • User Acceptance Test Sign-off memo	Business Sponsor, Users, Testing Organization	Training Organization	**This is mandatory for all projects.** **Note:** User Acceptance Test signoff is required regardless of who actually performs the testing activities.
Conduct Transition/ Deployment Meeting	• Deployment Plan and Package, • Meeting Agenda and Minutes, • Action Items	Development Team, Project Implementation Team	Support Organizations, Business Sponsor, ISD Support Teams	
Finalize Project Deliverables	• Operations Manual(s), • Implementation Plan, • Deployment Plan, • Security Plan, • Security Risk Assessment, • Security Features User's Guide	Development Team, Project Security Team, Project Implementation Team	Project Management Team, ISD Support Teams, Training Organization	
Submit Security Accreditation Package	Security Accreditation Package	Computer Security Officer (CSO), Business Sponsor	Development Team, Project Security Team, OIT Security Organization	**This is mandatory for all systems.** **Note:** Security Accreditation is approved by the Designated Approval Authority (DAA).
Prepare Production Move Request	• Production Move Request, • Draft Production Notice	Project Manager	Project CM Team, OIT CM Organization	

Stage 6 -- Acceptance Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Baseline the System	• Baselined System, • Baselined Documentation	OIT CM Organization, Project Manager	Project CM Team, Support Organizations	**Note:** If the Operational Readiness Stage is very short, this baseline may be identical to the Production Baseline created in Stage 7.
Prepare Production Readiness Review (PRR) Package	Production Readiness Review Package (including all work products to date, whether draft or final)	Project Manager	Project Team, User	
Conduct Production Readiness Review (PRR)	• PRR Agenda and Minutes, • Action Items List, • PRR Signoffs	Project Manager, Senior Management, Business Sponsor, Sponsoring (PM's) Division Director, Infrastructure Services Division Director, Supporting Division Directors	Infrastructure Services Division, Testing Organization, Training Organization, Development Team, Project QA Team, OIT Security Organization, Other Supporting Organizations	**This review is mandatory for all projects.** **Note:** All affected stakeholders must be included in agreement on the readiness of the system.

Stage 7 -- Operational Readiness

Stage 7 -- Operational Readiness Entry Criteria

- Production Readiness Review (PRR) is completed. OIT certifies that the system is tested and ready to access production data.

AND

- System is baselined

Stage 7 -- Operational Readiness Inputs

- System Acceptance
  - System Acceptance Test Plan
  - System Acceptance Test Cases/Scenarios and Results
  - System Acceptance Test Problem Reports
  - Testing Organization Recommendation
- User Acceptance
  - User Acceptance Test Cases/Scenarios and Results
  - User Acceptance Test Problem Reports
  - User Acceptance Test Sign-off memo
- Approved User Documentation and Training Materials
- Security Certification Package
- Security Accreditation Package
- Production-Ready Code
- Production-Ready Infrastructure
- Final Documents
  - Implementation Plan
  - Deployment Plan
  - Operations Manuals
  - Security Plan
  - Security Risk Assessment
  - Security Features User's Guide
- Baselined System and Documentation
- Production Readiness Review Sign-off Form
- SAT to Production Move Request
- Draft Production Notice

Stage 7 -- Operational Readiness Exit Criteria

- The Operational Readiness Review (ORR) is completed, signifying that the Business Sponsor has accepted the system to become operational.

AND

- System is baselined

Stage 7 -- Operational Readiness Outputs

- Project Lessons Learned documents
- Prepared Operational Sites
- Prepared Support Infrastructure
- Converted Data
- System Moved to Production and Education Environments
- Databases Moved to Production and Education Environments
  - Final User Documentation and Training Materials
  - Finalized System Documentation
  - Training Schedule (includes Operational Sites)
  - If Applicable
    - Pilot Test Report
    - Parallel Operations Evaluation Report
    - Pilot Training Class
- Operation Readiness Review Sign-off Form
- Production Baseline of System and Documentation
- Production Notice
- Updated Change Control Database

Stage 7 -- Operational Readiness Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Prepare for Installation	• Prepared Support Infrastructure, • Prepared Operational Site(s)	Project Implementation Team	Infrastructure Services Division	
Convert Data	Converted Data	Data Management Organization, OIT CM Organization	Development Team	
Move to Production Environment	• System Moved to Production and Education Environments, • Databases Moved to Production and Education Environments	OIT CM Organization, Data Management Organization, ISD Support Teams	Project CM Team, Training Organization	
Perform Pilot Testing	Pilot Test Report(s)	Development Team, Business Sponsor, Project Implementation Team	Infrastructure Services Division, Project QA Team	If applicable. **Note:** Pilot testing also includes beta tests, prototype tests, and field tests
Perform Parallel Operations	Parallel Operations Evaluation Report	Development Team, Business Sponsor, Project Implementation Team	Infrastructure Services Division, Project QA Team	If applicable.
Finalize Training Schedule	Training Schedule (includes Operational Sites)	Training Organization	Business Sponsor	
Conduct Training Pilot	Pilot Training Class	Training Organization		If applicable.
Finalize and Produce Training Materials	Finalized User Documentation and Training Materials	Training Organization	Business Sponsor	

Stage 7 -- Operational Readiness Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Finalize Project Plans and Documentation	Finalized plans and documentation	Project Manager	Development Team, Support Organizations	**Note:** Includes Final Operations Manual(s), System Administrator's Guide, Business System Overview, Data Dictionary, etc.
Prepare/Document Lessons Learned	Project Lessons Learned documents	Project Team, Support Organizations, Evaluation Organization	Business Sponsor, ISD Support Teams	**This deliverable is mandatory for all projects.**
Create Production Baseline	• Baselined System, • Baselined Documentation	OIT CM Organization, Project Manager	Project CM Team, Support Organizations	**This is mandatory for all projects.**
Conduct Operational Readiness Review (ORR)	• ORR Agenda and Minutes, • Action Items, • ORR Signoffs	Project Manager, Senior Management, Business Sponsor, Sponsoring (PM's) Division Director, Infrastructure Services Division Director, Supporting Division Directors	Support Organizations, Development Team, Project QA Team, OIT QA Organization	**This review is mandatory for all projects.** **Note:** Small legacy mainframe projects may hold this review at the same time as the PRR.
Release Production Notice	• Production Notice • Updated Change Control Database	Project Manager, OIT CM Organization	Business Sponsor	

Stage 8 – Operations

Stage 8 -- Operations Entry Criteria

- The Operational Readiness Review (ORR) is completed, signifying that the Business Sponsor has accepted the system to become operational.

AND

- System is baselined

Stage 8 -- Operations Inputs

- Project Lessons Learned documents
- Prepared Operational Sites
- Prepared Support Infrastructure
- Converted Data
- System Moved to Production and Education Environments
- Databases Moved to Production and Education Environments
  - Final User Documentation and Training Materials
  - Finalized System Documentation
  - Training Schedule for Operational Sites
  - If Applicable
    - Pilot Test Report
    - Parallel Operations Report
    - Pilot Training Class
  - Operation Readiness Review Signoff Form
  - Production Baseline of System and Documentation
  - Production Notice
- Updated Change Control Database

Stage 8 -- Operations Exit Criteria

- A management decision is made to retire or terminate a system.

Stage 8 -- Operations Outputs

- System Being Used in the Field
- Capacity and Performance Monitoring Reports
- Operational Problem Reports
- Help Desk Reports
- Work Requests and System Change Requests
- Upgraded/Replaced System Software/Hardware/Firmware
- Post Implementation Review (PIR) Reports
- Evaluation Reports and Audits
- Performance Measures for System Performance and System Contribution to Customs Mission
- Trained Users
- Updated User Documentation and Training Materials
- Updated Security Documentation
  - Contingency Test Plans and Reports
  - Operational Lessons Learned documents
- Security Reassessments, Re-Certification, and Re-Accreditation

Stage 8 -- Operations Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Activate the System	• System Outputs as Designed, • Improved Business Processes	Users	Infrastructure Services Division	
Train Users	Trained Users	Training Organization	Business Sponsor	
Roll-out to Additional Sites		Business Sponsor, Project Manager, Project Implementation Team	Development Team, Infrastructure Services Division, Support Organizations, Training Organization	If applicable

Stage 8 -- Operations Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Monitor Performance	Capacity and Performance Monitoring Reports	Infrastructure Services Division	Software Development Division	
Ensure Continuous Operations	• Operational Problem Reports, • Work Requests, • Change Requests, • Archived Data	Infrastructure Services Division	Software Development Division	
Manage Production Problem Reports	• Change Requests, • Operational Problem Reports, • Help Desk Reports, • Change Impact Analyses, • CCB Agendas and Minutes	Help Desk Organization	Infrastructure Services Division	
Analyze Problem Reports	• Work Requests, • Change Requests	Infrastructure Services Division	Software Development Division	
Capacity Planning and Replanning	Evaluation Reports	Capacity Planning Organization	Infrastructure Services Division	
Evaluate and Upgrade Systems Software/COTS	Upgraded/Replaced System Software	Infrastructure Services Division	Architecture Organization, Software Development Division	
Analyze and Install Hardware/Firmware Upgrades	Upgraded/Replaced Hardware / Firmware	Infrastructure Services Division	Architecture Organization	
Document Operational Lessons Learned	Operational Lessons Learned documents	Software Development Division, Business Sponsor, Infrastructure Services Division		

Stage 8 -- Operations Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	

Post-Implementation Evaluations	• Post Implementation Review (PIR) Reports,
	• Evaluation Reports and Audits,
	• Performance Measures for
	  ▸ System Performance
	  ▸ Contribution to Customs Mission
		Evaluation Organization,
		OIT CM Organization,
		Business Sponsor
			Planning Organization,
			Users
				This is mandatory for all projects.

Update User Documentation and Training Materials	Updated User Documentation and Training Materials	Training Organization	Business Sponsor	
Update Required Security Documentation	• Security Plan, • Security Risk Assessment, • Security Features User's Guide, • Trusted Facility Manual, • Disaster Recovery Plan, • Contingency Plan	Business Sponsor	OIT Security Organization, BIR, BITR	**These deliverables are mandatory for all systems.**
Evaluate Disaster Recovery and Contingency Plans	Contingency Test Plans and Reports	Business Sponsor, Infrastructure Services Division	OIT Security Organization, BIR, BITR	**These deliverables are mandatory for all systems.**

Stage 8 -- Operations Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Perform Security Re-Certification and Re-Accreditation	Re-Certification and Re-Accreditation Package	Business Sponsor, Computer Security Officer (CSO)	OIT Security Organization, BITR, BIR	**This is mandatory for all systems. Note:** Security Certification is approved by the ISSM; Security Accreditation is approved by the DAA.

Stage 9 -- Retirement

Stage 9 -- Retirement Entry Criteria

- A management decision is made to retire or terminate a system

.

Stage 9 -- Retirement Inputs

- A system that no longer meets the users needs
- All project and system documentation for the system to be retired/terminated

Stage 9 -- Retirement Exit Criteria

- System is removed from operation

AND

- Appropriate data archiving is complete

Stage 9 -- Retirement Outputs

- Federal Register Notice if required
- Notification of Intent to Retire
- Removal Plans as required
  - Retirement Project Plan
  - Security Conversion Plan
  - Data Conservation/Conversion Plan
  - Infrastructure Retirement/Conversion Plan
  - System Cut-Over Plan
- Archived data from the retired system if appropriate
- Archived source code and machine code
- Archived system and project documentation
- Updated Archive Documentation
  - Notification of Retirement
- Retirement Process Lessons Learned document

Stage 9 -- Retirement				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Perform Impact Analysis	Decision to Retire	Business Sponsor, Stakeholders		If a system is being replaced, this will be part of the new system's CBA.

Stage 9 -- Retirement				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Create System Retirement Team and Retirement Project Plan	• Retirement Project Team, • Retirement Project Plan	Business Sponsor, Senior Management, Project Manager	Support Organizations	**Note:** The Project Plan for a system to be retired with no replacement includes activities from Stages 1, 2, 9, and Project Management Support. If a replacement system is being developed, these Stage 9 tasks may be incorporated within a full life cycle Project Plan for the new system.
Notification of Intent to Retire System	• Federal Register Notice, • Notices to Internal and External Stakeholders	Business Sponsor	Office of the Chief Counsel, Support Organizations	Notice should include projected date, what will replace it, etc.
Create Security Conversion Plan	Security Conversion Plan	Project Manager	OIT Security Organization	If the system is being replaced, this will be part of the new system's Security Plan.
Develop Data Conservation/ Conversion Plan	Data Conservation/ Conversion Plan	Project Manager	Data Management Organization, Support Organizations	If the system is being replaced, this will be part of the new system's Data Management Plan.
Define/Document System Cut-Over Plan	System Cut-Over Plan	Project Manager	Infrastructure Services Division	If the system is being replaced, this will be part of the new system's Implementation and Deployment Plan.
Define/Document Infrastructure Retirement/ Conversion Plan	Infrastructure Retirement/ Conversion Plan	Project Manager	Infrastructure Services Division	If the system is being replaced, this will be part of the new system's Infrastructure Plan.
Review and Verify Removal Plans		BITR, Sponsoring (PM's) Division Director, Infrastructure Services Division Director	Business Sponsor	**This is mandatory for all retirement projects.**

Stage 9 -- Retirement				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Prepare and Submit Program Move Request		Project Manager	Project CM Team	
Archive Programs and Data	• Archived Machine Code, • Archived Source Code, • Archived Data	OIT CM Organization	Infrastructure Services Division	**This is mandatory for all retirement projects.** **Note:** Data is required to be archived only if the system is not replaced; otherwise data will be converted for use in the new system.
Archive System and Project Documentation	• Archived System Documentation, • Archived Project Documentation	Project Manager, Business Sponsor	Project CM Team, OIT CM Organization	**Note:** These may be in electronic form. System and Project documentation includes User and Functional Requirements, Design Documentation, Lessons Learned, etc.
Remove Programs/ Infrastructure		OIT CM Organization, Infrastructure Services Division		
Update Archive Documentation to Show Archive Locations	Updated Archive Documentation	OIT CM Organization		
Notification of Completion	• Federal Register Notice, • Notices to Internal and External Stakeholders	Business Sponsor	Office of the Chief Counsel, Support Organizations	If applicable.
Document Retirement Process Lessons Learned	Retirement Process Lessons Learned documents	Project Manager, Business Sponsor	Infrastructure Services Division	

Project Management Support

(Ongoing Throughout the Entire Life Cycle)

Project Management Support Entry Criteria

- These tasks/activities occur during more than one stage throughout the life of the project.
- These tasks/activities should begin as soon as possible in Stage 1, but no later than the end of Stage 1 when funding is approved.

Project Management Support Inputs

- Customs policies, procedures, and standards

Project Management Support Exit Criteria

- System is removed from operation

AND

- Appropriate data archiving is complete

Project Management Support Outputs

- Agendas, Minutes, Action Item Lists
- Updated Project Documentation
- Budgets, Schedules, Estimates, and Agreements
- Contractor Evaluation Reports
- Quality Assurance Reports
- Risk data and Risk Mitigation Plans
- SDLC/Process/Architectural Compliance Reports
- Change Requests and Impact Analyses
- CM activities, status reports, audit reports, and baselines
- Metrics data, analyses, and reports

Project Management Support Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Perform Project Planning, Costing and Budgeting Activities	• Project Plans, • Budgets, • Schedules, • Estimates	Project Manager, Business Sponsor	Affected Support Organizations, Project Management Team	**This activity is mandatory for all projects.**
Prepare/Conduct Project Status Meetings	• Agenda, • Minutes, • Action Item Lists, • Updated Risk Lists	Project Manager, Development Team	Support Organizations, Project Management Team	**This activity is mandatory for all projects.**
Prepare/Conduct Senior Management Reviews	• Agenda, • Minutes, • Action Item Lists, • Updated Risk Lists	Project Manager, Senior Management	Business Sponsor, Division Director	**This activity is mandatory for all projects.**
Prepare/Conduct Peer Reviews	• Minutes (including time spent in preparation for and during review), • Defects found and Action Item Lists	Development Team, Team Leaders	Project Manager	**This activity is mandatory for all projects.**
Contractor/ Subcontractor Management	Evaluation Reports	Project Manager, Acquisition Organization	Project Management Team	Mandatory if the project includes acquisition of products and/or services.
Conduct SDLC and Architectural Compliance Reviews	• SDLC Compliance Report • Architectural Compliance Report	Evaluation Organization	Development Team, Support Organizations, Architectural Organization	**This activity is mandatory for all projects**

Project Management Support Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Perform Requirements Management	• Change Requests, • Impact Analyses, • CCB Meeting Agendas and Minutes, • Updated Project Plans, • Reports to Management	Project Manager, Business Sponsor, Project Change Control Board (CCB)	Users, Development Team, Infrastructure Services Division, Support Organizations, Project Management Team	**This activity is mandatory for all projects.**
Collect, Analyze, and Report Data on Actual Project Management Performance (i.e., Project Tracking)	• Raw Data Reports, • Data Analyses, • Reports to Senior Management	Project Manager, Program Monitoring Group (PMG), OIT QA Organization, Infrastructure Services Division	Project Management Team, Development Team, Project Implementation Team, Project QA Team, Support Organizations	**This activity is mandatory for all projects.** **Note:** For specific data required, see Policy on Metrics in Chapter 2, Section 2.4.4
Negotiate, Update and Rebaseline Project Plans, Agreements, and Documents	• Updated Agreements, Plans • Rebaselined Project Plans and Documents	Project Manager, Business Sponsor, Support Organizations	Project Management Team, Acquisition Organization, Project QA Team, Project CM Team	**This activity is mandatory for all projects. In particular, updating the project plans and documentation occurs at <u>every</u> stage in the life cycle.**
Perform Quality Assurance	QA Audit Reports	Project QA Team, Project Manager, OIT QA Organization	Process Groups, PATs, SLC Organization, Evaluation Organization	**This activity is mandatory for all projects.**
Perform Configuration Management	• Configuration Audit Reports, • Status Reports, • Baselines	Development Team, Project CM Team	OIT CM Organization, Project CCB	**This activity is mandatory for all projects.**

Project Management Support Tasks/Activities				
Task/Activity	**Deliverable(s)/ Outputs**	**Responsibilities**		**References, Resources, Notes and Comments**
		Primary	**Support**	
Perform Risk Management	• Project Risks Database, • Risk Mitigation Plans	Project Management Team, Project Manager	Project Team, Support Organizations	**This activity is mandatory for all projects.**
Ongoing Project Oversight		IRB, ITC, Division Director	Investment Organization, Evaluation Organization, PMG, Project Manager, Senior Management	
Prepare for and Respond to External Oversight Requests	Reports as required	Project Manager, Project Management Team, Senior Management	OIT QA Organization	

Chapter 5
Waterfall-Based Development Models

5.1 Introduction

This chapter presents the Waterfall-based life cycles that may be used at Customs to develop software. The first model presented is the Traditional Waterfall Life Cycle. To date, it is the model that has been most commonly used at Customs.

There are five variants of the Waterfall life cycle approved for use at Customs. These are:

- Traditional Waterfall Life Cycle
- Small Project, Maintenance, and Enhancements Life Cycle
- Off-the-Shelf (COTS) Application Life Cycle
- Infrastructure Projects Life Cycle
- Information Engineering (IE) Life Cycle

Chapter 6 presents alternative development models to those shown in this chapter. No matter which life cycle model is chosen, projects must account for all of the activities, reviews, and deliverables defined in Chapter 4, Customs Standard Life Cycle, and receive validation by OIT's Planning Group and approval of Senior Management.

5.2 When to Use Which Life Cycle

The choice of life cycle is the joint responsibility of the Project Manager, the Business Sponsor, and Senior Management. The choice should be based on the project's cost, schedule, and type of product being produced. Figure 5.1 presents a high-level decision tree to assist in this choice.

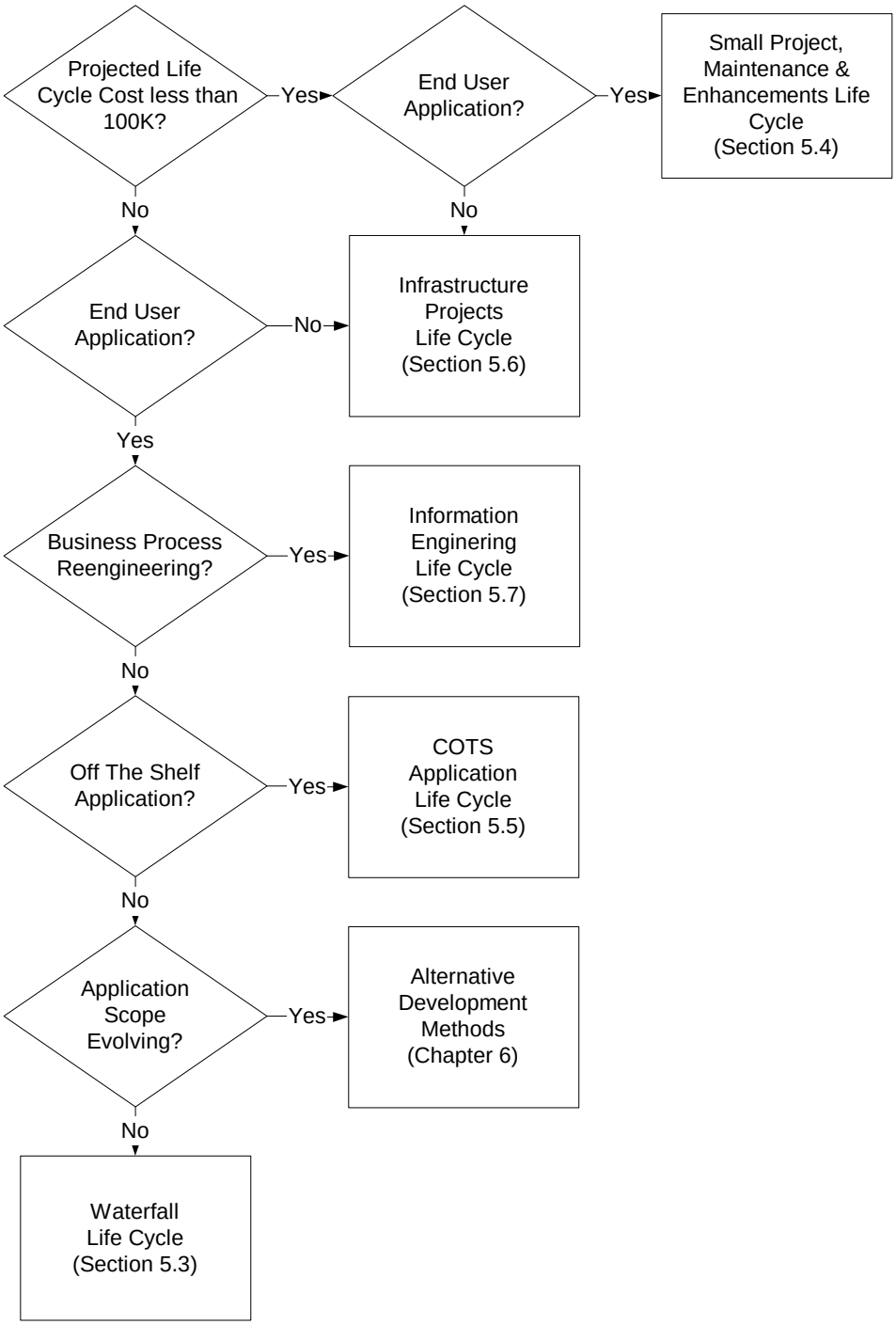


Figure 5.1, Decision Tree for Life Cycle Selection

5.3 Traditional Waterfall Life Cycle

The "traditional waterfall" life cycle is one of the oldest models known for developing an automated data system. It owes much of its underlying philosophy to manufacturing. The waterfall model was given its name because the effort cascades down a single line of steps that many view as the essential components of software development. (See Figure 5.2)

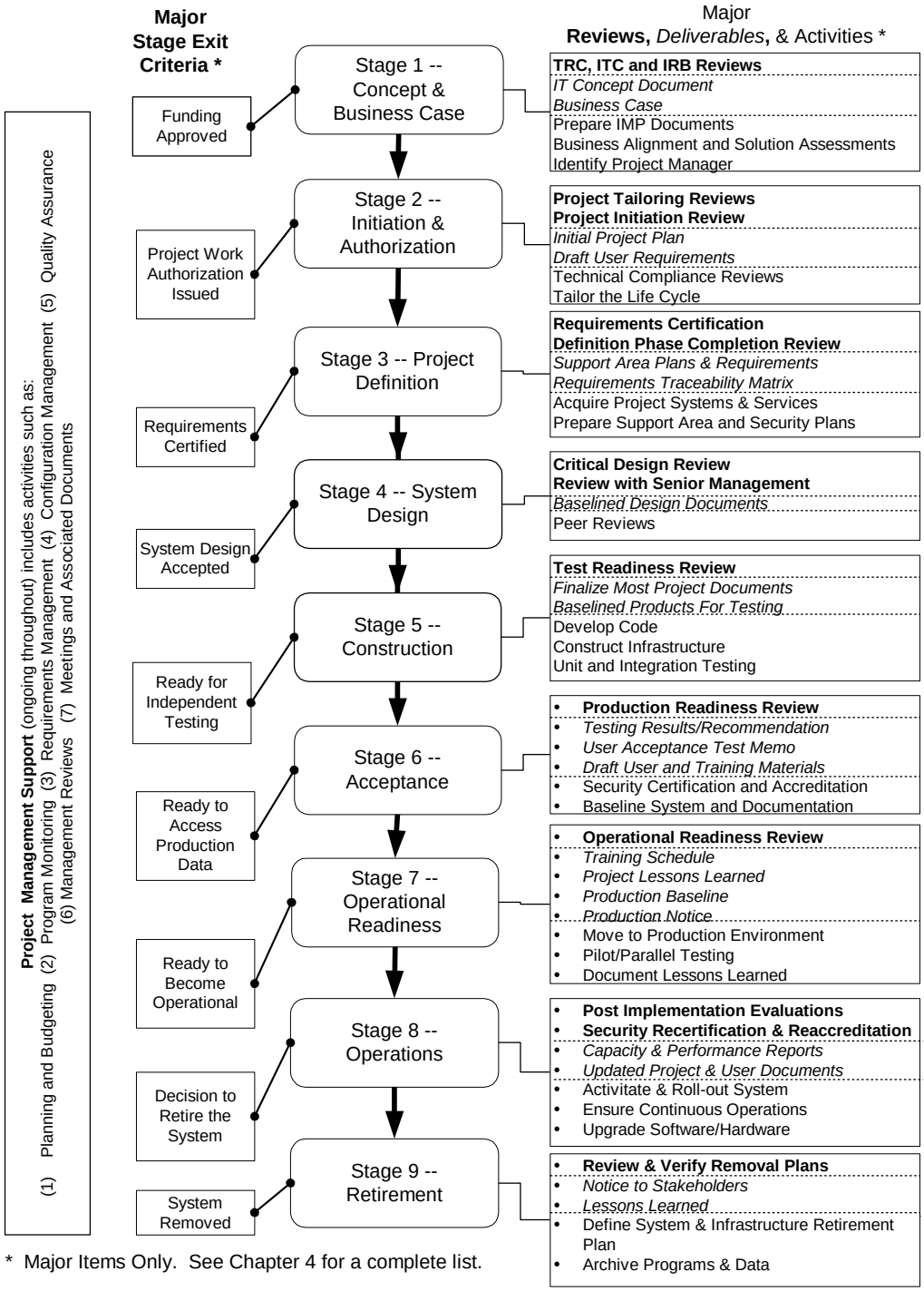


Figure 5.2, Waterfall Life Cycle

Customs encourages the use of feedback loops with this life cycle model. For example, design activities may cause changes in requirements definitions and plans; construction activities may cause changes to design and requirements, etc. However, it is critical that the planning and description documents from prior stages be updated to incorporate such changes at each stage.

5.3.1 Advantages and Disadvantages

Advantages

Versatility: The Waterfall model has been used to produce almost every kind of software system known. It is easily adapted to any type of system, from a totally-batch system to systems that are almost exclusively transaction driven.

Top Down: The Waterfall model is a top down approach that subdivides tasks in order to identify milestones in the development process.

Management Approval: Managers like the waterfall model because:

- It is orderly and predictable;
- It gives them a clear picture of where each project is at a given point in time; and
- The boundaries of each task are clear and unambiguous.

Specialization: Because each stage is self-contained, it allows individuals to specialize in a specific stage. This leads to horizontal integration where an individual performs a specified function on a project and then moves to another project once the function is completed.

Completeness: If all the deliverables/outputs of a stage are complete, then the stage is completed.

Documentation: The system is completely and properly documented. A well documented system supports easier modifications and upgrades as user requirements change over time.

Disadvantages

Document-Driven: Because there may be different sub-teams performing each stage of the life cycle, documentation becomes a critical means of communication.

- This reliance on documentation can, at times, slow product development.
- Incomplete documentation makes it difficult for the next sub-team to perform their functions (including maintenance).

Requirements: It is often impossible for users to specify all their system requirements up front. This can result in costly and time-consuming re-work later in the life cycle unless baselining and change control are enforced.

Note: If this is a major concern, it may be more advantageous for the project to use an Alternative Development method described in Chapter 6.

Time: On large projects, it can take a very long time before any benefits are realized from the software project.

Project Size: A traditional waterfall life cycle model (where each stage must be completed before the next stage begins) can be very difficult to use on extremely large or extremely complex projects because it does not lend itself to decomposition.

Development Time: This approach does not lend itself to Rapid Development projects of less than 6 months.

5.4 Small Project, Maintenance, and Enhancements Life Cycle

This life cycle is intended for small software projects, software maintenance projects, and software enhancements to existing systems where the total life cycle cost is less than $100,000.

5.4.1 Differences from the Standard Life Cycle by Stage

Concept and Business Case:

- May be approved by the TRC and/or ITC (See Table 4-1, page 4-2).
- Business Case may be tailored or may not be required.

Initiation and Authorization: QA Plan, CM Plan, and Implementation Plan strategies may be combined into the Project Plan. Other documentation requirements may be met by updating existing system documentation.

Project Definition: User and Functional Requirements documentation may be combined. Requirements must be certified. Security documentation must be reviewed and revised as necessary.

System Design: Preliminary and detailed design documents may be combined.

Construction: A reduced set of deliverables may be tailored to fit the project. Regardless of what else may be tailored and combined, the modification log in the source code must be updated.

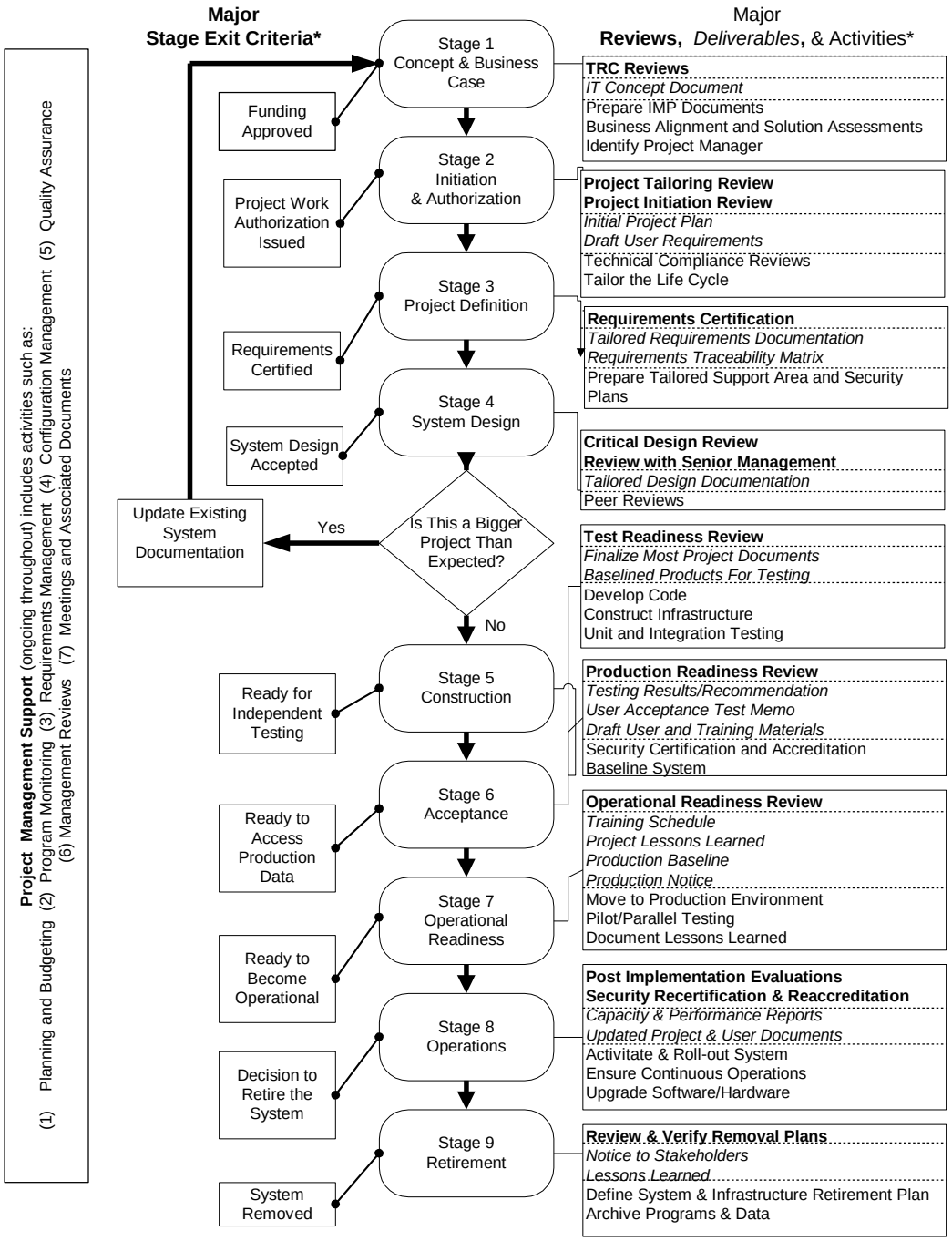
Acceptance: No Difference. Regression testing is important to ensure that no new problems occur because of the modifications.

Operational Readiness: No Major Differences. This stage must be tailored to fit the impact the change will have on the users.

Operations and Retirement: No Differences.

5.4.2 Advantages and Disadvantages

Advantages	Disadvantages
It is a tailored version of the Customs Standard Life Cycle. Many deliverables may be combined to facilitate documentation by small projects.	It cannot and must not be used for projects with a total cost of more than $100,000. If the project turns out to be larger than anticipated, it may be necessary to • Return to the approving body for authorization to continue; and • Prepare a more extensive set of project documents.



* Major Items Only. See Chapter 4 for a complete list.

Figure 5.3, Small Project, Maintenance, and Enhancements Life Cycle

5.5 Off-the-Shelf (COTS) Application Life Cycle

The Off-the-Shelf (COTS) life cycle model utilizes commercial software to satisfy all or part of the project's requirements. COTS covers everything from "install-and-go" software (such as Microsoft Office) to systems containing a complex mix of commercially-developed components and custom-developed components. This model also applies to Government-off-the-shelf (GOTS) applications.

A good COTS product has the following characteristics:

- Few (if any) defects
- Established and accepted by industry
- Adheres to government standards
- Published interfaces
- Can be tailored by the user (i.e., altering or setting parameters, adding templates and/or scripting without altering the source code.)

5.5.1 Differences from the Customs Standard Life Cycle by Stage

Projects must coordinate the COTS evaluation and selection of products with the Architecture Organization, OIT's Acquisition Organization, and the Office of Finance Procurement Division (OFPD). The following figure illustrates the high-level decision process used to find a product within the Customs Enterprise Architecture Technical Reference Model or to research how user needs will be met.

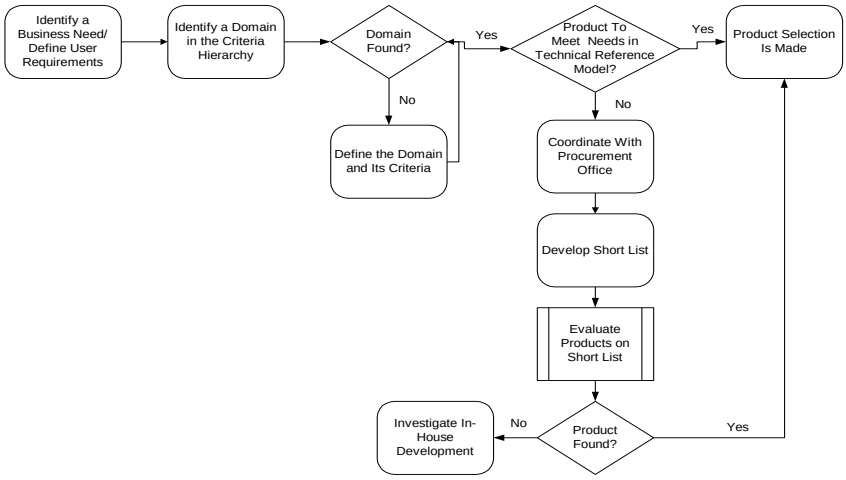


Figure 5.4, COTS Decision Process Diagram

Concept and Business Case:
- Make the decision to investigate COTS (Figure 5.4 above)
- Sufficiently define User Requirements for selection
- Document a product evaluation or selection process (in the case of a domain not currently in the Customs Enterprise Architecture)
- Document the rationale for the final product selection.

Initiation and Authorization:
- User Requirements must be finalized to serve as the basis for the SOW
- An Acquisition Plan must be developed in coordination with the Acquisition Organization and OFPD.

Project Definition: The project must develop:
- A Deployment Plan
- A Data Management Plan
- A Training Plan, including Training Requirements
- System and Security Test Plans
- Other Security deliverables as required

System Design: This stage is necessary only if any interface code is required.

Construction: Construction is necessary only if any interface code is required. The COTS application will be installed, tailored, and verified.

Acceptance: No Differences.

Operational Readiness: No Major Differences. This stage must be tailored to fit the impact the change will have on the users. Data conversions, site preparation, and pilot testing may be of particular concern when implementing COTS applications.

Operations and Retirement: No Differences.

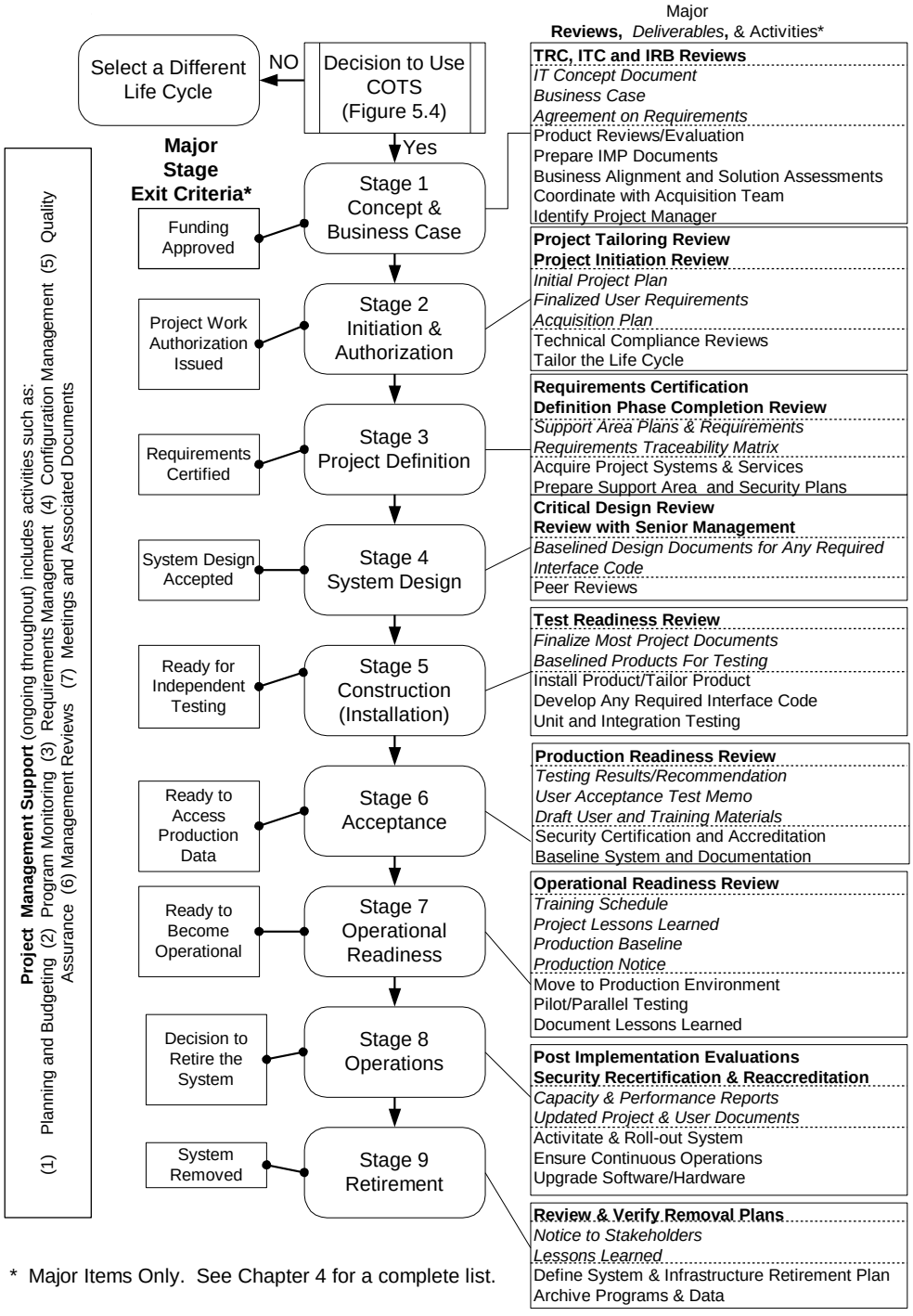


Figure 5.5, COTS Application Life Cycle

5.5.2 Advantages and Disadvantages

Advantages

Integration vs. Custom Coding: By using COTS, an organization can take advantage of using one underlying architecture as a system base. If this base remains stable, additional components can be integrated in a relatively short amount of time.

Proven Track Record: If other agencies and private sector organizations are using a component, it is possible to verify their experiences with the software, the vendor, and perhaps the integrator.

Compliance with The Information Technology Management Reform Act, OMB Circular A-120, OMB Circular A-127 and OMB Circular 109: This law and associated regulations require that government agencies avoid duplicating development efforts from other agencies and/or the private sector if at all possible.

Reduced Development Costs: The vendor has already borne the development costs and will recoup these costs through product licensing fees. The agency does not have to make as large an investment in development and quality testing.

Reduced Staffing: Staffing level reductions may be possible because the agency will not be involved in development. COTS allows scarce development resources to be used for unique, mission-specific applications and components.

Reduced Maintenance Cost: By using off-the-shelf software, the organization reduces the risk of out-year maintenance issues and cost, as these activities are often handled by the vendor.

Access to New Technologies: By using COTS, the organization gains access to the newest programming technologies through upgrades and new version releases by the vendor.

Disadvantages

Awareness: The project must be aware of what is available in the market place, management's motivation for or against a specific product, and technical issues arising from the interfaces of multiple components.

Relationships: In order to manage an Off-The-Shelf environment, the project must balance relationships between vendors, users, and technical personnel who support the selected products.

Change Management:

- Each time a component is changed, there may be unexpected and unpredictable results.
- Components in a distributed environment may be tailored or customized locally, leading to version control problems during upgrades.

Acquisition: In Statements of Work (SOWs) and Requests for Proposals (RFPs), it is difficult to specify component requirements to ensure that the agency obtains the appropriate functionality without violating procurement regulations.

Resource Management:

- There is a shortage of trained managers for COTS-based systems. Also, savings realized by reduced development staffing may be offset by the increased staffing needed for requirements definition.
- There is no accurate way to measure the platform or infrastructure resource consumption of specific sets of off-the-shelf components.

Process Dynamics:

- There are no universal standards for COTS
- The wait time for fixes and enhancements may become unacceptable.

5.6 Infrastructure Projects Life Cycle

The Customs Investment Management Process (IMP) requires that all initiatives (both software and infrastructure) be managed as investments using the principles of formal project management.

Infrastructure projects, like software projects, must formally document requirements, project plans, reviews, approvals, etc. This life cycle delineates that process whether or not "code" is involved.

5.6.1 Differences from the Standard Life Cycle by Stage

Concept and Business Case: No Differences

Initiation and Authorization: If the project is small, a section should be added to the Project Plan outlining the strategy to be used to procure the required equipment and/or software. For larger projects, it may be necessary to develop a separate Infrastructure, Acquisition, and/or Implementation Plan.

Project Definition: While the procurement activities are progressing, formal attention should be given to the training and security implications of the coming change. Also, initial test cases should be developed and documented.

System Design: The technical design may consist of hardware, network, software, or communications designs as required by the project. Whatever the form, the design must be documented, reviewed, and approved.

Construction: This stage begins with receipt and installation of the new software/ equipment in the appropriate initial test environment. If required, interface code shall be installed and any required data shall be loaded at the same time.

Acceptance: After the initial trials, the software/equipment shall be migrated through all the appropriately defined test environments. At each level, problem reports shall be analyzed and measures taken to mitigate any unforeseen impacts.

Operational Readiness: No Major Differences. This stage must be tailored to fit the impact the change will have on the users, including OIT stakeholders.

Operations and Retirement: No Differences

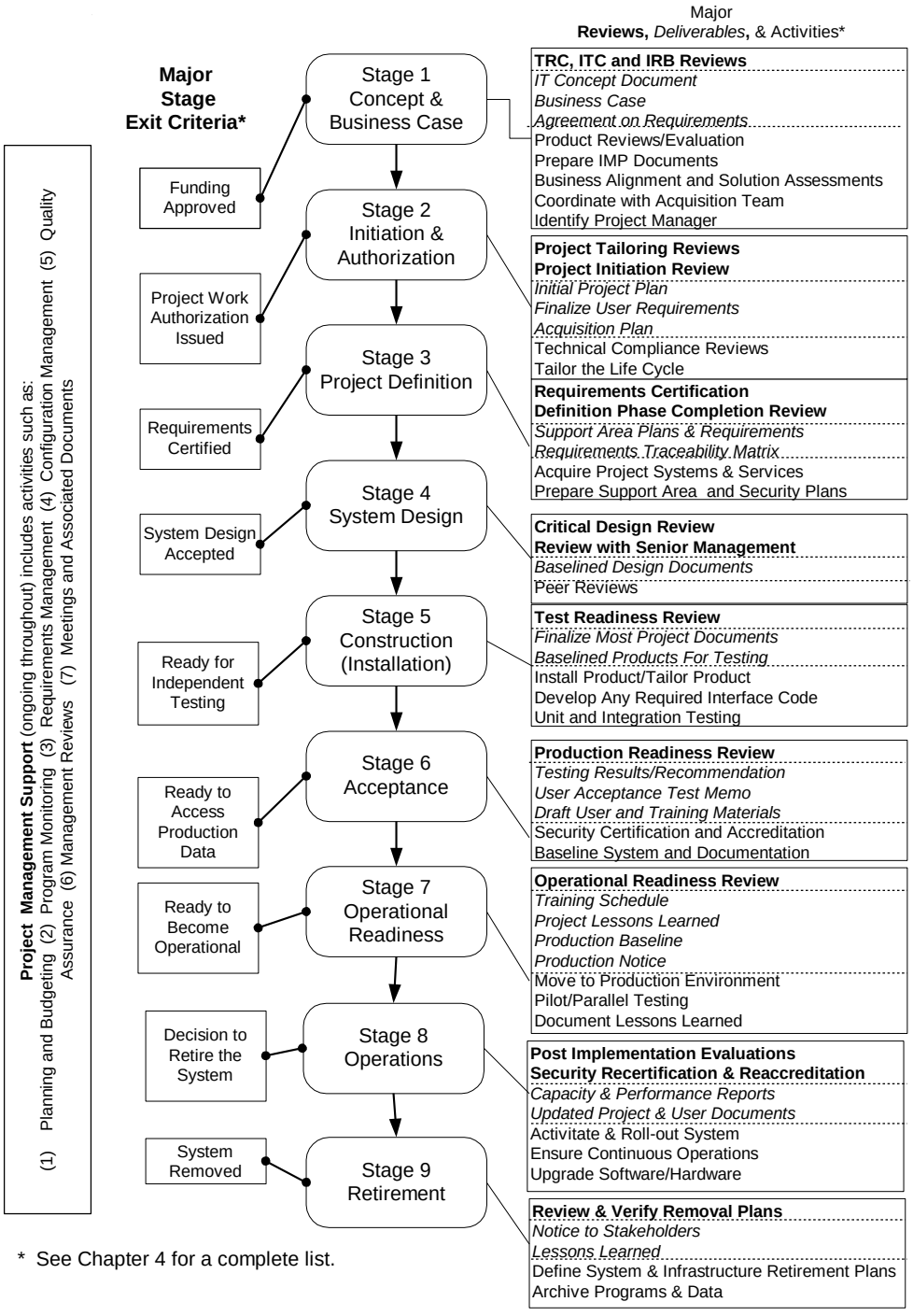


Figure 5.6, Infrastructure Projects Life Cycle

5.7 Information Engineering (IE) Life Cycle

Information Engineering (IE) is a comprehensive system development methodology using formal techniques for the planning, analysis, design, and construction of information systems on an enterprise-wide basis.

The basic premise of IE is that data is the center of modern business organizations. It begins by representing the data model needed to support the organization's strategic plan, objectives and future goals; and then defines the information system required to implement the plan.

The first three stages in this life cycle focus on defining and reengineering the business processes of the sponsoring organization rather than just IT systems. These stages are the responsibility of the Business Sponsor/Process Owner. When the sponsoring organization has completed its process re-engineering, it should identify specific IT alternatives to support the revised business processes. The project to implement the selected alternative are reviewed and approved through the IMP process; and the project selects a life cycle to be tailored to the project's needs.

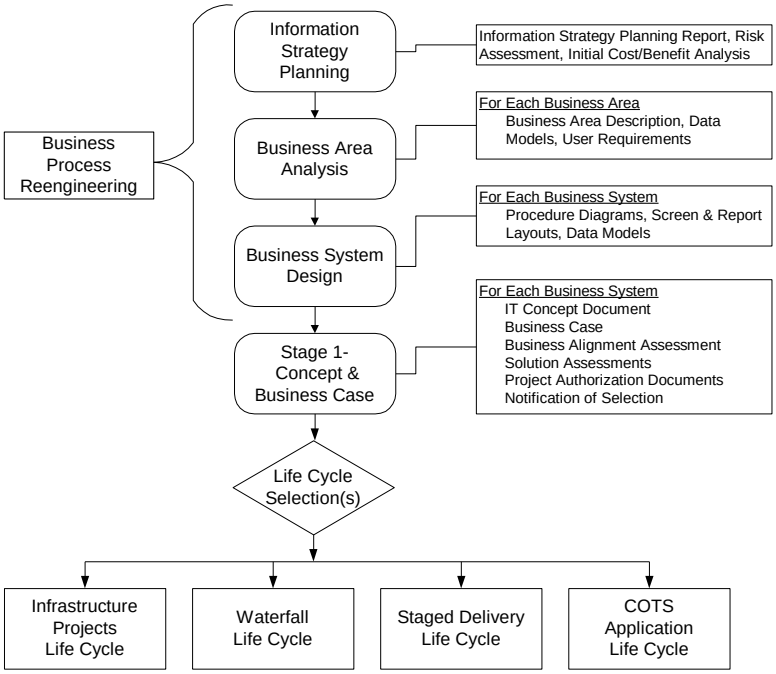


Figure 5.7, Information Engineering Life Cycle

5.7.1 Differences from the Standard Life Cycle by Stage

Information Strategy Planning (ISP): Planners gain a broad view of the information needs of the business. From this information, they create a blueprint for the future and subdivide the blueprint into smaller segments.

Business Area Analysis (BAA): Business Area Analysis (BAA) refines data and the information derived from the Information Strategy Plan at the strategic and at the tactical management levels of an organization. During a BAA, analysts examine a selected area of the business in detail. Designers use these results in succeeding stages to define the computerized systems needed to manage the enterprise's information resources.

Business System Design (BSD): During Business System Design (BSD), designers detail a business system within a particular business area. They consider how the user will interact with the business system, including its data and activities, without concerning themselves with any specific target computing environment.

Note: The three previous stages are not part of the Standard Life Cycle.

Concept and Business Case: Much of the information required during this stage can be met by documentation prepared in the previous phases. A cost/benefit analysis (CBA) is part of a traditional Information Strategy Plan. It may be possible to tailor/modify the CBA for each Business System. Also, analysis of process automation requirements provides the foundation for the IT Concept Document and the User Requirements.

Initiation and Authorization: It may be possible to have multiple life cycles in use in a single project, depending on the nature of the process automation requirements to be met.

Project Definition and System Design: The activities of these two stages may be combined into a Technical Design Stage. Information documented in the first three stages form the foundation for the analysis and work products to be developed in this stage. However, all mandatory reviews, certifications and signoffs must occur in the proper order.

Construction, Acceptance, Operational Readiness, Operations, and Retirement: No differences.

5.7.2 Advantages and Disadvantages

Advantages

Data Oriented: IE identifies:

- Data that is fundamental to the organization
- Data that supports management decision making

This defines the standard terminology essential for common information systems or tailored expert systems.

Data Consolidation: IE includes cross-checking steps, both manual and automated, to identify redundant data, data flows, and gaps in data integrity. The result is an integrated data model able to be shared by all authorized parties who use the same data.

Use of Modeling Techniques: Graphics are used to represent data, illustrating strategies and expert rules for the management of the data and the organization itself. This is represented in a schematic data model..

Process Redesign: The early steps of IE allow for analysis of current processes/ procedures and redesign the existing processes if so desired. The redesign is then supported by the automated system(s) under development.

User Involvement: IE draws on the expert knowledge of users throughout the organization. Joint Application Development (JAD) techniques and one-on-one interviews with strategically placed users can also be used to facilitate this process.

Evolutionary: IE uses top-down design and formal steps that progressively expand and enrich the definition of the data model and its strategies and expert rules, as the process extends through various management levels in the organization

Disadvantages

Up-Front Costs:

- Funding: The Business Sponsor must be willing to support a large up-front analysis effort before seeing system outputs.
- Changes: Many changes will occur before there are any results. However, this problem can be mitigated by doing parts of the process that can be considered stand-alone.
- Time: It can take up to two years or more to complete the first three stages of Information Engineering (ISP, BAA, and BSD).
- RAD Limitations: IE does not lend itself to Rapid Application Development (RAD) techniques; although prototyping can be used effectively during the Technical Design stage.

Tasks and Deliverables: In addition to the deliverables required by the Customs Standard Life Cycle, IE requires more deliverables in the up-front analysis stages.

Technical Risks:

- Many products supporting IE claim to generate machine executable code. However, current technology for code generation is not yet mature. Updates and modifications to the code are almost always required.
- Code changes must be tracked and may need to be re-entered whenever the base code is regenerated.

Chapter 6
Alternative Development Models

6.1 Introduction

The Waterfall Life Cycle models described in Chapter 5 are well suited for projects where user requirements are well defined and the technology architecture is familiar. However, the Waterfall models may be difficult to apply when user requirements are vague, when new technology is being deployed, or when the project schedule requires the rapid delivery of at least some functionality.

To address these situations, alternative models have been incorporated into this handbook. This chapter presents three models that may be used at Customs after validation by OIT's Planning Group and approved by Senior Management:

6.1.1 If You Plan To Use An Alternative Model

Because of Customs' limited experience with these models, the required activities, outputs, and reviews have not been completely defined. Nevertheless, it is required that the Project Plan contains the appropriate outputs and reviews as described in the Customs Standard Life Cycle in Chapter 4. Any project that plans to use one of the alternative models should contact OIT's Planning Group for help in defining and tailoring the appropriate outputs and reviews.

Projects will select an appropriate life cycle model from Chapter 5 or 6 based on the needs of the project. After considering the Customs Life Cycle Policies defined in Chapter 2, projects will be guided by the stages, tasks, and activities of the Customs Standard Life Cycle shown in Chapter 4. Also, the Customs Process Asset Library (PAL) contains templates, examples, and procedures which projects will consult in order to take advantage of existing good practices.

Everything in the Customs Standard Life Cycle as defined in Chapter 4 must be accounted for by the project when developing its Project Plan. Based on project size, complexity, visibility, and risk, the tasks/activities or deliverables listed may be combined or expanded. However, each must be specifically accounted for and maintained along with tailoring rationale as part of the tailoring documentation. When approved by Senior Management, the tailored Project Plan, including a written account of tailoring actions, will be the project's SDLC-compliant road map.

6.1.2 Alternative Models

Each of the three alternative models is appropriate for a unique situation where the Waterfall model is impractical.

- **Staged Delivery** is well suited for the incremental rollout of new functionality in a large system.
- **Spiral Development** is an effective model for managing the risk associated with new technology.
- **Evolutionary Prototyping** is appropriate for those cases where the user can only define his requirements through "hands on" interaction with the system.

No one model is universally strong in all capabilities. Ultimately, the selection of a lifecycle model is a trade-off between that model which best matches the unique aspects of the project and the development team's familiarity with the model.

Due to Customs limited experience with these models, Project Tailoring and the Project Initiation Review will be more detailed for any project implementing these models. This is to ensure that required activities and deliverables are accounted for and agreed to by Support Organizations and Senior Management.

Among the most important decision criteria for a project's Senior Management will be an evaluation of the experience level of the team's leaders and managers in actually using the proposed model.

6.2 Staged Delivery

6.2.1 Description

Staged Delivery is a life cycle model where the system is divided into multiple "builds" or releases. The system is developed one release at a time. A project performs project planning and requirements analysis one time only, and then repeats the design, construction, and testing processes multiple times to develop each build of the system. The first build of the system incorporates a subset of the planned capabilities; the next build adds another subset of the planned capabilities, and so on, until the system is complete. The project manager must work with the customers to determine the number, size, and schedule of the builds that will lead to a complete system.

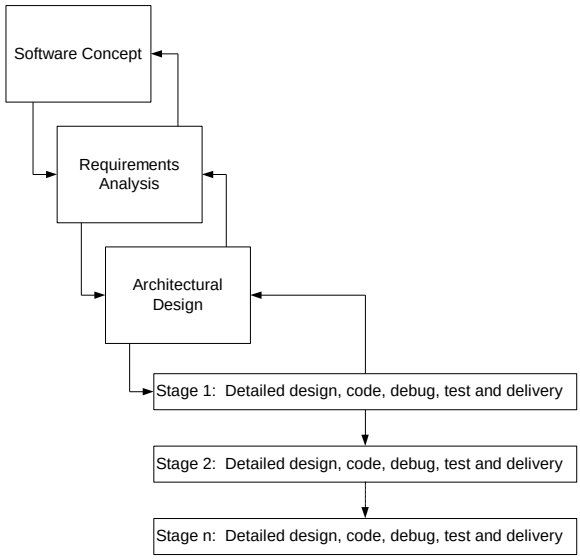


Figure 6.1, Staged Life Cycle

6.2.2 Advantages and Disadvantages

Staged Delivery is most appropriate for large, new systems where system and software requirements are fully defined and clearly understood. The primary advantage of this model is the use of multiple development cycles. This allows the customer to interact with an actual system much sooner and provide feedback to the developers.

The main disadvantage of Staged Delivery is its dependence on having clearly and completely defined system and software requirements at the beginning. It does not allow projects to respond easily to changing requirements.

6.2.3 Implementing this Model

To implement Staged Delivery, the Project Manager coordinates with the customer to determine the number, size, and schedule of incremental builds. A project performs one project initiation phase, one requirements analysis phase, and one architectural design phase. Then the project incrementally designs, constructs, and tests each software unit. The release schedule is built to reflect this arrangement of processes. The Project Manager and customer must work within the Investment Management Process for approvals.

6.2.4 Additional Resources

To learn more about this model, please consider the following sources:

Gilb, Thomas. *Principles of Software Engineering Management*. Wokingham, England, Addison-Wesley, 1988.

6.3 Spiral Development

6.3.1 Description

The Spiral model is a risk-oriented lifecycle model that breaks a software project into mini-projects. Each mini-project addresses one or more major risks until all major risks have been accounted for. Examples of risk are poorly understood user requirements, unfamiliar technology, potential performance concerns, and so on. After the major risks have been accounted for, the spiral model terminates in the familiar stages of the Waterfall Life Cycle (i.e., detailed design, construction, acceptance test and release).

Figure 6.2 presents the Spiral Development model. The basic idea behind the diagram is that you start on a small scale at the center of the spiral, identify the risk facing your project, explore the risk with a prototype, refine requirements and design based on the success of the prototype, and then commit to an approach for the next iteration. Each iteration leads the project to a larger scale.

6.3.2 Advantages and Disadvantages

The greatest advantage of the Spiral model is that as costs increase, risks decrease. That is, risks (e.g. unfamiliar technology, unclear requirements) are accounted for early in the project's life cycle through prototypes – before large-scale development activity has begun. When properly implemented, the Spiral model provides at least as much management control as the traditional Waterfall. It provides checkpoints at the end of each iteration and detailed in risk mitigation reviews. If the risk of an iteration proves insurmountable, an alternative solution can be explored.

The major disadvantage of the Spiral model is that it is complicated. It requires more planning and managerial sophistication than the waterfall models. It requires that the risks faced by the project be well understood from the start. It also requires that objective and quantifiable criteria be in place to assess each iteration. In addition, customer expectations must be carefully managed since the prototypes developed are not production-ready 'mini-systems'. Because of the iterative nature of the spiral model, it is sometimes difficult to estimate total project completion dates.

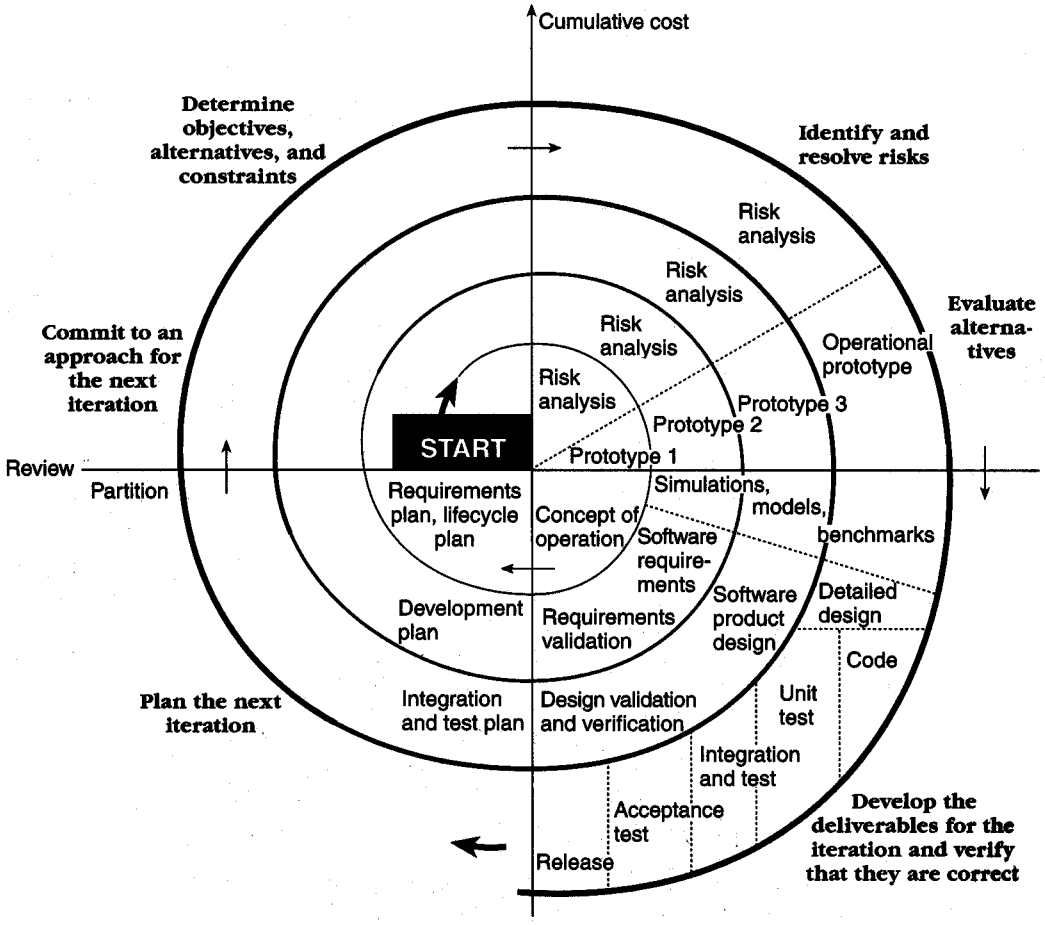


Figure 6.2, Spiral Life Cycle

6.3.3 Implementing this Model

To begin the Spiral model, the Project Manager must identify the major risks that are inherent to the project. Each iteration of the spiral represents a prototype project designed to resolve a specific risk. The initial Project Plan must identify the objective of each iteration and the criteria for graduation to the next iteration. The Project Manager and customer must work within the Investment Management Process for approvals.

6.3.4 Additional Resources

To learn more about the spiral model, please consider the following sources:

- Boehm, Barry W, *Software Risk Management*, Washington, D.C. IEEE Computer Society Press, 1989
- DeGrace, Peter and Leslie H. Stahl. *Wicked Problems, Righteous Solutions.* Englewood Cliffs, N.J. Yourdon Press, 1990.
- McConnell, Steve, *Rapid Development*, Redmond, Washington, Microsoft Press, 1996

6.4 Evolutionary Prototyping

6.4.1 Description

Evolutionary Prototyping is a lifecycle model where the system concept is refined as the project progresses. The most visible aspects of the project (usually the user interface) are developed first. That aspect is then delivered to the customer as a prototype and is refined as feedback is received. When the user decides that the prototype is satisfactory, the internal features of the system are completed. Figure 6.3 depicts this model graphically.

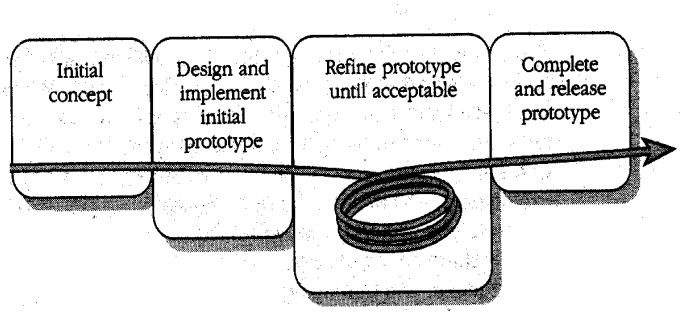


Figure 6.3, Evolutionary Prototyping Method

The Evolutionary Prototyping model is best suited for those projects where there is frequent and informal interaction with the end-user. This model should not be confused with "code-and-fix" development or "throw-away prototyping". Real evolutionary prototyping includes real requirements analysis, real design and real maintainable code – just in smaller increments than is usually found in traditional approaches.

6.4.2 Advantages and Disadvantages

Evolutionary prototyping is especially useful when requirements are changing rapidly or when the user and developer are unsure of the application area. It produces steady, visible signs of progress which can be useful when there is a demand for development speed.

There are significant disadvantages with this model, however, that should be clearly understood and carefully managed:

- Unrealistic schedule and budget expectations. When the end user sees the visible aspects of a system developed so quickly, he often expects the internal (and more complex) aspects of the system to be developed with equal speed.

- Poor design and performance. Because the system is developed "from the outside in", systems performance is often inadequately considered during design.

- Diminished project control. Because the full set of requirements is unknown at the project's start, it is impossible to determine the full schedule and budget of the project.

These disadvantages are so great that the Project Plan should contain explicit steps for how they will be managed.

6.4.3 Implementing this Model

When using this model, the Project Manager's first step should be to negotiate the ultimate scope and schedule of the system with the user. Knowledge of the ultimate load that will be placed on the system – and the user's expectation of when the final system will be developed – are necessary to prevent unrealistic expectations about the project.

- Understanding of the scope and schedule are also needed to identify that aspect of the system that should be prototyped first. Failure to understand the ultimate scope of the system, early in the project's life, significantly increases the chances that the prototype will be discarded.

- The Project Manager and the customer must work within the Investment Management Process for approvals.

6.4.4 Additional Resources

If you are interested in learning more about this model, please consider the following sources:

Gordon, V. Scott, and James M. Bieman. "Rapid Prototyping: Lessons Learned," *IEEE Software*, January 1995.

Connell, John, and Linda Shafer. *Object-Oriented Rapid Prototyping.* Englewood Cliffs, N.J. Yourdon Press, 1995

Reilly, John P. *Rapid Prototyping: Moving to Business-Centric Development*. New York: International Thomson Computer Press, 1996.

Appendix A
Glossary

A.1 Introduction

This appendix contains the definitions of acronyms and terms used in this handbook. Glossary definitions have been specifically tailored and clarified for Customs unique requirements. These definitions are useful in fully understanding the intent of many portions of the basic document. For example, Policy 2.3.1.3 says that "Each project shall have a single Project Manager officially designated by Senior Management." The meaning of both Project Manager and Senior Management are defined in this Glossary.

In Section A.2, Acronyms, each acronym is listed alphabetically with its meaning.

In Section A.3, Definitions, each term is listed in alphabetical order with its definition as used by the Customs Service. **Bolded** items reference other definitions in this section.

A.2 Acronyms

AC	Assistant Commissioner
AIS	Automated Information System
ATD	Applied Technology Division
BAA	Business Area Analysis
BIA	Business Impact Analysis
BIR	Business Interface Representative
BITR	Business Information Technology Representative
BPR	Business Process Reengineering
BSD	Business Systems Design
CASE	Computer-aided Software Engineering
CBA	Cost/Benefit Analysis
CBT	Computer-Based Training
CCB	Change Control Board
CDR	Critical Design Review
CI	Configuration Item
CIO	Chief Information Officer
CIS	Customs Issuance System
CM	Configuration Management

CMM Capability Maturity Model
CMO Customs Modernization Office

COOP	Continuity of Operations Plan
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-the-Shelf
CSO	Computer Security Officer
DAA	Designated Approval Authority
DDL	Data Definition Language
ELCM	Enterprise Life Cycle Methodology
FIPS	Federal Information Processing Standards
GAO	General Accounting Office
GOTS	Government Off-the-Shelf
GSA	General Services Administration
HB	Handbook
IE	Information Engineering
IMP	Investment Management Process
IRB	Investment Review Board
ISA	Interconnection Security Agreement
ISPG	Infrastructure Services Process Group
ISSB	Information Systems Security Branch
ISD	Infrastructure Services Division
ISP	1. Infrastructure Support Process 2. Information Strategy Planning (Information Engineering Life Cycle)
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITC	Information Technology Committee
ITCD	Information Technology Concept Document
JAD	Joint Application Development
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NTEU	National Treasury Employees Union
OFPD	Office of Finance, Procurement Division
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OPR	Operational Problem Report
ORMS	Operations Run Manual System
ORR	Operational Readiness Review
PAL	Process Asset Library
PAT	Process Action Team

PG	Planning Group
PM	Project Manager
PMG	Program Monitoring Group
PRR	Production Readiness Review
QA	Quality Assurance
RAD	Rapid Application Development
RMG	Resource Management Group
RTM	Requirements Traceability Matrix
SAPG	System Acquisition Process Group
SAT	System Acceptance Testing
SDD	Software Development Division
SDLC	Systems Development Life Cycle
SEI	Software Engineering Institute of Carnegie Mellon University
SEPG	Software Engineering Process Group
SLC	Systems Life Cycle Team
SOP	Standard Operation Procedure(s)
SOW	Statement of Work
TAG	Technology and Architecture Group
TD	Treasury Directive
TPR	Test Problem Report
TRC	Technology Review Committee
TRR	Test Readiness Review
USCS	United States Customs Service
WBS	Work Breakdown Structure

A.3 Definitions

Acceptance Stage (Stage 6) This life cycle stage includes two types of testing:

1. The system is tested to ensure that it interfaces properly with other automated systems within the Customs environment.
2. Independent testers and the users test the system to ensure that the system meets the needs stated in the **User Requirements** and the **Functional Requirements**.

In addition, Security Certification and Accreditation are obtained during this stage. This stage is preceded by the **Construction Stage (Stage 5)** and followed by the **Operational Readiness Stage (Stage 7)**.

Acceptance Testing Acceptance testing is done by independent testers after all developer system and integration testing is done. Acceptance testing should not be used as part of the debugging process.

Accreditation See **Security Accreditation Statement**.

Acquisition Organization The organization within OIT (part of the **Planning Group**) that serves as the primary interface between application developers and the Procurement Division in the **Office of Finance (OFPD)**.

Acquisition Plan The plan developed with the **Acquisition Organization** to acquire products and services for completing the Project. It forms the basis for the **Statement of Work** issued by OFPD.

See also: **Infrastructure Plan**
Subcontractor

Action Item A **task** or **issue** assigned to an individual to research or resolve by a specific date.

Activity The action, steps, or process taken to create or achieve a specific product, service, or result.

See also: **Task**

Application A software grouping of related functions, or a series of interdependent or closely related programs, that when executed accomplish a specified objective or set of user requirements.

See also: **Automated Information System (AIS)**
Information Technology
System

Applied Technology Division (ATD) The division within OIT responsible for supporting all elements of the Customs enforcement and facilitation processes through the identification of operational requirements and, when applicable, the development, acquisition, testing, and maintenance of new technology and equipment.

Architecture Compliance Reviews Reviews by the Technology and Architecture Group to determine if the documentation, functional analysis, general design, detailed design are in compliance with the architecture components approved through the **Technical Compliance Reviews** process.

Architecture Organization The part of **TAG** responsible for all activities relating to the development, implementation, and management of Customs architectures and technology domains. This includes maintenance of the **Enterprise Architecture** Repository and Technical Reference Model. They also facilitate and support the **TRC**.

Audit An independent examination of work products or processes to verify accuracy and assess compliance with specifications, standards, contractual agreements, or other criteria.

See also: **Audit Trail**

Audit Trail A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. Written or electronic documentation is necessary to provide auditable records.

See also: **Audit**

Automated Information System (AIS) An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

See also: **Application**
System
Information Technology

Automation Framework The family of hardware and software automation tools supported by U.S. Customs to identify and resolve problems in processing all components of the **application**.

Automation Readiness Automation readiness is established when an **application** is capable of detecting and reporting status information to the **automation framework** without manual intervention. See the *Automation Standards Definition* for specifics.

Baseline A specification or product that has been formally reviewed and agreed upon, which thereafter serves as the basis for further development. Changes to a baseline can be done only through formal change control procedures. Multiple baselines can be defined for a project representing different stages of its life cycle.

See also: **Change Management**

Business Alignment Assessment The architecture process to determine if the project ideas submitted by the business process area is in alignment with Customs strategic plans, goals, and objectives.

See also: **Solution Proposal Assessment**
Technical Compliance Reviews
Architecture Compliance Reviews

Business Area Analysis (BAA) One of the early phases in the Information Engineering Life Cycle, which occurs prior to defining automation requirements to support the **business functions**.

Business Case The Business Case organizes the information necessary to justify the project and to make a funding decision in a consistent, structured format. It consists of a Business Case Worksheet and appropriate attachments for **ITC** and **IRB** review. Projects under $100K may use a tailored version of this as defined in the *Investment Management Process System*

Description. The Business Case is developed during the **Concept and Business Case Stage (Stage 1)** and is updated periodically thereafter.

Business Function A group of related, higher-level business activities that completely support one aspect of the enterprise. Each function describes something the enterprise does, independent of the structure of the organization.

Business Impact Analysis (BIA) A document which spans all business areas and which sets the restoration priority of all **business functions** as compared to other business functions. This prioritization is a source for enterprise contingency planning and disaster recovery planning.

See also: **Continuity of Operations Plan (COOP)**
Disaster Recovery Plan

Business Interface Representative (BIR) OIT's representative to the **Business Sponsor** and **users**. The BIR is responsible for maintaining strategic communication between OIT and the business area and serving as the single point of contact for the **BITR** and Business Sponsor.

Business Information Technology Representative (BITR) The **Business Sponsor**'s primary representative to OIT. For each business area, OIT has assigned a **BIR** as its primary point of contact for the BITR. The BITR is a member of the **Information Technology Committee (ITC)**. The BITR may delegate specific project-related duties to a **Business Project Manager**.

Business Process A defined process whose execution is of value to the customer, i.e. meets a business need..

Business Project Manager If the Business Sponsor/BITR chose to designate a Business Project Manager, that person is the project's point of contact representing the **Business Sponsor** and **Users**.

See also: **BITR**

Business Sponsor The Customs executive who represents the business organization and the **end-users**, and who is ultimately responsible for sponsoring projects that provide functional value to the business. The AC, OIT will assign a Business Sponsor within OIT for OIT sponsored projects (such as infrastructure).

Business System Design (BSD) One of the early phases in the Information Engineering Life Cycle, which occurs prior to defining automation requirements to support the **business functions**.

Capability Maturity Model (CMM) A model or framework that describes the key elements of an effective process for managing and developing products in a disciplined and consistent way. It is based on the assumption that an organization's process maturity level can be measured and improved.

Capacity Planning Organization The OIT organization responsible for monitoring computer resource usage by various applications and notifying Senior Management when the resource usage reaches a level where the service level agreements cannot be met.

See also: **Support Organizations**
Infrastructure Services Division (ISD)

CASE Tools An integrated set of software tools and automated programs that simplify application development and enhance productivity.

Certification See **Requirements Certification** or **Security Certification**.

Change Control Board (CCB) Reviews each change request, evaluates the impact on the project, and either renders an approve/disapprove decision for change requests within the scope of approved resources or refers them to **Senior Management**. The CCB also helps prioritize approved changed requests and requirements for release.

Change Management The process used by **Configuration Management (CM)**, **Requirements Management**, and **CCB**s to evaluate and make decisions about changes that impact technical **baselines**, operational baselines, or approved schedules and plans.

Commercial Off-the-Shelf (COTS) Products developed by commercial organizations and offered for sale. Also used as a generic term encompassing both COTS and GOTS products.

See also: **GOTS**

Computer Security Officer (CSO) The person in the Business or Development area assigned responsibility for the security of an application or other IT system.

Concept and Business Case Stage (Stage 1) This life cycle stage begins with the business need for a particular automated solution and ends with the approval for funds to be released. Included in this stage are reviews by the **TRC**, **ITC**, and **IRB**. This is the first stage of the life cycle and is followed by the **Initiation and Authorization Stage (Stage 2)**.

See also: **Customs Standard Life Cycle**

Configuration A snapshot in time of the properties, characteristics, or specifications of a system or product.

Configuration Control Management of the properties, characteristics, or specifications of a system or product.

See also: **Configuration Management**

Configuration Item (CI) An item (consisting of hardware components, software units, or both) that is designated for **configuration management** and treated as a single entity in the configuration management process.

Configuration Management (CM) A discipline that, throughout the lifecycle:

- Identifies the configuration of the work products at given points in time
- Systematically controls changes to the work products
- Maintains the integrity and traceability of the configuration.

See also: **OIT CM Organization**
Project CM Team
Baseline

Configuration Management Plan A document that identifies the project's **configuration items**, assigns responsibilities, and defines the mechanisms the project will use to control changes and to ensure visibility and traceability within the project **baselines**.

See also: **Configuration Management**
Project CM Team
Project Definition Stage (Stage 3)

Construction Stage (Stage 5) During this stage, the requirements and design developed during the previous stages are translated into operational work products (e.g., infrastructure, source code, and databases). Also, equipment is received and checked. This stage is preceded by the **System Design Stage (Stage 4)** and followed by the **Acceptance Stage (Stage 6)**.

See also: **Customs Standard Life Cycle**

Contingency Plan The document that describes the organized process for a project or system to respond to emergencies and interruptions that are less than a disaster and that can be resolved using routine procedures.

See also: **Disaster Recovery Plan**

Continuity of Operations Plan (COOP) This document, developed by the business areas within specific locations, defines the procedures for restoring **business functions** (both manual and automated) in the case of a disaster.

See also: **Business Impact Analysis (BIA)**
Disaster Recovery Plan

Contracting Officer The individual from the Customs **Office of Finance, Procurement Division (OFPD)** with authority to procure, enter into, administer, and/or terminate contracts and make related determinations and findings. It is their responsibility to obtain goods and services for the Government by contract when and where needed, at the most reasonable price, and in accordance with applicable laws and regulations.

Contracting Officer's Technical Representative (COTR) The principal program representative assigned to a Government acquisition. They are a legal representative of the Government and are delegated authority to make certain commitments such as accepting or rejecting the contractor's work. They are not authorized to make changes to the contract's requirements.

Cost/Benefit Analysis (CBA) A study projecting the costs and benefits of a system. Costs include all resources required for development as well as for operating the system over the system's life. This document is required during the **Concept and Business Case Stage (Stage 1)** prior to **IRB** approval and is updated periodically thereafter.

See also: **IT Concept Document (ITCD)**
Business Case
Investment Management Process (IMP)

Critical Design Review (CDR) The quality gate review that occurs at the end of the **System Design Stage (Stage 4)** to ensure that the system design has been accepted by the **Business Sponsor** and all affected **stakeholders** including **Support Organizations** and **Senior Management**. On completion of the CDR signoffs, the **Construction Stage (Stage 5)** begins.

See also: **Reviews**
Design Review

Customs Modernization Office (CMO) The OIT organization responsible for the high-level management, implementation, and execution of the Customs Modernization Program and the business process reengineering that it enables.

See also: **System Acquisition Process Group (SAPG)**

Customization Altering the source code of a COTS or GOTS product in order to meet one or more requirements.

See also: **Tailoring**

Customs Standard Life Cycle The framework that describes management expectations of the activities, reviews, and deliverables that shall occur during the development life cycle.

See also: **Life Cycle**
Concept and Business Case Stage (Stage 1)
Initiation and Authorization Stage (Stage 2)
Project Definition Stage (Stage 3)
System Design Stage (Stage 4)
Construction Stage (Stage 5)
Acceptance Stage (Stage 6)
Operational Readiness Stage (Stage 7)
Operations Stage (Stage 8)
Retirement Stage (Stage 9)
Project Management Support

Data Conservation/Conversion Plan The plan which documents how data will be managed/stored when the system it supports is removed from **Production**. If the system is being replaced, this will be part of the new system's **Data Management Plan**.

Data Integrity A measure of the reliability, usefulness, or lack of corruption of data or a data set.

See also: **Data Management Organization**
Security Requirements

Data Management Organization The organization(s) within OIT with the following responsibilities:

- Creation and maintenance of the logical and physical data models
- Generation of Data Definition Language statements
- Technical design and management of the physical database and database objects
- Evaluation, selection, and implementation of the data dictionary and database catalog
- Management, administration, and performance of the Database Management System (DBMS) software

See also: **Support Organizations**

Data Management Plan A document updated throughout the project's life cycle that provides details on the data management activities, data models, database designs, and conversion plans for the project.

Data Privacy/Confidentiality The need to protect the data from unauthorized disclosure, as required by the Privacy Act of 1974 as amended, the trade secrets acts, or some other policy.

Data Requirements Information needs, data elements, data standards, data management and data integrity requirements for a system.

See also: **Data Management Plan**
Functional Requirements

Definition Phase Completion Review A **review** held by the **Development Team** and the **Project Manager** at the end of the **Project Definition Stage (Stage 3)** to ensure that all **deliverables** are appropriate, **requirements** have been certified, and that the project is ready to proceed to the **System Design Stage (Stage 4).**

Deliverable An **output** from a system development activity. Some deliverables may consist of components produced in different life cycle stages.

Deployment Plan A plan, defined by agreements between the **Project Team**, the **Business Sponsor**, and the **Users**, that identifies the strategies and schedules for fielding a system. This plan is activated during the **Acceptance Stage (Stage 6)** following the **PRR**, and covers activities conducted during the **Operational Readiness Stage (Stage 7)** and the **Operations Stage (Stage 8)**. It may include pilot testing, version releases, fielding plans, etc. Depending on the needs of the project, this information may be defined separately or included within the **Project Plan**, a **Release Plan**, or combined with information in the **Implementation Plan**.

Design Review Both Preliminary and Detailed Design Reviews may occur multiple times in the **System Design Stage (Stage 4)** with different attendees to validate different aspects of the

design (e.g., architecture, interfaces, screen, communications, security, logical and physical data models, modules).

See also: **Critical Design Review (CDR)**
Reviews

Designated Approval Authority (DAA) The individual appointed by the Commissioner of Customs to exercise authority and assume formal responsibility for operating all Customs systems at an acceptable level of risk (currently the AC, OIT).

See also: **Security Accreditation**

Detailed Design Review See **Design Review**.

Development Team The group/individual responsible for analyzing, designing, developing, documenting, testing, and implementing a **system**. The Development Team is one part of the **Project Team**.

See also: **Project Implementation Team**

Disaster Recovery Plan The document that describes the organized process for implementing emergency responses, back-up operation, and post-disaster recovery that will ensure the availability of critical IT resources and facilitate continuous operations in a disaster. A Disaster Recovery Plan takes effect when normal procedures fail to resolve a problem.

See also: **Contingency Plan**

Division Director An executive level manager of an operational division who reports to the AC, OIT.

Documented Procedure A **procedure** documented by the project and available for reference in the **Process Asset Library (PAL)**.

Domain The primary classification level of the technology components of the **Technical Reference Model**.

End-User See **User**.

Enterprise Architecture The Enterprise Architecture is a strategic information asset base which defines the mission, the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to the changing needs of the mission.

See also: **TAG**
Architecture Organization
Technical Reference Model

Enterprise Life Cycle Methodology (ELCM) The Enterprise Life Cycle Methodology provides a framework for executive direction, control, and management of the major life cycle

processes for information and technology systems and infrastructure. These high-level processes include Strategic Planning, Budget, Enterprise Architecture, Investment Management, and the SDLC.

Enterprise Process Improvement Program (EPIP) The Enterprise Process Improvement Program coordinates and encourages all process improvement activities within OIT. It includes all divisions and staff functions. A Management Steering Committee (MSC) will lead this program, and sponsor Process Groups (e.g., the **SEPG, SAPG** and **ISPG**) to focus on improvements in specific disciplines.

See also: **Process Group**

Entry Criteria The conditions which must be met before a process, procedure, or specific life cycle stage or activity can begin. They are the same conditions as the **exit criteria** of the previous process, procedure or stage.

See also: **Inputs**
Outputs

Environment The collection of hardware, software, communications, networks, and components used to support **automated information systems**. Working/Operational Environments include the Development, Project Test, Staging, Lab, **System Acceptance Test (SAT)**, Education/Training, and **Production** environments.

Evaluation Organization The Evaluation Organization is an OIT organization that is responsible for the formal monitoring of various work products. It ensures that standards, policies, regulations, and anticipated benefits are being met. Responsibilities include performing evaluations, SDLC/Compliance **Audits**, Technical Architecture Compliance Audits, and Post-Implementation Reviews.

See also: **Post-Implementation Review (PIR)**
TAG

Event-Driven Review/Activity A **formal review** or activity whose performance is based on the occurrence of another event within the project (e.g., a problem/risk manifests, or a deliverable or life cycle stage is complete).

See also: **Periodic Review/Activity**.

Executive Management Team On some projects there may also be a separate group, at a higher level than the **Project Management Team**, with project management and oversight responsibilities.

Exit Criteria The conditions which must be met before a process, procedure or specific life cycle stage or activity can end. They are the same conditions as the **entry criteria** of the next process, procedure or stage.

See also: **Inputs**
Outputs

Formal Review A formal meeting at which a product is presented to the **end-user**, **Business Sponsor**, or other interested parties for comment and approval. This meeting can also include a review of management and technical activities and of the progress of the project.

See also: **Reviews**

Functional Requirements A precise description of the requirements of a computer system. In a clear, testable manner, it includes:

- A statement of inputs to be supplied by the user
- A description of the outputs desired by the user
- The algorithms involved in any computations desired by the user
- A description of physical constraints such as response time, user hardware/environment, and transaction volumes
- Support requirements (e.g., QA, CM, Training, Security, and deployment requirements)

See also: **Project Team**
Support Organizations
Data Requirements
Security Requirements
Training Requirements
Quality Requirements

Government Off-the-Shelf (GOTS) Products developed by government agencies. Software products are currently being collected and distributed by the National Technical Information Service (NTIS).

See also: **COTS**

Hardware The physical equipment and electronic components associated with a system.

Help Desk Organization The OIT group responsible for documenting, routing, and tracking *reported* incidents and problems until they are resolved and the originator is notified

See also: **Support Organizations**
Infrastructure Services Division (ISD)

Implementation Plan This plan identifies all activities relating to the migration of the system into the Test and Production environments, including all configuration items and support items that must be in place. This agreement is between the **Project Team**, the **OIT CM Organization**, **Supporting Organizations**, and the **Infrastructure Services Division (ISD)**.

See also: **Deployment Plan**

Independent Review Review performed by personnel independent of the **Project Team**.

See also: **Quality Assurance**

Independent Testing Testing performed by staff who did not develop or construct the product under review.

See also: **Testers**
Acceptance Stage (Stage 6)
System Acceptance Test Plan
User Acceptance Testing

Information Security In total, information security involves the precautions taken to protect the confidentiality, integrity and availability of information. It encompasses three types of security: (1) Applications Security, (2) Installation Security, and (3) Personnel Security.

Information Strategy Planning (ISP) One of the early phases in the Information Engineering Life Cycle, which occurs prior to defining automation requirements to support the **business functions**.

Information Systems Security Branch (ISSB) See **OIT Security Organization**.

Information Systems Security Manager (ISSM) An OIT-assigned role, currently the head of **ISSB**, that has the following responsibilities:

- Responsible for the Customs-wide IS security program
- Coordinates with and provides leadership to an infrastructure of appointed security personnel, including the **CSOs** and **System Design Security Officers (SDSOs)**

See also: **OIT Security Organization**
Security Certification

Information Systems Security Officer (ISSO) The ISSO serves as the single point-of-contact within his/her business area on all IS security matters. The **BITR** for each business area serves as that area's ISSO. The ISSO appoints the required CSOs for each application/system.

Information Technology (IT) Information Technology (IT) is the sum of all equipment, software, and other things used to define, acquire, store, transport, communicate, process, or disseminate electronic data.

Information Technology Committee (ITC) A review committee composed of OIT **Senior Management** and the **Business Information Technology Representatives (BITRs)** responsible for ensuring proposed projects are sound and prudent business investments.

See also: **Investment Management Process (IMP)**

Infrastructure The underlying framework of an organization or system, including organizational structures, policies, standards, training, facilities, equipment, hardware, communications, and tools, that supports its ongoing performance.

See also: **Infrastructure Services Division (ISD)**

Infrastructure Plan A document that defines the architecture, communications, hardware, and other **infrastructure** support needs of the **Project**. It may form the basis of an **Acquisition**

Plan for infrastructure items as needed. Depending on the project, this information may be included within the **Project Plan**.

Infrastructure Retirement/Conversion Plan A document that defines how infrastructure items will be handled when the system they support is removed from **Production**. If the system is being replaced, this will be part of the new system's **Infrastructure Plan**.

Infrastructure Services Division (ISD) The division within OIT responsible for implementation and support of the Customs information **infrastructure**, supporting development including engineering and operation of all platforms, management of the Customs network and communications functions, database design and database administration for all platforms, and desktop support for all users of Customs automated systems.

See also: **Project Team**
Support Organizations
Capacity Planning Organization
Help Desk Organization
ISD Support Teams

ISD Support Teams Includes all the teams that make up the **Infrastructure Services Division (ISD)**, particularly those in ISD/Systems Engineering and ISD/Systems Operations.

See also: **Support Organizations**

Infrastructure Services Process Group (ISPG) A chartered organization within OIT formed to facilitate the definition, maintenance, and improvement of the OIT **processes** and **procedures** related to the discipline of Systems Engineering and Operations. It provides recommendations to its oversight body, the **Management Steering Committee (MSC)**. It guides and assists groups and projects within OIT with **infrastructure** process improvement tasks and activities.

See also: **Process Group**
Infrastructure Services Division (ISD)

Infrastructure Support Process (ISP) A process that brings **ISD** and **SDD** staff together during the **SDLC** development phases. This process allows the ISD Support Teams to provide technical guidance and resolve any issues prior to production implementation, and allows ISD to be prepared to support applications before they are moved into **Production**.

See also: **Life Cycle**

Initial Project Plan This Plan uses the Project Plan template. It is created during the **Initiation and Authorization Stage (Stage 2),** refined as more information is obtained in later stages and **baselined** as the **Project Plan** during the **System Design Stage (Stage 4)**. It includes at least:

- the general management strategy,
- tailored life cycle,
- tailored deliverables with rationales,
- an initial work breakdown structure (WBS),

- an estimate of time and costs for each task/WBS item, and
- a schedule.

See also: **Project Plan**

Initiation and Authorization Stage (Stage 2) This stage begins when funding is released to begin detailed project planning. This includes developing a draft of user requirements and infrastructure planning, an initial project plan, and appropriate life cycle tailoring. This stage ends with a review process (i.e., Project **Tailoring** Reviews) and a Project Initiation Review that authorizes the project to continue with development. This stage is preceded by the **Concept & Business Case Stage (Stage 1)** and followed by the **Project Definition Stage (Stage 3)**.

See also: **Customs Standard Life Cycle**

Inputs The work products that are used by a process, procedure, stage, or activity. These are products that were created previous to the "current" life cycle stage. They may be changed during the stage for which they are inputs, they may be referenced by or for other work products during that stage, or they may be carried through to a following process, procedure, or stage.

See also: **Entry Criteria**
Exit Criteria
Outputs

Integration Testing A type of testing that ensures that all new or modified components of the system interact correctly with its interfacing systems. It is conducted by members of the **Development Team** during the **Construction Stage (Stage 5)**.

See also: **System Test Plan**

Interconnection Security Agreement (ISA) A formal technical document that supports an approved Memorandum of Understanding and identifies connections between internal Customs systems and any non-Customs systems and networks. Signatories to the final agreement are the Customs CIO and the equivalent level in the non-Customs organization.

See also: **Project Definition Stage (Stage 3)**

Interface A connection between two components of a **system** or between components of two different systems.

Investment Management Process (IMP) A structured approach to managing IT investments that ensures that all IT investments (systems and projects) align with the Customs mission, support its business, minimize risks, and maximize returns throughout the investment's life cycle. This process is begun in the **Concept and Business Case Stage (Stage 1)** and continues throughout the life of the system.

Investment Organization The OIT organization (part of the **Planning Group**) responsible for development and maintenance of the **Investment Management Process (IMP)**, supporting documentation, and subsidiary processes. They also provide support to the **ITC** and **IRB**, and to

Projects in the **Concept and Business Case Stage (Stage 1)** and **Initiation and Authorization Stage (Stage 2)**.

Investment Review Board (IRB) Consisting of Customs Deputy Commissioner and Assistant Commissioners, the IRB is responsible for selecting, controlling, and evaluating all strategic investment decisions. They participate in and direct the **Investment Management Process (IMP)**.

Issue Anything that might affect the achievement of a program or project objective. This may include risks, constraints, and other project concerns.

IT Concept Document (ITCD) This document provides the basic information required for the **TRC** to decide on proposed information technology projects while they are still at the concept stage.

See also: **Investment Management Process (IMP)**

IT Portfolio A collection of IT projects, including applications and other technical investments, defined as the mixture of projects that best meet the mission needs of the Customs Service and which are managed as investments.

Library The controlled collection of configuration items or work products associated with defined baselines.

Life Cycle A series of ordered, repeatable processes used to design, develop, maintain, and retire a product or configuration. It defines when and what activities will occur during the life of a system.

See also: **Customs Standard Life Cycle**

Major Application An **application** that requires special attention to its security due to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or unauthorized modification of the information in the application.

Management Steering Committee (MSC) This steering committee leads and sponsors the **Enterprise Process Improvement Program (EPIP)** across all organizations in OIT. Membership includes the AC, OIT; the Directors of SDD, ISD, ATD, CMO, PG, and TAG; the Chair of each Process Group; and the Planning Group Lead for MSC Support.

See also: **Process Group**
Software Engineering Process Group (SEPG)
System Acquisition Process Group (SAPG)
Infrastructure Services Process Group (ISPG)

Measure The dimension, capacity, or quantity of a process or product. Measurement data is collected and compared with expected values to provide insight into specific issues/activities.

See also: **Metrics**

Metrics A **measure** that provides objective information about Project Schedule, Resources (staff, level of effort, computer), Costs, Requirements and Work Product Sizes and Changes, and Product Quality. They are collected to use for decision making within the current project and to provide historical data for use in future projects.

Milestone A significant point in a project. A milestone has no duration; it represents the start or the completion of a portion of work.

See also: **Schedule**

Mission-related Performance A metric that focuses on **Performance Measures**.

Office of Finance, Procurement Division (OFPD) The Customs organization responsible for producing, authorizing, and monitoring contracts for acquiring products and/or services.

See also: **Contracting Officer**
Acquisition Organization

OIT CM Organization The organization(s) within OIT responsible for defining standards and procedures that contribute to maintaining the integrity of all enterprise work products and for controlling assigned **Production** baselines.

See also: **Project CM Team**

OIT QA Organization The organization(s) within OIT responsible for overseeing and verifying **Quality Assurance** activities, independent of the project.

See also: **Project Quality Assurance**
Project QA Team

OIT Security Organization The OIT Security Organization consists of infrastructure staff who maintain enterprise IT security policies, provide enterprise IT security planning, review all security-relevant SDLC documents, and provide IT security and advice and assistance to IT Project Managers.

See also: **Support Organizations**
Project Security Team

On-going Costs Those costs which can be reasonably expected to recur on a regular basis during a product's life cycle.

See also: **Up-Front Costs**

Operation A system in operation is one that has been accepted by the **Business Sponsor**. It is in the process of being rolled out for general use, and is running in the Customs **Production** environment.

See also: **Operations Stage (Stage 8)**

Operational Readiness Stage (Stage 7) This life cycle stage is the point at which the new system is moved into the Customs **Production** environment. Transition activities during this stage include: site preparations, infrastructure installation/deployment, data conversions, database and system code installation into the Production environment, field testing, parallel operations, and training. In the case of some legacy mainframe systems and very small projects, this stage may take less than a day to complete. This stage is preceded by the **Acceptance Stage (Stage 6)** and followed by the **Operations Stage (Stage 8)**.

See also: **Customs Standard Life Cycle**

Operational Readiness Review (ORR) The meeting that occurs at the end of the **Operational Readiness Stage (Stage 7)** during which the **Business Sponsor**, the **Project Manager**, **Supporting Organizations**, and **Senior Management** document their concurrence that the new system may be deployed into full operation. On completion of the ORR signoffs, the **Production Notice** may be released and the **Operations Stage (Stage 8)** begun.

See also: **Reviews**

Operations Stage (Stage 8) This lifecycle stage is the period during which the system is in general use throughout the Customs Service. This stage consists of activating and rolling out the system to all of the implementation sites plus the activities to monitor performance of the system in **Production** and ensure continuity of operations. Activities during this stage include:

- Performance monitoring and management feedback
- Managing system and infrastructure problems
- Implementing system and infrastructure changes

The system is reviewed while in **operation** to ensure that it continues to meet user needs and accreditation requirements. This stage is preceded by the **Operational Readiness Stage (Stage 7)** and followed by the **Retirement Stage (Stage 9)**.

See also: **Customs Standard Life Cycle**

Outputs The work products that are generated or produced by a specific process, procedure, stage, or activity. These are products that were created or changed in the "current" life cycle stage or they may be carried through to a following process, procedure, or stage unchanged.

See also: **Entry Criteria**
Exit Criteria
Inputs

Peer Review A review of a work product, following defined **procedures**, by peers of the producers of the product for the purpose of identifying defects and improvements.

See also: **Reviews**
Walkthroughs

Performance Measure An indicator that shows the progress of an action against the plan. It monitors the extent to which a specific goal or objective has been reached. It is generally used to track:

- the responsiveness of the configuration of equipment and software to the needs of users, and

- the availability and reliability of individual components and the system as a whole.

See also: **Measure**
Metrics

Periodic Review/Activity A review or activity that occurs at specified, regular time intervals (such as weekly Project Status Meetings).

See also: **Event-Driven Review/Activity**

Planning Group (PG) An OIT organization with the following responsibilities:

- Develops, communicates, and coordinates OIT's plans, including budget formulation, strategic plans, and performance measures
- Provides CMM® and life cycle policy expertise and support for the Enterprise Process Improvement Program (EPIP) and associated organizations (e.g., Process Groups) and projects
- Provides assistance and support to the ITC and IRB
- Provides advice and assistance for OIT acquisition requests.

See also: **Planning Organization**
SLC Organization
Investment Organization
Acquisition Organization

Planning Organization The OIT organization (part of the **Planning Group**) responsible for developing, communicating, and coordinating OIT's strategic plans, annual plans, performance plans, and budget submissions.

Policy A guiding principle, typically established by **Senior Management**, that is adopted by an organization or project to influence or determine decisions. Policy reflects management's expectations for actions or outcomes.

See also: **Procedure**
Process

Post-Implementation Review (PIR) A **review** conducted after the implementation of a system, by an **Evaluation Organization** independent of the project team and its support organizations, to objectively determine how well the operational system: meets Customs strategic goals and mission needs; supports the user; fulfills its intended use in a cost-effective manner; and complies with the Customs architecture, and project development processes, procedures and standards.

Preliminary Design Review See **Design Review**.

Primary Responsibility A functional **Team/Role** grouping that identifies the functional roles that perform hands-on activities or who have specific approval authority for specific tasks/activities in the Customs Standard Life Cycle.

See also: **Responsibilities**

Support Responsibility

Procedure A written description of the course of action to be taken to perform a given task or implement a **process**. It describes the "how-to" or "step-by-step" instructions needed to obtain a specified outcome.

See also: **Policy**

Process A written description of the sequence of **procedures**, **activities**, steps, events, or phases performed over time for a given purpose. It describes "what happens" or what is necessary within the organization or project to build products that meet the standards and requirements set in Customs **policy**.

Process Action Team (PAT) A team sponsored by a **Process Group** that is formed to document, develop, improve, or support the implementation of a particular **process,** discipline, or set of **procedures**.

Process Asset Library (PAL) A collection of artifacts, maintained by an organization, for use by projects in developing, tailoring, maintaining, and implementing their processes. These items include process and procedure descriptions, the organization's standard life cycle and policies, documentation templates, approved life cycle descriptions, guidelines for tailoring, examples of project- and process-related documentation and best practices. Any item that the organization considers useful in performing the activities of project management or process definition and maintenance could be included as a process asset. The current interim PAL is the OIT Toolbox.

Process Group A chartered permanent group within OIT formed to facilitate the definition, maintenance, and improvement of the **processes** and **procedures** related to a particular discipline.

See also: **Software Engineering Process Group (SEPG)**
System Acquisition Process Group (SAPG)
Infrastructure Services Process Group (ISPG)

Process Verification A **process** or **procedure** that ensures that another process is documented, that the team is following the documented process, and that appropriate artifacts and metrics are created as evidence that the documented process is followed. An outcome of the **verification** process is the accumulation of data or metrics that allows a process to be reviewed, analyzed, and improved as appropriate.

See also: **Quality Assurance**
Process Group

Production The **environment** in which current, "live" data is used to conduct tasks in support of Customs mission that involve real-time communication with the public, the business community, and other **external stakeholders**. Systems enter the Production environment following a **Production Readiness Review (PRR)** at the end of the **Acceptance Stage (Stage 6)**

and remain there during the **Operational Readiness Stage (Stage 7)** and the **Operations Stage (Stage 8)**.

Product Evaluation Team A **Project Team** subgroup that evaluates and documents **COTS** or **GOTS** applications. This team:

- Evaluates the candidate components/products to ensure that they meet mandatory user requirements, architectural standards, and appropriate domain criteria
- Documents those evaluations in a manner that will satisfy any applicable legal and/or contracting standards.

Production Notice A document or e-mail sent by the **Project Manager** with the agreement of the **Business Sponsor(s**), to the **BITR** and **users** of a system to be changed or implemented in **Operation** after the **Operational Readiness Review (ORR)**. The intent is that all affected organizations and sites shall be notified of the implementation with sufficient time to manage potential impacts.

Production Readiness Review (PRR) The meeting that occurs at the end of the **Acceptance Stage (Stage 6)** during which the **Business Sponsor**, the **Project Manager**, **Supporting Organizations**, and **Senior Management** document their concurrence that the new system may be deployed into the **Production environment**. On completion of the PRR signoffs, the **Operational Readiness Stage (Stage 7)** begins.

See also: **Reviews**

Program Monitoring Group (PMG) The OIT organization responsible for coordinating management reviews, liaison and support for external oversight organization reporting, for tracking project management performance and for formulating **audit trails** in accordance with GAO government accounting standards. Also responsible for collecting and consolidating high-level project **metrics** for OIT executive and **IMP** review.

Program Specifications A precise written description of the requirements of an individual **application** which clearly describes the process to be performed by the application. It includes statements of expected **inputs** and **outputs**, the algorithms involved in any computations, and a description of physical constraints such as execution speed or memory limitations. This documentation may include flowcharts and may also include comments within the code.

Project A group of **tasks** performed in a definable time period in order to meet a specific set of objectives. A project consumes resources, has a beginning and an end, an objective, a leader and a team, and a plan.

See also: **Customs Standard Life Cycle**

Project Change Control Board (CCB) See **Change Control Board**.

Project Concept Defines the business functions, user needs/objectives, technical alignment, and resource requirements of a desired IT system at a high-level for initial consideration. This

business need is first described in the **IT Concept Document (ITCD)** developed during the **Concept and Business Case Stage (Stage 1)**.

Project Configuration Manager See **Project CM Manager**.

Project CM Manager The person responsible for the leadership and activities of the **Project CM Team**. This individual is also a member of the **Project Management Team**.

Project CM Team The group responsible for:

- Establishing and maintaining the integrity of all the project work products and baselines in the development environment
- Identifying appropriate configuration items (CIs) so that the development environment can be re-established if necessary
- Ensuring the proper turnovers to the **OIT CM Organization**.

See also: **Project CM Manager**
Project Team
Project Librarian

Project Definition Stage (Stage 3) During this life cycle stage information created in the previous stage (Initiation) is further refined until clear sets of **user requirements** and of **functional requirements** can be produced and certified by the **Business Sponsor**. On the basis of these requirements, the technical planning and support area documentation are then created. This stage is preceded by **Initiation and Authorization (Stage 2)** and followed by the **System Design Stage (Stage 4)**.

See also: **Customs Standard Life Cycle**

Project Implementation Team A subteam defined within the overall **Project Team** if required, responsible for site planning and fielding of the system.

Project Initiation Review The Project Initiation Review ensures that the project management controls are in place and appropriate for the respective project size and complexity. The review, held at the end of the **Initiation and Authorization Stage (Stage 2)**, verifies adherence to USCS directives, SDLC policy, and IMP policy. The review team core group consists of members from the project's **Senior Management**, **Planning Group's Investment Organization**, **PMG**, **TAG** and **BIR**s. The outcome of this review would be the issuance of a **Project Work Authorization Memo**.

See also: **Reviews**

Project Initiation Team A group that consists of the **Project Manager**, **Business Sponsor**, and the personnel assigned to perform the project management, planning, and control tasks during Stages 1 and 2 of the life cycle. The members of this team are not necessarily the same group who will do the actual project development.

See also: **Project Management Team**

Project Initiation Worksheet The **IMP** document created to accompany the tailored **Project Plan** and materials for approval during the **Project Initiation Review**.

Project Librarian A member of the **Project CM Team**.

Project Management Performance Data Data that is collected and analyzed for the purpose of providing the Project Management Team with objective information on the project's status and of indicating the need for potential corrective actions early enough to influence the project results.

See also: **Metrics**

Project Management Support (Stage) While not a formal stage, the **tasks/activities** included in this "**stage**" of the **Customs Standard Life Cycle** occur during multiple **life cycle** stages throughout the duration of the project. These mandatory activities include **project planning** and budgeting activities, program/**project monitoring** activities, **requirements management**, **configuration management**, **quality assurance**, **management reviews**, and miscellaneous project support activities.

See also: **Customs Standard Life Cycle**

Project Management Team The group that consists of the **Team Leaders**, and the personnel assigned to assist the **Project Manager** in performing the project management, planning, and control tasks.

See also: **Project Plan**
Project CM Manager
Project QA Manager
Risk Manager/Coordinator/Administrator
Project Initiation Team
Executive Management Team

Project Manager The person who is responsible for the day-to-day planning, directing, controlling, structuring and motivating the project. The Project Manager is ultimately responsible to the **Business Sponsor** and **Senior Management** for the overall success of the project, and for meeting cost, schedule, and quality goals.

Project Monitoring The set of tasks and responsibilities that ensure that:

- All projects track and control project progress in an objective, proactive manner
- Project results, changes, and commitments are communicated to all interested groups, including **Senior Management**

See also: **Project Planning**
Project Management Team

Project Plan A management document describing the approach that will be taken for a project. It typically describes the work to be done, resources required, the methods to be used, and the milestones and schedules to be met. It is **baselined** in the **System Design Stage**

(Stage 4) and thereafter used to track and predict progress on the project. The Project Plan may sometimes be referred to as the Software Development Plan (in CMM® terms).

See also: **Initial Project Plan**
Project Status Meeting
Project Management Team

Project Planner A member of the **Project Management Team** who is responsible for updating and maintaining the **Project Plan**.

Project Planning The set of tasks and responsibilities that ensure that

- Resources, capabilities, costs, and constraints are accounted for and are traceable
- A documented plan is produced, agreed to, and used for tracking the project

See also: **Project Monitoring**
Project Plan
Project Management Team

Project Quality Assurance The planned and systematic approach to assessing, monitoring, and improving the quality of a project's work products. It includes methodical processes for internal Project technical **reviews**, **walkthroughs**, and **audits** of the **work products** and the **procedures** and **processes** used to produce them.

See also: **Project QA Team**
Project QA Manager
Quality Assurance

Project QA Manager The person responsible for the leadership and activities of the **Project QA Team**. This individual is also a member of the **Project Management Team** and is responsible for reporting to them on QA results.

Project QA Team The group on the Project responsible for:

- Formal monitoring of various work products of the project to ensure that standards, policies and regulations are being met
- Reviewing requirements and project plans to ensure that project quality concerns are being accounted for
- Monitoring the compliance and effectiveness of the processes being used on the project

See also: **Project QA Manager**
Project Team
Project Quality Assurance
Quality Assurance Plan
Quality Requirements

Project Risks Any risks that can potentially impact a project's cost, schedule, or product quality in a negative manner. These can include technical, management, maintainability, and programmatic risks or **issues**. Plans can be made to track and mitigate identified risks so that they do not develop into unexpected problems.

See also: **Risk**

Risk Analysis
Risk Management
Risk Mitigation
Security Risks

Project Security Manager The person responsible for the leadership and activities of the **Project Security Team**. This person may also be assigned as the **Computer Security Officer (CSO)**.

Project Security Team Members of the **Project Team** with the responsibility for:

- Monitoring and overseeing that the appropriate level of security is incorporated into an application's hardware and software as it is being designed/developed/acquired
- Ensuring that appropriate consideration is also given to personnel security, physical security, information security, etc. in relation to the system/project
- Monitoring and overseeing the appropriate level of security while an application remains operational and/or is being modified
- Providing the project with expertise in various aspects of security, including computer security, communications security, emissions security, and network security.

See also: **Security Requirements**
Computer Security Officer (CSO)
OIT Security Organization
Information Security

Project Status Meeting A regularly scheduled **review** held by the **Project Manager** with the individuals who are directly responsible for the day-to-day detailed results of the project.

See also: **Project Team**

Project Tailoring Review One of a series of reviews held by the Project to ensure that key parties agree with the proposed tailored **Project Plan**, deliverables, and schedule. Because projects must create their own Project Plan from SDLC guidance (by **tailoring**), this review validates proper tailoring. Participants include the project's **Senior Management**, **Business Sponsor, BIR**, affected **Support Organizations**, the **Evaluation Team**, **PMG**, **TAG**, and the **SLC Organization**.

See also: **Reviews**

Project Team The group responsible for ALL activities in a project. This group includes the following subgroups, which may share the services of the same individuals:

- **Development Team**
- **Project Implementation Team**
- **Project Management Team**
- **Project QA Team**
- **Project CM Team**
- **Project Security Team**
- **Product Evaluation Team**
- Designated members of **Support Organizations**

Project Tracking The process of monitoring **Project Management Performance Data** to ensure that the project meets the cost, time, and quality objectives that are identified in the planning phases.

See also: **Project Status Meetings**
Project Monitoring

Project Work Authorization Memo Issuance of the Project Work Authorization Memo marks the point at which the project is authorized to begin project engineering, development, and detailed definition work. This document is issued after the **Project Initiation Review** at the end of the **Initiation and Authorization Stage (Stage 2)** and/or whenever new funding is authorized. The memo is issued by the Director of the Planning Group and indicates that the project is approved to proceed to the **Project Definition Stage (Stage 3)**. The memo may also contain corrective actions, special directions and restrictions

Quality

1. The degree to which a system, component, or process meets specified requirements.
2. The degree to which a system, component, or process meets customer or user needs or expectations.

See also: **Quality Assurance**
Quality Requirements

Quality Assurance (QA)

1. The management of defined activities that are in place throughout the life cycle to ensure that user requirements are met, processes are documented and followed, products are compliant with standards, and interim deliverables are fit for use.
2. All the actions necessary to ensure the quality of the work products, documentation, and processes.

QA verifies that **work products**, **procedures**, and **processes** comply with applicable, documented standards, as well as provides the **Project Team**, **Project Managers**, and **Senior Management** with the results of these reviews and audits. QA activities include internal **reviews** and **audits** as well as **independent reviews** by external organizations.

See also: **Project QA Team**
Project QA Manager
Project Quality Assurance
OIT QA Organization

Quality Assurance Plan The document that specifies the strategies, procedures, staff organizational responsibilities, and schedule for project activities that will be performed to provide visibility into both the products being built and the processes used by the project. For smaller projects, this information may be included within the Project Plan.

See also: **Project QA Team**
Project Quality Assurance
Project Definition Stage (Stage 3)

Quality Requirements Requirements relating to the quality of the system to be developed including usability, maintainability, performance, portability, etc.

See also: **Functional Requirements**

Rebaseline To reestablish a defined and approved point from which the affected plan or configuration item can be modified in the future. Both the prior version and the new version are held for historical use with lessons learned, the change rationales, and new assumptions and estimates.

See also: **Baseline**
Configuration Management
Project Planning

Release Plan A Release Plan provides a clear definition of each release of functionality groupings for a project. It includes the functionality to be included as part of each release, a description of how each release will interact/change and interface with other releases, a cost/benefit analysis of each release, and projected dates of implementation. For smaller projects this information may be included in a high-level **Project Plan**, or **Project Concept** document.

Requirements The various user and IT needs that determine the capabilities and design of a system. These may include: system function or procedural changes, new hardware or firmware functionality, or new or revised operational or supporting capabilities. They are the difference between an existing system or operation and a proposed system or operation.

See also: **Functional Requirements**
User Requirements

Requirements Certification

1. The activity of reviewing and approving the documented **User Requirements** and the **Functional Requirements**. The certifying authorities are the **Business Sponsor** and the **Project Manager**.
2. Also used to refer to the certification statement itself which documents the acceptance and approval of the defined requirements.

Requirements Management The process of capturing, tracing, and maintaining **requirements** for software, hardware, services, and documentation for both applications and infrastructure. **User Requirements** and **Functional Requirements** are gathered in a **Requirements Traceability Matrix (RTM)**.

See also: **Change Management**

Requirements, Changed Revised **requirements** where the original requirements were **baselined** and where the modifications or enhancements were identified by activities including prototyping, reviews, user-generated updates, changes mandated by law, and team-generated corrections.

Requirements, New Additional **requirements** discovered or identified after the requirements have been **baselined** and certified.

Requirements Traceability Matrix (RTM) A document that is created during the **Project Definition Stage (Stage 3)** from the requirements identified in the **User Requirements** and the **Functional Requirements**. The RTM is used and updated through the subsequent life cycle stages to ensure that each requirement can be mapped through design, development, testing, and operations.

Responsibilities A high-level description of the general tasks or activities for which a **Team/Role** is accountable as part of the **Customs Standard Life Cycle**.

See also: **Primary Responsibility**
Support Responsibility

Resource Management Group (RMG) The organization within OIT responsible for facilities management and logistical support for all OIT activities, budget execution and support, and human resources and OIT staff training activities.

Retirement Stage (Stage 9) The lifecycle stage where, when a system no longer meets Customs needs, its existence is terminated and any data or modules not needed by replacement systems are archived and stored in a secure off-site location. This stage is preceded by the **Operations Stage (Stage 8)**.

See also: **Customs Standard Life Cycle**

Retirement Project Plan A **Project Plan** covering the activities needed to remove a system from **Production**. This plan is developed when the retiring system is not being replaced by a new system. If the system is being replaced, these activities should be included as part of the Project Plan for the new system.

Review A meeting, which may be formal or informal, for the purpose of determining the status of a project or work product. Completion of a review may be documented through agendas and minutes or through specific signoffs, certifications, or memos.

See also: **Project Status Meeting**
Senior Management
Formal Review
Work Product Review
Peer Review
Walkthrough
Design Review
Project Tailoring Review
Project Initiation Review
Requirements Certification
Definition Phase Completion Review
Critical Design Review (CDR)

Test Readiness Review (TRR)
Production Readiness Review (PRR)
Operational Readiness Review (OPR)
Post-Implementation Review (PIR)

Risk Any potential loss to Customs. Risks include both **Project Risks** and **Security Risks**. Examples of possible risks include poorly understood requirements, unfamiliar technology, limited resources, and/or the potential for unauthorized access to data.

See also: **Risk Analysis**
Risk Management
Risk Mitigation

Risk Analysis The process of identifying project and security risks, determining their magnitude, and identifying areas needing safeguards. This can be done by an analysis of an organization's information resources, its existing controls, potential project problems, and its remaining organizational and AIS vulnerabilities.

See also: **Project Risks**
Security Risks
Risk Manager/Coordinator/Administrator
Risk Management
Security Risk Assessment

Risk Management The process of identifying, assessing, prioritizing, documenting, tracking, mitigating, reviewing, and communicating risk information to reduce or avoid problems and negative impacts on a project.

See also: **Risk Manager/Coordinator/Administrator**
Risk Analysis
Risk Mitigation
Project Risks
Security Risks

Risk Manager/Coordinator/Administrator A member of the **Project Management Team** responsible for tracking and reporting on risk priorities and the status of risk mitigation plans and action items. This person may also be responsible for coordinating risk management review meetings for the project on a regular basis.

See also: **Risk Analysis**
Risk Management
Risk Mitigation

Risk Mitigation The process of developing and implementing plans to eliminate or avoid the majority of the negative impacts anticipated if a risk manifests as a problem.

See also: **Project Risks**
Security Risks
Risk Management
Security Risk Assessment

Schedule A document that uses the WBS tasks, task effort estimates, staff availability, and critical dependencies and interweaves them to create the most efficient plan of accomplishments over time. This timeline is often depicted graphically and is used to track completion of project activities and milestones. A schedule is one key part of the Project Plan.

See also: **Work Breakdown Structure (WBS)**
Milestone
Task

Scope The range of functionality to be covered or supported by a specified work product.

See also: **Requirements**

SDLC Assist Visit The SLC Organization actively assists projects in understanding the Systems Development Life Cycle (SDLC) in order to create their tailored Project Plan. These SDLC Assist Visits may also include representatives from the Investment Organization and Evaluation Organization.

See also **Tailoring**

Security The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

See also: **Computer Security Officer (CSO)**
Risk
OIT Security Organization

Security Accreditation See **Security Accreditation Statement**.

Security Accreditation Statement Senior management's acceptance of the **Security Certification**. By signing the accreditation statement, the **Designated Approval Authority (DAA)**, who in Customs is the AC/OIT:

- Approves the Security Certification
- Accepts all residual **security risks**
- Authorizes the IT application and/or infrastructure system to become operational

Security Certification A Security Certification is a sign-off by the **Computer Security Officer (CSO)** and the **Information Systems Security Manager (ISSM)** that the security aspects of a proposed IT application or infrastructure system:

- Meet the defined **security requirements** for that system
- Are in compliance with all applicable policies and directives; and
- Are reasonable, appropriate, and sufficient for the planned operational environment.

Certification must be complete prior to using any **Production** data.

See also: **Security Accreditation**

Security Control Physical, environmental, hardware, software, communications, administrative or procedural measure in place to restrict access or prevent the unauthorized destruction, damage, disclosure or denial of use of AIS resources.

Security Conversion Plan A security plan detailing how data removed from Production when a system is retired will be safeguarded and stored. If the system is being replaced, this information should be part of the new system's Security Plan.

Security Features User's Guide A document that describes the security features provided by the system, how to use them, and how they interact with one another. It is drafted during the **Construction Stage (Stage 5)** and completed during the **Acceptance Stage (Stage 6)**. The **Project Security Team** has primary responsibility for its content and production in consultation with the **Training Organization**.

Security Plan A document updated during the entire life cycle, that ensures development and implementation of security measures for the system under development.

Security Requirements Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policies.

See also: **Project Security Team**
Functional Requirements

Security Risk Assessment This defines the extent to which the system, application, and the data it processes are or will be at risk. The document, created by the **Project Security Team**, includes defining and valuing the assets, defining threats to those assets, determining the system's **vulnerabilities**, and recommending reasonable safeguards and controls to bring the risks down to acceptable levels.

See also: **Risk**
Risk Analysis
Risk Mitigation
Security Risks
Major Application

Security Risks Security risks focus primarily on concerns relating to the electronic data. These may involve unauthorized disclosure, unauthorized data modification, the loss of information resources, and/or unacceptable delays in data availability. Security risks can also involve unauthorized access to or authorized but improper use of computer resources.

See also: **Risk**
Risk Analysis
Risk Management
Risk Mitigation
Project Risks

Security Test Plan A document that defines the planned activities, test data, and acceptance criteria for testing the security features of the delivered system. This plan may be combined with the **System Test Plan**.

See also: **Security Testing**

Security Testing Testing, conducted by the **Project Security Team** that:

- Evaluates compliance of the product with security and data integrity guidelines, including security backup, recovery and audit trails
- Ensures that all security measures have been properly implemented in the operating environment and are effective in satisfying security requirements
- Accounts for all aspects of security to include internal controls, physical and environmental security, and administrative procedural security requirements

See also: **Security Test Plan**
System Acceptance Test Plan

Senior Management A management and oversight functional role at a high enough level above the **Project Manager** that the primary focus of the person filling the role is the long-term vitality of the organization, rather than short-term project and contractual concerns and pressures. These individuals have the authority to direct the allocation or reallocation of resources in support of organizational goals, and they direct the work of one or more subordinate Projects/Project Managers. This role may be performed by a Branch Chief, Division Director, or higher-level manager depending on the organizational structure to which the Project/ Project Manager reports.

See also: **Team/Role**
Reviews

Sensitive Information A category of unclassified Government controlled information.

Reference: *Information Systems Security Policy and Procedures Handbook*, CIS HB 1400-05A.

Short List A list of three to four **commercial off-the-shelf (COTS)** products that can satisfy a specified business need. When the technology insertion process begins, there may be many COTS products that can satisfy a business need. The short list is selected by researching the market place and eliminating those products that do not fit Customs **technical reference model** and/or business need.

Software The programs, languages, and/or routines that control the operations of a computer in solving a given problem.

See also: **Application**

Software Development Division (SDD) The division within OIT responsible for the design, development, and maintenance of software applications developed by or for the United States Customs Service.

Software Engineering Process Group (SEPG) A chartered organization within OIT formed to facilitate the definition, maintenance, and improvement of the OIT **processes** and **procedures** related to the discipline of Software Engineering. It provides recommendations to its oversight body, the **Management Steering Committee (MSC)**. It guides and assists other groups and projects within OIT with software process improvement tasks and activities.

See also: **Process Group**

Solution Proposal Assessment An examination of a proposed solution in an **ITCD** and/or **Business Case**, at a high level, to determine the level of impact on the Customs technology **environment**.

Stage A set of related tasks on a project, grouped at an intermediate level of detail in the work breakdown structure. The division of a project into stages is governed by the **life cycle** model.

See also: **Customs Standard Life Cycle**

Stakeholder, External

1. All interested parties outside of the **Project Team**, including **Users**, the **Business Sponsor**, and all **Support Organizations**

2. Users/customers outside of Customs who depend on Customs data collection and data processing for all or part of their business activities.

   See also: **Stakeholder, Internal**

Stakeholder, Internal

1. All individuals and interested parties within the **Project Team**

2. Users/customers within Customs who depend on a specific system for all or part of their mission-critical activities.

   See also: **Stakeholder, External**

Standards Specifications with which a product or service must comply, providing a disciplined uniform approach to development and evaluative measures for acceptance.

Statement of Work (SOW) A description of all the work required to complete a project, which is provided by the customer to a contractor and forms the basis of a contractual agreement.

See also: **Acquisition Plan**

Subcontractor For Customs, this term refers to both contractors and subcontractors who provide services for Customs, whether independently or, more commonly, as an integral part of a Customs **team**. In CMM terms, the term "subcontractor" refers only to those who independently manage themselves to develop and turn over a completed product, rather than those non-Federal employees who are integrated into a Customs team environment.

Support Organizations All those organizations who assist the system development effort by performing the ancillary tasks associated with creating or maintaining systems. This includes individuals, groups, or teams performing required functional roles such as Networks, Database Administration, Middleware, CM, and other ISD Engineering and Operations Support Team roles. In addition, where not critically called out or mandated as a separate organizational responsibility for an activity, Support Organizations also include Training, Testing, Security, and staff functions.

See also: **Training Organization**
Testing Organization
Data Management Organization
OIT Security Organization
OIT CM Organization
OIT QA Organization
Infrastructure Services Division (ISD)
Technology and Architecture Group (TAG)
Planning Group (PG)
Program Monitoring Group (PMG)
Resource Management Group (RMG)

Support Responsibility A functional role grouping that identifies those who provide assistance, reviews, and concurrence with results/outputs. Also includes sources that the project can tap for expert advice.

See also: **Responsibilities**
Primary Responsibility

System A collection of components organized to accomplish a specific function or set of functions.

See also: **Application**
Information Technology

System Acceptance Test **Independent testing** to ensure a system meets the **user and functional requirements** (including **security acceptance testing**).

See also: **System Testing**
Testers
Testing Organization

System Acceptance Test Plan A document, created and used by the **Testing Organization**, that defines the testing activities to be performed, test data, and acceptance criteria for testing the delivered modules and system. It will include **security acceptance testing** as needed. It may also include **test cases/scenarios** or those may be separately defined and used to record test results.

See also: **System Test Plan**

System Acquisition Process Group (SAPG) A chartered organization within OIT formed to facilitate the definition, maintenance, and improvement of the OIT **processes** and **procedures**

related to the discipline of system acquisition. It provides recommendations to its oversight body, the **Management Steering Committee (MSC)**. It guides and assists other groups and projects within OIT with system acquisition process improvement tasks and activities.

See also: **Process Group**
Customs Modernization Office (CMO)
Applied Technology Division (ATD)
Office of Finance, Procurement Division (OFPD)
Acquisition Organization

System Cut-Over Plan This plan identifies all activities relating to the removal of software from **Production,** including notification of **users**. If a system is being replaced, this information would be part of the new system's **Implementation** and/or **Deployment Plans.**

System Design A document or set of documents that provide a detailed description of how the system will work. It includes:

- A description of the technical approach and security features used for the target architecture
- An identification of all programs and other software components associated with a particular application
- A description of how the programs interact with other applications and specific database(s).

System Design Security Officer (SDSO) A project's point-of-contact within **ISSB** who provides advice concerning IT security policies, procedures, requirements, documents, and issues as appropriate for each project.

System Design Stage (Stage 4) During this stage the **Development Team** uses the **Requirements** to create the technical design of the system to be developed. This phase ends with a Critical Design Review (CDR), in which the **Business Sponsor** reviews the work products and certifies that the development team design meets the business need. This stage is preceded by **the Project Initiation Stage (Stage 3)** and is followed by the **Construction Stage (Stage 5)**.

See also: **Customs Standard Life Cycle**

System Performance See **Performance Measures**.

System Test Plan A document, created and used by the **Development Team**, that defines the planned activities, test data, and acceptance criteria for testing the delivered modules and system. It may be combined with the **Security Test Plan**. It may also include the **test cases/ scenarios** developed to meet the user acceptance criteria or those may be separately defined and used to record test results.

See also: **System Acceptance Test Plan**
Project Definition Stage (Stage 3)

System Testing Testing, conducted by independent **Testers**, to determine whether all elements of the system interface properly and satisfy overall system function and performance objectives.

See also: **Integration Testing**
Unit Testing
Security Testing
System Acceptance Test
User Acceptance Testing

Systems Development Life Cycle (SDLC) The Customs SDLC Handbook. Also it is the all-encompassing term for management's statement of policies, approved life cycles, high-level processes, and standards which apply to system development.

See also: **Customs Standard Life Cycle**

Systems Life Cycle (SLC) Organization The OIT organization (part of the **Planning Group**) that is responsible for the development and maintenance of system life cycles, including support and advice to projects. They also provide CMM® and life cycle policy expertise and support and assistance the **Enterprise Process Improvement Program (EPIP)**, OIT's process improvement **Management Steering Committee (MSC)**, **Projects**, and **Process Groups** (e.g., the SEPG).

Tailoring

1. Modifying a Customs standard or model life cycle process, activity, or document format for use on a particular project. Project tailoring must be done formally, documented, and approved by **Senior Management**.

   See also: **Project Tailoring Review**

2. For COTS products, refers to altering the product's functionality or outputs without altering the product's source code.

   See also: **Customization**

Task A well-defined unit of work for one or more persons on a project. A task should have a measurable end. It is commonly used to describe a significant activity which is decomposed to another level.

See also: **Activity**

Team A collection of people, often drawn from diverse but related groups, assigned to perform a well-defined function for an organization or a project.

See also: **Team/Role**
Team Leader

Team/Role A functional grouping used within the **Customs Standard Life Cycle** to associate **Responsibilities** descriptions with **Primary Responsibility** and **Support Responsibilities**.

See also: **Team**

Team Leader

Team Leader The person responsible for leading a collection of people, often drawn from diverse but related groups, assigned to perform a specific set of tasks for the project. Team Leaders may also be members of the **Project Management Team**.

See also: **Team**
Team/Role

Technical Compliance Reviews Reviews by the Technology and Architecture Group to verify that the technology of the solution proposed is in compliance with enterprise standards, architecture (information, data, applications, knowledge, technology) and methodology (software development, data definitions, network design) as defined by the **TRM**.

Technical Reference Model (TRM) A generally-accepted representation of the generic components of an information system. It describes the main components of a complete information system as a set of services categorized by functional area. The TRM includes the hardware and software products approved for use at Customs.

Technology and Architecture Group (TAG) The OIT organization responsible for the functional architecture, work architecture, information architecture, and infrastructure architecture and their related processes. They provide analytical and administrative support to the TRC and perform architecture and post-implementation system evaluations. They also assist projects in the **Concept and Business Stage (Stage 1)** and the **Initiation and Authorization Stage (Stage 2)**.

See also: **Post-Implementation Review (PIR)**
Enterprise Architecture
Support Organizations
Evaluation Organization
Architecture Organization

Technology Review Committee (TRC) The management group responsible for ensuring that proposed projects support and comply with Customs **Enterprise Architecture**. They also verify that projects are supportable and do not duplicate existing systems. TRC activities occur during the **Concept and Business Case Stage (Stage 1)**.

See also: **Investment Management Process (IMP)**

Test Case/Scenario A document that specifies the test(s) to be accomplished, the expected results, and may also include the actual results for each specific identified project, function, module, screen, and requirement to be validated according to the **Test Plan**.

See also: **Test Script**

Test Plan A document that is a formal specification and is used to guide the conduct of a test. It is used to construct the **Test Case/Scenario** document.

See also: **System Test Plan**

Security Test Plan
System Acceptance Test Plan

Test Readiness Review (TRR) The meeting that occurs at the end of the **Construction Stage (Stage 5)** during which the **Testers**, the **Project Manager**, **Supporting Organizations**, and **Senior Management** document their concurrence that the new system is ready for **independent testing**. On completion of the TRR signoffs, the **Acceptance Stage (Stage 6)** begins.

See also: **Reviews**
Tests
System Acceptance Test Plan

Test Script The detailed, complete specification of all aspects of a test including test initialization, data structures, keystrokes, other inputs, expected outcomes and validation criteria.

See also: **Test Case/Scenario**
Test Plan

Testers Members of the **Testing Organization** or other individuals who are independent of the Developers of the product and perform **independent testing**. They are responsible for verifying that system functions, as defined by the requirements and design documentation, perform as expected. Their testing and verification activities are performed in accordance with a **Test Plan**, using **Test Cases/Scenarios** whose details are specified in a **Test Script**. Their planning activities take place during early stages of the life cycle and their testing activities take place during the **Acceptance Stage (Stage 6)**.

See also: **Tests**

Testing Organization The OIT organization responsible for independent **system testing** and **security testing** for all application systems to be implemented in the Customs **Production** environment.

See also: **Independent Testing**
Testers

Tests The process of determining that a system, subsystem, module or other portion of a system meets specified criteria.

See also: **Independent Testing**
Integration Testing
System Testing
Unit Testing
System Acceptance Test
User Acceptance Testing

Trainer A member of the **Training Organization** or other qualified individual who performs **training** activities.

Training Training is the provision of materials and opportunities to assist an individual in learning facts, concepts, processes, procedures, or principles.

See also: **Training Organization**

Training Organization The OIT organization that is responsible for the **training** of the **end-users** of **applications**. It prepares **user documentation and training materials** and trains both new and experienced users on the application being built, purchased, updated or integrated. It also arranges logistics, develops schedules and coordinates training requirements with users and **Project Team** members.

See also: **Support Organizations**
Training Plan
Training Requirements

Training Plan A document that is created by the **Training Organization** during the **System Design Stage (Stage 4)**, based on the approved **Training Requirements** document. It is activated during the **Construction Stage (Stage 5)** with the creation of draft **User Documentation and Training Materials**, finalized for the **Test Readiness Review (TRR)**, and fully implemented during the **Operations Stage (Stage 8)**.

Training Requirements A document that is created by the **Training Organization** during the **Project Definition Stage (Stage 3)**. It is based on the **User Requirements** and **Functional Requirements** and may include additional input from the **Business Sponsor**. This document, approved by the Business Sponsor, provides the primary input to the **Training Plan**.

Trusted Facility Manual (TFM) A document developed by the **Project Security Team**. It presents cautions about functions/privileges that should be controlled when running a secure facility and procedures for examining and maintaining **audit trails** (including the audit trail record structure).

Turnover Package A collection of work products gathered into one deliverable used to facilitate the transfer of the project from one life cycle stage to another. The turnover package includes all work products to-date, whether in draft or final form. The Test Readiness Review (TRR) Package is often specifically referred to as the Turnover Package.

See also: **Test Readiness Review (TRR)**
Production Readiness Review (PRR)
Operational Readiness Review (ORR)
Project Initiation Review
Definition Phase Completion Review

Unit Testing Testing performed by the **Development Team** during the **Construction Stage (Stage 5)** in order to verify the code or changes to the code within a particular module or subroutine. This is the lowest level of testing that can be done on a code module or unit.

See also: **Integration Testing**
System Testing

Up-Front Costs Those cost items which occur at the beginning of a product's life cycle within the Customs environment.

See also: **On-going Costs**

User

1. Anyone who uses automated systems developed by or for the United States Customs Service.
2. Representatives of the user community who provide input in the development of automated systems.

The User is often referred to as the **end-user**, and is represented in the development life cycle by the **Business Sponsor** and **BITR**.

User Acceptance Testing **Independent testing** performed by the Users or their representative to ensure a system meets the **user requirements**.

User Acceptance Testing Sign-off The document signed by the **Business Sponsor** to indicate that the system meets the User Requirements and should be moved to **Production**. At the Business Sponsor's discretion, this may be signed based on **System Acceptance Test** results whether or not the **users** independently perform additional tests.

User Documentation and Training Materials Documents, files, applications or other materials that are developed by the **Training Organization** in accord with the principles of Instructional Systems Design and the **Customs Standard Life Cycle** for the purpose of providing training or training support to the Customs **end-users** of **applications** built, purchased, updated or integrated by Customs. These materials may include: user guides, quick reference guides, instructor-led training, online help, computer-based training, web-based training, audio or video conferences, or other training products. They are built and delivered, according to the design specified in the **Training Plan**, beginning in the **Construction Stage (Stage 5)** and continuing through the **Operations Stage (Stage 8)**.

User Requirements The document that is initially created in the **Initiation and Authorization Stage (Stage 2)** by the **Business Sponsor** and the **users** and completed in the **Project Definition Stage (Stage 3)**. It defines the user needs and forms the basis, along with the **Functional Requirements** document, of the **System Design**.

User Signoff/Certification of Acceptance This document is the **Business Sponsor's** certification that everything moved to **production** operates correctly and the system meets the user's needs. This signoff occurs as part of the **Operational Readiness Review (ORR)**.

Validation The process of evaluating systems at the end of the development process to ensure compliance with system requirements and to demonstrate that the product will actually meet its intended use in its intended environment. Validation occurs during the **Acceptance Stage (Stage 6)** to assure that "you built the right thing".

Verification The process of determining whether or not the products of a given phase of the development cycle fulfill the requirements. The act of reviewing, inspecting, testing, checking, auditing, or documenting whether items, processes, or documents conform to specified requirements. Verification occurs during every stage of the **Customs Standard Life Cycle** to assure that "you built it right".

See also: **Quality Assurance**

Vulnerability A weakness in a telecommunications system, automated information system, cryptographic system, or security procedures, hardware design, internal controls, etc., that could be exploited to gain unauthorized access to **sensitive information**.

See also: **Security Risk Assessment**

Walkthrough A structured meeting to review the completeness and quality of selected documents, designs, module(s) of the system, or of the entire system. A walkthrough is usually less formal than a peer review.

See also: **Peer Review**
Reviews

Work Breakdown Structure (WBS) A logical, hierarchical list of tasks for the project, consisting of various levels of detail which may include phases and steps as intermediate levels. Work breakdown structures are usually drawn with the top block representing the project objectives and the lowest level representing the tasks.

See also: **Task**
Schedule

Work Product Any intermediate or final product, service, or result of a process or activity. This includes plans, software code, documentation, and systems.

Work Product Review Work Product Reviews occur after major work products are completed to clarify understanding of and agreement with the substance of the work product under review, hand off the product from one group to another, and gain approval/acceptance of the item. All stakeholders with interest in the item may participate.

See also: **Reviews**

Appendix B
Roles and Responsibilities

B.1 Introduction

This appendix identifies the roles and responsibilities as they apply to and support projects and systems within the context of the Customs Standard Life Cycle. These responsibilities are the same as those listed in the Customs Standard Life Cycle in Chapter 4, where they are grouped by task/activity. They are grouped here by role for the convenience of the reader.

There are three categories of "roles" defined in this appendix. Within each category, roles are listed alphabetically. The categories are:

1. **Standing Organizations:** These are functional organizations or groups outside of a project that provide an ongoing service to all projects, applications, and/or users. They may be either primary organizational entities or part-time committees. They may be either actual or virtual groups that perform these functions. Existing organization titles may not match precisely due to recent or future reorganizations of those functions.

   Examples: Testing Organization, OIT Security Organization, Support Organizations

2. **Project-Specific Teams:** Project-Specific Teams are the defined functional teams within a specified project. They are concerned with the management, technical activities, and tasks involved in the actual development or maintenance of systems. Each Project-Specific Team is unique to the specified project and could be a part-time or full-time job for one or more of the Project Team members depending on the project's scope and complexity.

   Examples: Development Team, Project CM Team, Project Security Team

3. **Individual Project Roles:** These are the individual duties or functions associated within a specified project. This includes various managers, experts, liaisons, and support personnel. As with Project-Specific Teams, each role could be a part-time or full-time job for one or more of the Project Team members depending on the project scope and complexity. Also, one person may be assigned multiple Individual Project Roles.

   Examples: Project Manager, Business Sponsor, Tester, Developer, User

Notes:

1. These are functional definitions. They are not necessarily job titles, contract labor categories, nor organizational entity names (although some may be the same or similar). Each project may implement these functional roles in different ways. One person may perform multiple functions.

2. Some Individual Project Roles may duplicate the responsibilities of a Standing Organization or Project-Specific Team. In those cases, the Individual Project Role is grouped with the Team or Organization's description to avoid duplication of information in the responsibility tables.

   Examples:

   - The Individual Project Role of "Trainer" is grouped with the Standing Organization Team called "Training Organization (Branch)".

   - The Individual Project Role of "Team Leader" is grouped with the Project-Specific Team called "Project Management Team".

B.2 Standing Organization Responsibilities

Organization	Description	Standard Life Cycle Responsibilities[5]	
		Primary	Support
Acquisition Organization	The organization within OIT (part of the Planning Group) that serves as the primary interface between application developers and the Procurement Division in the Office of Finance (OPFD).	Initiation and Authorization • Develop Acquisition Plan Project Definition • Acquire Project Systems/Services Project Management Support • Contractor/Subcontractor Management	Concept and Business Case • Create Project Concept • Create Business Case Initiation and Authorization • Create Initial Project Plan Project Management Support • Negotiate, Update and Rebaseline Project Plans, Agreements, and Documents
Architecture Organization	The part of TAG responsible for all activities relating to the development, implementation, and management of Customs architectures and technology domains. This includes maintenance of the Enterprise Architecture Repository and Technical Reference Model. They also facilitate and support the TRC.	Concept and Business Case • Review High-level Business Alignment and Architecture	Concept and Business Case • Create Project Concept • Identify COTS/GOTS, etc. for further Application Product Evaluations Operations • Evaluate and Upgrade Systems Software/COTS • Analyze and Install Hardware/Firmware Upgrades Project Management Support • Conduct SDLC and Architectural Compliance Reviews

[5] Primary responsibilities include those who perform hands-on activities or who have specific approval authority; support responsibilities include assistance, reviews, and concurrence with results/outputs. Support responsibilities also include being a source that the project can tap for expert advice on a specific task/activity.

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Capacity Planning Organization	The OIT organization responsible for monitoring computer resource usage by various applications and notifying Senior Management when the resource usage reaches a level where the service level agreements cannot be met.	Operations • Capacity Planning and Replanning	
Data Management Organization	The organization(s) within OIT with the following responsibilities: • Creation and maintenance of the logical and physical data models • Generation of Data Definition Language statements • Technical design and management of the physical database and database objects • Evaluation, selection, and implementation of the data dictionary and database catalog • Management, administration, and performance of the Database Management System (DBMS) software.	System Design • Create Detailed System Design • Conduct Peer Reviews and Detailed Design Reviews Construction • Construct Infrastructure • Conduct Test Readiness Review (TRR) Operational Readiness • Convert Data • Move to Production Environment	Project Definition • Prepare Support Area (Data Management) Plans System Design • Baseline Design (Data Management Plan) Retirement • Develop Data Conservation/Conversion Plan
Designated Approval Authority (DAA)	The individual appointed by the Commissioner of Customs to exercise authority and assume formal responsibility for operating all Customs systems at an acceptable level of risk. **Note:** Currently the DAA is the AC, OIT.	Acceptance • Approval of Security Accreditation	

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Division Directors (DD)	An executive level manager of an operational division who reports to the AC, OIT.	Acceptance • Conduct Production Readiness Review (PRR) Operational Readiness • Conduct Operational Readiness Review (ORR) Retirement • Review and Verify Removal Plans Project Management Support • Ongoing Project Oversight	Initiation and Authorization • Perform Project Initiation Review System Design • Conduct Project Review with Senior Management/DD Project Management Support • Prepare/Conduct Senior Management Reviews
Evaluation Organization	The Evaluation Organization is an OIT organization (part of TAG) that is responsible for the formal monitoring of various work products. It ensures that standards, policies, regulations, and anticipated benefits are being met. Responsibilities include performing evaluations, SDLC/Compliance Audits, Technical Architecture Compliance Audits, and Post-Implementation Reviews (PIRs).	Concept and Business Case • Review High-level Business Alignment and Architecture Operational Readiness • Prepare/Document Lessons Learned Operations • Post-Implementation Evaluations Project Management Support • Conduct SDLC and Architectural Compliance Reviews	Concept and Business Case • Create Business Case Initiation and Authorization • Select Appropriate Life Cycle and Identify Tasks/Deliverables • Create Initial Project Plan • Conduct Project Tailoring Reviews Project Management Support • Perform Quality Assurance • Ongoing Project Oversight
Help Desk Organization	The OIT group responsible for documenting, routing, and tracking *reported* incidents and problems until they are resolved and the originator is notified.	Operations • Manage Production Problem Reports	

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Information Systems Security Manager (ISSM)	An OIT-assigned role that has the following responsibilities: • Responsible for the Customs-wide IS security program • Coordinates with and provides leadership to an infrastructure of appointed security personnel, including the CSOs and System Design Security Officers (SDSOs) **Note:** Currently the ISSM is the Head of the Information Systems Security Branch.	Acceptance • Approval of Security Certification package	
Information Technology Committee (ITC)	A review committee composed of OIT Senior Management and the Business Information Technology Representatives (BITRs) responsible for ensuring proposed projects are sound and prudent business investments.	Concept and Business Case • ITC Approval Process Project Management Support • Ongoing Project Oversight	
Infrastructure Services Division (ISD) ISD Support Teams	The division within OIT responsible for implementation and support of the Customs information infrastructure, supporting development including engineering and operation of all platforms, management of the Customs network and communications functions, database administration for all platforms and desktop support for all users of Customs automated systems. **Note:** Also see responsibilities listed for: Support Organizations Capacity Planning Organization Help Desk Organization	Initiation and Authorization • Create Infrastructure Plan Project Definition • Acquire Project Systems/Services Construction • Establish Working Environments • Construct Infrastructure • Create System Acceptance Test Plan Acceptance • Prepare/Update Test Cases • Finalize System Acceptance Test Plan • Conduct System Acceptance Test (SAT) • Prepare Production-Ready	Concept and Business Case • Create Project Concept • Review High-level Business Alignment and Architecture • Create Business Case Initiation and Authorization • Conduct Project Tailoring Reviews Project Definition • Walkthrough Functional Requirements • Conduct Support Organization Interface Meeting(s) System Design • Create Preliminary

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
		Environment	System Design

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	**Support**
Infrastructure Services Division (ISD) ISD Support Teams (Continued)		Acceptance (continued) • Prepare Testing Organization's SAT Reports Operational Readiness • Move to Production Environment • Evaluate Disaster Recovery and Contingency Plans Operations • Monitor Performance • Ensure Continuous Operations • Analyze Problem Reports • Evaluate and Upgrade Systems Software/COTS • Analyze and Install Hardware/Firmware Upgrades • Document Operational Lessons Learned Retirement • Remove Programs/ Infrastructure Project Management Support • Collect Analyze and Report Data on Actual Project Management Performance	System Design (continued) • Create Detailed System Design Construction • Prepare Operations Manual(s) • Conduct Test Readiness Review (TRR) Acceptance • Conduct Transition/ Deployment Meeting • Finalize Project Deliverables • Conduct Production Readiness Review (PRR) Operational Readiness • Prepare for Installation • Perform Pilot Testing • Perform Parallel Operations • Prepare/Document Lessons Learned Operations • Activate the System • Roll-out to Additional Sites • Manage Production Problem Reports • Capacity Planning and Replanning Retirement • Define/Document System Cut-Over Plan

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Infrastructure Services Division (ISD) ISD Support Teams (Continued)			Retirement (continued) • Archive Programs and Data • Define/Document Infrastructure Retirement/ Conversion Plan • Document Retirement Process Lessons Learned Project Management Support • Perform Requirements Management
Investment Review Board (IRB)	Consisting of Customs Deputy Commissioner and Assistant Commissioners, the IRB is responsible for selecting, controlling, and evaluating all strategic investment decisions. They participate in and direct the Investment Management Process (IMP).	Concept and Business Case • IRB Approval Process Project Management Support • Ongoing Project Oversight	Concept and Business Case • Release Funding
Investment Organization	The OIT organization (part of the Planning Group) responsible for development and maintenance of the Investment Management Process (IMP), supporting documentation, and subsidiary processes. They also provide support to the ITC and IRB, and to Projects as required.	Initiation and Authorization • Perform Project Initiation Review	Concept and Business Case • Create Business Case • ITC Approval • IRB Approval Initiation and Authorization • Create Initiation Documentation • Conduct Project Tailoring Reviews Project Management Support • Ongoing Project Oversight

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Office of Finance, Procurement Division (OFPD)	The Customs organization responsible for producing, authorizing, and monitoring contracts for acquiring products and/or services.		Initiation and Authorization • Develop Acquisition Plan Project Definition • Acquire Project Systems/ Services
Contracting Officer	The person with authority to procure, enter into, administer, and/or terminate contracts and make related determinations and findings.		
OIT CM Organization	The organization(s) within OIT responsible for defining standards and procedures that contribute to maintaining the integrity of all enterprise work products and for controlling assigned Production baselines.	Acceptance • Migrate Software to Test Environment • Baseline the System Operational Readiness • Convert Data • Move to Production Environment • Create Production Baseline • Release Production Notice Operations • Post-Implementation Evaluations Retirement • Archive Programs and Data • Remove Programs/ Infrastructure • Update System Document to Show Archive Location	Project Definition • Prepare Support Area (CM) Plans Acceptance • Resolve Test Problems • Prepare Production Move Request Retirement • Archive System and Project Documentation Project Management Support • Perform Configuration Management

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
OIT QA Organization	The organization within OIT responsible for overseeing and verifying quality assurance activities, independent of the project.	Project Management Support • Collect, Analyze and Report Data on Actual Performance • Perform Quality Assurance	Initiation and Authorization • Conduct Project Tailoring Reviews Project Definition • Prepare Support Area (QA) Plans Operational Readiness • Conduct Operational Readiness Review (ORR) Project Management Support • Prepare for and Respond to External Oversight Requests
OIT Security Organization Information Systems Security Branch (ISSB)	The OIT Security Organization consists of infrastructure staff who maintain enterprise IT security policies, provide enterprise IT security planning, review all security-relevant SDLC documents and provide IT security and advice and assistance to IT Project Managers.	Construction • Conduct Test Readiness Review (TRR) Acceptance • Security Certification • Submit Security Accreditation Package Operations • Perform Security Re-Certification and Re-Accreditation	Project Definition • Prepare Required Security Deliverables • Negotiate and Document ISAs Construction • Create System Acceptance Plan • Conduct Unit/Integration Testing • Submit Security Accreditation Package Acceptance • Finalize System Acceptance Test Plan
System Design Security Officer (SDSO)	A project's point-of-contact with ISSB who provides advice concerning IT security policies, procedures, requirements, documents, and issues as appropriate for each project.		
Computer Security Officer (CSO)	The person in the Business or Development area assigned responsibility for the security of an application or other IT system.		

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
OIT Security Organization Information Systems Security Branch (ISSB) System Design Security Officer (SDSO) Computer Security Officer (CSO) (Continued)			Acceptance (continued) • Conduct Production Readiness Review Operations • Update Required Security Documentation • Evaluate Disaster Recovery and Contingency Plans Retirement • Create Security Conversion Plan
Planning Group (PG)	An OIT organization with the following responsibilities: • Develops, communicates, and coordinates OIT's plans, including budget formulation, strategic plans, and performance measures • Provides CMM® and life cycle policy expertise and support for the Enterprise Process Improvement Program (EPIP) and associated organizations (e.g., Process Groups) and projects • Provides assistance and support to the ITC and IRB • Provides advice and assistance for OIT acquisition requests.	Concept and Business Case • Release Funding	

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Planning Organization	The OIT organization (part of the Planning Group) responsible for developing, communicating, and coordinating OIT's strategic plans, annual plans, performance plans, and budget submissions.		Operations • Post-Implementation Evaluations
Process Action Teams (PATs)	A team sponsored by a Process Group that is formed to document, develop, improve, or support the implementation of a particular process, discipline, or set of procedures.		Program Management Support • Perform Quality Assurance
Process Group (e.g., SEPG)	A chartered permanent organization within OIT formed to facilitate the definition, maintenance, and improvement of the OIT processes and procedures related to a particular discipline.		Initiation and Authorization • Create Initial Project Plan Project Management Support • Perform Quality Assurance
Program Monitoring Group (PMG)	The OIT organization responsible for coordinating management reviews, liaison and support for external oversight organization reporting, and conducting performance audits and formulating audit trails in accordance with GAO government accounting standards. Also responsible for collecting and consolidating high-level project metrics for OIT executive and IMP review.	Project Management Support • Collect, Analyze and Report Data on Actual Performance	Initiation and Authorization • Conduct Project Tailoring Reviews • Perform Project Initiation Review Project Management Support • Ongoing Project Oversight
Resource Management Group (RMG)	The organization within OIT responsible for facilities management and logistical support for all OIT activities, budget execution and support, and human resources and OIT staff training activities.		Project Definition • Acquire Project Systems/ Services

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Senior Management	A management and oversight functional role at a high enough level above the Project Manager that the primary focus of the person filling the role is the long-term vitality of the organization, rather than short-term	Concept and Business Case • Identify Project Manager Initiation and Authorization • Identify Initial Members of the Project Team • Conduct Project Tailoring Reviews	Concept and Business Case • Review High-level Business Alignment and Architecture • Conduct Project Review With Senior Management/DD

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Senior Management (Continued)	project and contractual concerns and pressures. These individuals have the authority to direct the allocation or reallocation of resources in support of organizational goals, and they direct the work of one or more subordinate Projects/Project Managers. This role may be performed by a Branch Chief, Division Director, or higher-level manager depending on the organizational structure to which the Project/Project Manager reports.	Project Definition • Negotiate and Document ISAs • Perform Definition Phase Completion Review Acceptance • Conduct Production Readiness Review (PRR) Operational Readiness • Conduct Operational Readiness Review (ORR) Retirement • Create System Retirement Team and Retirement Project Plan Project Management Support • Prepare/Conduct Senior Management Reviews • Prepare for and Respond to External Oversight Requests	System Design • Conduct Project Review with Senior Construction • Conduct Test Readiness Review (TRR) Project Management Support • Ongoing Project Oversight

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
SLC Organization	The OIT organization (part of the Planning Group) that is responsible for the development and maintenance of system life cycles, including support and advice to projects. They also provide CMM® and life cycle policy expertise and support and assistance the Enterprise Process Improvement Program (EPIP), OIT's process improvement Management Steering Committee (MSC), Projects, and Process Groups (e.g., the SEPG).		Initiation and Authorization • Select Appropriate Life Cycle and Identify Tasks/ Deliverables • Create Initial Project Plan • Conduct Project Tailoring Reviews • Perform Project Initiation Review Program Management Support • Perform Quality Assurance
Software Development Division (SDD)	The division within OIT responsible for the design, development, and maintenance of software developed by or for the United States Customs Service.	Operations • Document Operational Lessons Learned	Operations • Monitor Performance • Ensure Continuous Operations • Analyze Problem Reports • Evaluate and Upgrade Systems Software/COTS

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Support Organizations	All those organizations who assist the system development effort by performing the ancillary tasks associated with creating or maintaining systems. This includes individuals, groups, or teams performing required functional roles such as Networks, Database Administration, Middleware, CM, and other ISD Engineering and Operations Support Team roles. In addition, where not critically called out or mandated as a separate organizational responsibility for an activity, Support Organizations also include Training, Testing, Security, and staff functions. **Note:** Also see the responsibilities listed for: Training Organization Testing Organization Data Management Organization OIT Security Organization OIT CM Organization OIT QA Organization Infrastructure Services Division (ISD) Technology and Architecture Group (TAG) Planning Group (PG) Program Monitoring Group (PMG) Resource Management Group (RMG)	Project Definition • Walkthrough Functional Requirements Operational Readiness • Prepare/Document Lessons Learned Project Management Support • Negotiate, Update and Rebaseline Project Plans, Agreements, and Documents	Concept and Business Case • Identify COTS/GOTS etc. for further Application Product Evaluations Initiation and Authorization • Select Appropriate Life Cycle and Identify Tasks/ Deliverables • Create Initial Project Plan • Conduct Project Tailoring Review Project Definition • Prepare Functional Requirements • Certify User and Functional Requirements • Prepare Support Area Plans • Conduct Support Organization Interface Meeting(s) • Perform Definition Phase Completion Review System Design • Conduct Peer Reviews and Preliminary Design Reviews • Conduct Peer Reviews and Detailed Design Reviews •

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Support Organizations (Continued)			System Design (Continued) • Conduct Critical Design Review (CDR) • Baseline Design Construction • Document Work Products • Finalize Project Deliverables Acceptance • Conduct Transition/Deployment Meeting • Baseline the System • Conduct Production Readiness Review (PRR) Operational Readiness • Finalize Project Plans and Documentation • Create Production Baseline • Conduct Operation Readiness Review (ORR) Operations • Roll-Out to Additional Sites Retirement • Create System Retirement Team and Retirement Project Plan • Notification of Intent to Retire System • Develop Data Conservation/Conversion Plan • Notification of Completion

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Support Organizations (Continued)			Project Management Support • Perform Project Planning, Costing and Budgeting Activities • Prepare/Conduct Project Status Meetings • Conduct SDLC and Architectural Compliance Reviews • Perform Requirements Management • Collect, Analyze and Report Data on Actual Project Management Performance • Perform Risk Management
Technology and Architecture Group (TAG)	The OIT organization responsible for the functional architecture, work architecture, information architecture, and infrastructure architecture and their related processes. They provide analytical and administrative support to the TRC and perform architecture and post-implementation system evaluations.		Concept and Business Case • TRC Approval Process Initiation and Authorization • Create Initial Project Plan • Perform Project Initiation Review
Technology Review Committee (TRC)	The group responsible for ensuring that proposed projects support and comply with Customs Enterprise Architecture. They also verify that Projects are supportable and do not duplicate existing systems.	Concept and Business Case • TRC Approval Process	

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Testing Organization (Branch) Testers	The OIT organization responsible for independent system and security testing for all application systems to be implemented in the Customs Production environment. Independent testers responsible for verifying that the system functions, as defined by the requirements and design documentation, perform as expected. This includes functional, security, and user acceptance testing.	Project Definition • Define Test Requirements Construction • Create System Acceptance Plan • Conduct Test Readiness Review (TRR) Acceptance • Prepare/Update Test Cases • Finalize System Acceptance Test Plan • Conduct System Acceptance Test (SAT) • Prepare Testing Organization's SAT Reports • User Acceptance Testing	Project Definition • Prepare Support Area Plans Construction • Prepare Turnover Package Acceptance • Migrate Software to Test Environment • Resolve Test Problems • Develop/Update Initial User Documentation and Training Materials • Conduct Production Readiness Review (PRR)
Training Organization (Branch) Trainer	The OIT organization that is responsible for the training of the end-users of applications. It prepares user documentation and training materials and trains both new and experienced users on the application being built, purchased, updated or integrated. It also arranges logistics, develops schedules, and coordinates training requirements with users and Project Team members. A member of the Training Organization or other qualified individual who performs training activities.	Project Definition • Define Training Requirements System Design • Create Training Plan Construction • Prepare Draft User Documentation and Training Material Outlines Acceptance • Develop/Update Initial User Documentation Operational Readiness • Finalize Training Schedule • Conduct Training Pilot • Finalize and Produce Training Materials Operations • Train Users • Update User Documentation	Concept and Business Case • Create Business Case Project Definition • Prepare Support Area Plans Construction • Establish Working Environments • Conduct Unit/Integration Testing Acceptance • User Acceptance Testing • Finalize Project Deliverables • Conduct Production Readiness Review (PRR) Operational Readiness • Move to Production

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
		and Training Materials	Environment

Organization	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Training Organization Trainer (Continued)			Operations • Roll-out to Additional Sites

B.3 Project-Specific Team Roles and Responsibilities

Project Team	Responsibilities	Standard Life Cycle Responsibilities	
		Primary	Support
Development Team	The group/individual responsible for analyzing, designing, developing, documenting, testing, and implementing a system. The Development Team is one part of the Project Team. **Note:** Also see responsibilities listed for: Project Implementation Team	Project Definition • Prepare Functional Requirements • Walkthrough Functional Requirements • Create RTM • Define Test Requirements • Prepare Required Security Deliverables • Prepare Support Area Plans System Design • Create Preliminary System Design • Conduct Peer Reviews and Preliminary Design Reviews • Create Detailed System Design • Conduct Peer Reviews and Detailed Design Reviews • Conduct Critical Design Review (CDR) • Baseline Design	Initiation and Authorization • Document User Requirements Project Definition • Update User Requirements • Certify User and Functional Requirements • Define Training Requirements • Perform Definition Phase Completion Review Construction • Construct Infrastructure • Prepare Draft User Documentation and Training Material Outlines Acceptance • Develop/Update Initial User Documentation and Training Materials • Submit Security Accreditation Package • Conduct Production Readiness Review (PRR)

Project Team	Responsibilities	Standard Life Cycle Responsibilities	
		Primary	**Support**
Development Team (Continued)		Construction • Establish Working Environments • Develop/Code Software Package • Document Work Products • Conduct Unit/Integration Testing • Prepare Operations Manual(s) • Conduct Work Product Walkthroughs • Conduct Peer Reviews • Finalize Project Deliverables • Prepare Turnover Package Acceptance • Resolve Test Problems • Prepare Production-Ready Environment • Conduct Transition/Deployment Meeting • Finalize Project Deliverables Operational Readiness • Perform Pilot Testing • Perform Parallel Operations Project Management Support • Prepare/Conduct Project Status Meetings • Prepare/Conduct Peer Reviews • Perform Configuration Management	Operational Readiness • Convert Data • Finalize Project Plans and Documentation • Conduct Operational Readiness Review (ORR) Operations • Roll-out to Additional Sites Project Management Support • Conduct SDLC and Architectural Compliance Reviews • Perform Requirements Management • Collect, Analyze and Report Data on Actual Project Management Performance

Project Team	Responsibilities	Standard Life Cycle Responsibilities	
		Primary	Support
Project Implementation Team	A subteam defined within the overall Project Team if required, responsible for site planning and fielding of the system.	Project Definition • Prepare Support Area Plans Acceptance • Conduct Transition/Development Meeting • Finalize Project Deliverables Operational Readiness • Prepare for Installation • Perform Pilot Testing Operations • Roll-out to Additional Sites	Construction • Construct Infrastructure Acceptance • Prepare Production-Ready Environment Project Management Support • Collect, Analyze and Report Data on Actual Project Management Performance
Product Evaluation Team	A Project Team subgroup that evaluates and documents COTS or GOTS applications. This team: • Evaluates the candidate components/products to ensure that they meet mandatory user requirements, architectural standards, and appropriate domain criteria • Documents those evaluations in a manner that will satisfy any applicable legal and/or contracting standards	Concept and Business Case • Identify COTS/GOTS, etc. for further Application Product Evaluations	
Project Change Control Board (CCB)	Reviews each change request, evaluates the impact on the project, and either renders an approve/disapprove decision for change requests within the scope of approved resources or refers them to Senior Management. The CCB also helps prioritize approved changed requests and requirements for release.	Project Management Support • Perform Requirements Management	Project Management Support • Perform Configuration Management

Project Team	Responsibilities	Standard Life Cycle Responsibilities	
		Primary	Support
Project CM Team Project CM Manager Project Librarian	The group responsible for: • Establishing and maintaining the integrity of all the project work products and baselines in the development environment • Identifying appropriate configuration items (CIs) so that the development environment can be re-established if necessary • Ensuring the proper turnovers to the OIT CM Organization.	Project Definition • Prepare Support Area (CM) Plans System Design • Baseline Design Acceptance • Resolve Test Problems Project Management Support • Negotiate, Update and Rebaseline Project Plans, Agreements, and Documents • Perform Configuration Management	Project Definition • Certify User and Functional Requirements Construction • Finalize Project Deliverables Acceptance • Migrate Software to Test Environment • Prepare Production Move Requests • Baseline the System Operational Readiness • Move to Production Environment • Create Production Baseline Retirement • Prepare and Submit Program Move Request • Archive System and Project Documentation
Project Management Team Project Planner	The group that consists of the Team Leaders, and the personnel assigned to assist the Project Manager in performing the project management, planning, and control tasks. **Note:** Also see the potentially delegated responsibilities listed for: Project Manager	Concept and Business Case • Create Business Case Project Definition • Prepare Support Area Plans Construction • Finalize Project Deliverables Project Management Support • Prepare/Conduct Peer Reviews • Perform Risk Management • Prepare for and Respond to External Oversight Requests	Initiation and Authorization • Develop Acquisition Plan Acceptance • Finalize Project Deliverables Project Management Support • Perform Project Planning, Costing and Budgeting Activities • Prepare/Conduct Project Status Meetings • Contractor/Subcontractor Management

Project Team	Responsibilities	Standard Life Cycle Responsibilities	
		Primary	Support
Project Management Team (continued)			Project Management Support (continued) • Collect, Analyze and Report Data on Actual Project Management Performance • Negotiate, Update and Rebaseline Project Plans, Agreements, and Documents
Executive Management Team	On some projects there may also exist a separate group at a higher-level than the Project Management Team with project management and oversight responsibilities.		
Project Initiation Team	A group that consists of the Project Manager, Business Sponsor, and the personnel assigned to perform the project management, planning, and control tasks during Stages 1 and 2 of the life cycle. The members of this team are not necessarily the same group who will do the actual project development.		
Team Leader	The person responsible for leading a collection of people, often drawn from diverse but related groups, assigned to perform a specific set of tasks for the project.		
Risk Manager/ Coordinator/ Administrator	A member of the Project Management Team responsible for tracking and reporting on risk priorities and the status of risk mitigation plans and action items. This person may also be responsible for coordinating risk management review meetings for the project on a regular		

Project Team	Responsibilities	Standard Life Cycle Responsibilities	
		Primary	Support
	basis.		

Project Team	Responsibilities	Standard Life Cycle Responsibilities	
		Primary	Support

Project Quality Assurance (QA) Team
 	
Project QA Manager
	A group on the Project responsible for:
	• Formal monitoring of various work products of the project to ensure that standards, policies, and regulationsare being met
	  • Reviewing requirements and project plans to ensure that project quality concerns are being accounted for
	  • Monitoring the compliance and effectiveness of the processes being used on the project.
	
	Note: All Project Team members are responsible for ensuring that quality (e.g., usability) requirements are included in the development and for performing adequate reviews and testing throughout the lifecycle
		Project Definition
		• Prepare Support Area (QA) Plans
		• Define Test Requirements
		Project Management Support
		• Perform Quality Assurance
			Project Definition
			• Walkthrough Functional Requirements
			• Perform Definition Phase Completion Review
			System Design
			• Conduct Peer Reviews and Preliminary Design Reviews
			• Conduct Peer Reviews and Detailed Design Reviews
			• Conduct Critical Design Review (CDR)
			• Baseline Design
			Construction
			• Conduct Work Product Walkthroughs
			• Conduct Peer Reviews
			• Conduct Test Readiness Review (TRR)
			Acceptance
			• Conduct Production Readiness Review (PRR)
			Operational Readiness
			• Perform Pilot Testing
			• Perform Parallel Operations
			• Conduct Operational Readiness Review (ORR)
			Project Management Support
			• Collect, Analyze and Report Data on Actual Project Management Performance
			• Negotiate, Update & Rebaseline Plans, Agreements, & Documents

Project Team	Responsibilities	Standard Life Cycle Responsibilities	
		Primary	Support
Project Security Team AIS Security Analyst	Members of the Project Team with the responsibility for: • Monitoring and overseeing that the appropriate level of security is incorporated into an application's hardware and software as it is being designed/developed/acquired • Ensuring that appropriate consideration is also given to personnel security, physical security, information security, etc. in relation to the system/project • Monitoring and overseeing the appropriate level of security while an application remains operational and/or is being modified • Providing the project with expertise in various aspects of security, including computer security, communications security, emissions security, and network security.	Project Definition • Prepare Required Security Deliverables System Design • Create Preliminary System Design • Create Detailed System Design Construction • Prepare Draft User Documentation and Training Material Outlines Acceptance • Finalize Project Deliverables .	Construction • Conduct Unit/Integration Testing Acceptance • Security Certification • Submit Security Accreditation Package

Project Team	Responsibilities	Standard Life Cycle Responsibilities	
		Primary	Support
Project Team	The group responsible for ALL activities in a project. This group includes the following subgroups, which may share the services of the same individuals: • Development Team • Project Implementation Team • Project Management Team • Project QA Team • Project CM Team • Project Security Team • Product Evaluation Team • Designated members of Support Organizations **Note:** Also see the responsibilities listed for the above named subgroups.	Initiation and Authorization • Create Initiation Documentation Operational Readiness • Prepare/Document Lessons Learned	Acceptance • Prepare Production Readiness Review (PRR) Package Project Management Support • Perform Risk Management

B.4 Individual Project Roles and Responsibilities

Individual Project Role	Description	Standard Life Cycle Responsibilities	
		Primary	Support
AIS Security Analyst See Section B.3, Project Security Team, page B-24			
Analyst See Section B.3, Development Team, page B-18			
Business Interface Representative (BIR)	OIT's representative to the Business Sponsor and users. The BIR is responsible for maintaining strategic communication between OIT and the business process and serving as the single point of contact for the BITR and Business Sponsor.	Project Definition • Update User Requirements	Concept and Business Case • Create Project Concept • Create Business Case Initiation and Authorization • Document User Requirements • Conduct Project Tailoring Reviews

Individual Project Role	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Business Interface Representative (BIR) (Continued)			Initiation and Authorization (Continued) • Project Initiation Review System Design • Create Preliminary System Design • Create Detailed System Design • Conduct Critical Design Review (CDR) Operations • Update Required Security Documentation • Evaluate Disaster Recovery and Contingency Plans • Perform Security Re-Certification and Re-Accreditation
Business Information Technology Representative (BITR) Business Project Manager	The Business Sponsor's primary representative to OIT. For each business area, OIT has assigned a BIR as its primary point of contact for the BITR. The BITR is a member of the Information Technology Committee (ITC). The BITR may delegate specific project-related duties to a Business Project Manager. **Note**: The BITR may also assume additional responsibilities as delegated by the Business Sponsor – see responsibilities listed below. If the Business Sponsor/BITR chose to designate a Business Project Manager,	Concept and Business Case • Create Business Case Project Definition • Update User Requirements Retirement • Review and Verify Removal Plans	Concept and Business Case • Create Project Concept Initiation and Authorization • Document User Requirements System Design • Create Preliminary System Design • Create Detailed System Design • Conduct Critical Design Review (CDR) Operations • Update Required Security Documentation • Evaluate Disaster

Individual Project Role	Description	Standard Life Cycle Responsibilities	
		Primary	Support
	that person is the project's point of contact representing the Business Sponsor and Users.		Recovery and Contingency Plans

Individual Project Role	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Business Information Technology Representative (BITR) Business Project Manager (Continued)	(Also see responsibilities listed below for potential responsibilities as delegated/defined by the BITR and Business Sponsor.)		Operations (Continued) • Perform Security Re-Certification and Re-Accreditation
Business Sponsor	The Customs executive who represents the business organization and the end-users, and who is ultimately responsible for sponsoring projects that provide functional value to the business. The AC, OIT will assign a Business Sponsor within OIT for OIT sponsored projects (such as infrastructure).	Concept and Business Case • Create Project Concept • Identify COTS/GOTS, etc. for further Application Product Evaluations • Create Business Case Initiation and Authorization • Document User Requirements • Create Initial Project Plan • Develop Acquisition Plan • Create Initiation Documentation Project Definition • Update User Requirements	Concept and Business Case • Review High-level Business Alignment and Architecture • TRC Approval Process Initiation and Authorization • Conduct Project Tailoring Reviews Project Definition • Walkthrough Functional Requirements • Define Test Requirements System Design • Create Training Plan

Business Sponsor (Continued)		Project Definition (Continued) • Certify User and Functional Requirements • Acquire Project Systems/Services • Define Training Requirements • Perform Definition Phase Completion Review System Design • Conduct Critical Design Review (CDR) • Baseline Design • Conduct Project Review with Senior Management/DD Acceptance • User Acceptance Testing • Submit Security Accreditation Package • Conduct Production Readiness Review (PRR) Operational Readiness • Perform Pilot Testing • Perform Parallel Operations • Conduct Operational Readiness Review (ORR) Operations • Roll-out to Additional Sites • Document Operational Lessons Learned • Post-Implementation Evaluations • Update Required Security Documentation • Evaluate Disaster Recovery and Contingency Plans	Acceptance • Conduct Transition/ Deployment Meeting Operational Readiness • Finalize Training Schedule • Finalize and Produce Training Materials • Prepare/Document Lessons Learned • Release Production Notice Operations • Train Users • Update User Documentation and Training Materials Retirement • Review and Verify Removal Plans Project Management Support • Prepare/Conduct Senior Management Reviews

Individual Project Role	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Business Sponsor (Continued)		Operations (Continued) • Perform Security Re-Certification and Re-Accreditation Retirement • Perform Impact Analysis • Create System Retirement Team and Retirement Project Plan • Notification of Intent to Retire System • Archive System and Project Documentation • Notification of Completion • Document Retirement Process Lessons Learned Project Management Support • Perform Project Planning, Costing and Budgeting Activities • Perform Requirements Management • Negotiate, Update, and Rebaseline Project Plans, Agreements, and Documents	
Project Configuration Manager See Section B.3, Project CM Team, page B-21			
Designer See Section B.3, Development Team, page B-18			
Developer See Section B.3, Development Team, page B-18			
Project Librarian See Section B.3, Project CM Team, page B-21			

Individual Project Role	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Project Manager	The person who is responsible for the day-to-day planning, directing, controlling, structuring and motivating the project. The Project Manager is ultimately responsible to the Business Sponsor and Senior Management for the overall success of the project, and for meeting cost, schedule, and quality goals.	Initiation and Authorization • Identify Initial Members of the Project Team • Select Appropriate Life Cycle and Identify Tasks/Deliverables • Create Initial Project Plan • Create Infrastructure Plan • Develop Acquisition Plan • Conduct Project Tailoring Reviews Project Definition • Certify User and Functional Requirements • Acquire Project Systems/ Services • Conduct Support Organization Interface Meeting(s) • Negotiate and Document ISAs • Perform Definition Phase Completion Review System Design • Conduct Critical Design Review (CDR) • Baseline Design • Conduct Project Review with Senior Management/DD Construction • Construct Infrastructure • Finalize Project Deliverables • Conduct Test Readiness Review (TRR)	Initiation and Authorization • Create Initiation Documentation System Design • Conduct Peer Reviews and Preliminary Design Reviews • Conduct Peer Reviews and Detailed Design Reviews • Create Training Plan Project Management Support • Prepare/Conduct Peer Reviews • Ongoing Project Oversight

Individual Project Role	Description	Standard Life Cycle Responsibilities	
		Primary	Support
		Acceptance • Prepare Production Move Request	

Individual Project Role	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Project Manager (Continued)		Acceptance (Continued) • Baseline the System • Prepare Production Readiness Review Package • Conduct Production Readiness Review (PRR) Operational Readiness • Finalize Project Plans and Documentation • Create Production Baseline • Conduct Operational Readiness Review (ORR) • Release Production Notice Operations • Roll-Out to Additional Sites Retirement • Create System Retirement Team and Retirement Project Plan • Create Security Conversion Plan • Develop Data Conservation/Conversion Plan • Define/Document System Cut-Over Plan • Define/Document Infrastructure Retirement/ Conversion Plan • Prepare and Submit Move Request • Archive System and Project Documentation • Document Retirement Process Lessons Learned	

Individual Project Role	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Project Manager (Continued)		Project Management Support • Perform Project Planning, Costing and Budgeting Activities • Prepare/Conduct Project Status Meetings • Prepare/Conduct Senior Management Reviews • Contractor/Subcontractor Management • Perform Requirements Management • Collect, Analyze and Report Data on Actual Project Management Performance • Negotiate, Update, and Rebaseline Project Plans, Agreements, and Documents • Perform Quality Assurance • Perform Risk Management • Prepare for and Respond to External Oversight Requests	
Project Planner See Section B.3, Project Management Team, page B-23			
Project Quality Assurance (QA) Manager See Section B.3, Project QA Team, page B-22			
Risk Manager/Coordinator/Administrator See Section B.3, Project Management Team, page B-21			
Senior Manager See Section B.2, Senior Management, page B-12			

Individual Project Role	Description	Standard Life Cycle Responsibilities	
		Primary	Support
Stakeholder, External	1. All interested parties outside of the Project Team, including Users, the Business Sponsor, and all Support Organizations **Note:** Also see responsibilities listed for: Users and Business Sponsor 2. Users/customers outside of Customs who depend on Customs data collection and data processing for all or part of their business activities.	Project Definition • Negotiate and Document ISAs Retirement • Perform Impact Analysis	
Stakeholder, Internal	1. All individuals and interested parties within the Project Team **Note:** Also see responsibilities listed for: Project Team and Development Team 2. Users/customers within Customs who depend on a specific system for all or part of their mission-critical activities.	Retirement • Perform Impact Analysis	
System Design Security Officer (SDSO) See Section B.2, OIT Security Organization, page B-10			
Team Leader See Section B.3, Project Management Team, page B-21			
Technical Writer See Section B.3, Development Team, page B-18			
Tester See Section B.2, Testing Organization, page B-17			
Trainer See Section B.2, Training Organization, page B-17			

Individual Project Role	Description	Standard Life Cycle Responsibilities	
		Primary	Support
User	1. Anyone who uses automated systems developed by or for the United States Customs Service. 2. Representatives of the user community who provide input in the development of automated systems. The User is often referred to as the end-user, and is represented in the development life cycle by the Business Sponsor and BITR.	Initiation and Authorization • Document User Requirements Acceptance • User Acceptance Testing Operations • Activate the System Retirement • Perform Impact Analysis	Project Definition • Update User Requirements System Design • Create Preliminary System Design • Create Detailed System Design Acceptance • Prepare Production Readiness (PRR) Review Package Operations • Post-Implementation Evaluations Project Management Support • Perform Requirements Management

Appendix C
Standard Life Cycle Requirements Summary

C.1 Introduction

This appendix has been assembled for the convenience of the handbook user. It is intended to be a quick checklist of the major aspects of the SDLC Policies presented in Chapter 2 and the Customs Standard Life Cycle presented in Chapter 4.

> This appendix does not replace Chapters 2 and 4. It should be used in conjunction with the more detailed guidance in those chapters.

This appendix lists the mandatory reviews, deliverables, and roles that a project must include in its tailored Project Plan. It also presents information on mandatory metrics and processes that must be performed to manage the project.

Additional guidance (such as templates, examples, and procedures) for these required activities and outputs may be found in the Customs Process Asset Library (PAL).

C.2 Synopsis of Mandatory Reviews

All projects regardless of size must successfully complete and document these reviews:

Review	When It Occurs	Who Signs Off
Initial Investment Management Process Reviews	At the start of the project	TRC, ITC and/or IRB as appropriate to project size, cost, risk, and funding availability
Project Tailoring Reviews	• During Project Initiation and • Anytime that the project baseline documentation is to be tailored	• Project Manager • Senior Management • Support Organizations

Review	When It Occurs	Who Signs Off
Project Initiation Review	• The end of Project Initiation and • Whenever the project's cost, schedule, or scope is modified by 10% or more	• Division Director • Planning Group

Review	When It Occurs	Who Signs Off
Requirements Walkthrough and Certification	During the Project Definition stage.	• Business Sponsor • Project Manager
Critical Design Review (CDR)	During the System Design stage	• Business Sponsor • Project Manager • Support Organizations
Test Readiness Review (TRR)	At the end of the Construction stage	• Project Manager • Testing Organization • Data Management Organization • OIT Security Organization
System and User Acceptance	During the Acceptance stage	• Business Sponsor • Users • Testing Organization
Security Certification	During the Acceptance stage	Information Systems Security Manager (currently the Head of ISSB)
Security Accreditation	During the Acceptance stage	Designated Approval Authority (currently the AC, OIT)
Production Readiness Review (PRR)	At the end of the Acceptance stage	• Project Manager • Senior Management • Business Sponsor • Division Directors
Operational Readiness Review (ORR)	At the end of the Operational Readiness stage	
Regularly scheduled Project Team and Senior Management Reviews	Ongoing throughout the entire life cycle	• Project Manager • Senior Management

In addition to project status, both project risks and security risks shall be monitored and reassessed regularly, particularly when the schedule is being revised and at major milestones.

All certifications, signoffs, meeting minutes, and decisions shall be maintained in the project repository.

C.3 Mandatory Project Roles Summary

As defined in Chapter 2, the following project roles at minimum must be assigned by name in writing in the Project Plan. Refer to Appendix B for specific project role definitions and responsibilities.

Role	Assigned by	Notes
Project Manager (PM)	Senior Management	The PM is the technical manager responsible for project success.
Project Quality Assurance (QA) Manager and QA Team	Project Manager	• Depending on project size and complexity, these roles could range from part-time tasks for one person to full time tasks for several people. • One person may fill more than one role.
Project Configuration Manager and CM Team	Project Manager	
Risk Management Coordinator	Project Manager	
Project Change Control Board (CCB)	• Senior Management • Business Sponsor(s) • Project Manager	Membership includes representation for all users of the system.
Computer Security Officer (CSO)	Business Sponsor/BITR	See Information Systems Security Policy and Procedures Handbook.
Quality Assurance Verification	OIT QA Organization	
Team Leads and Teams	Project Manager	As required. Must include identified staff to perform Planning and Requirements Management activities.

C.4 Mandatory Deliverables/Information Summary

All projects regardless of size must consider each of the following deliverables/information for applicability. The results of that deliberation must be documented. While all the information noted below is required, documents listed may be combined with each other or with one of the required project deliverables as documented in the project's tailoring rationale.

See Chapter 2, Section 2.3.3, for further information on Tailoring policies. Also see Appendix A, Glossary, for definitions of terms and documents.

Document	Description	Notes
IT Concept Document and Business Case documents	As defined by the Investment Management Process	Contact Planning Group for assistance
Project Plan	Summarizes cost, schedule, resource information, life cycle methodologies selected, and management strategies for the project	This specific document is mandatory; it may also include some of the information identified below as additional sections in this plan.
Data Management Plan	Identifies the data requirements, data models, database design, and data management activities	Contact Data Management Organization for assistance

Document	Description	Notes
Configuration Management Plan	Defines the configuration management procedures to be used and specific configuration items for the project	
Quality Assurance Plan	Identifies the project's personnel and activities to ensure the quality of the work products being developed and to verify compliance with standards, procedures, and plans.	
Security Plan	Identifies all security-related activities	• This specific document is mandatory. • NONE of the elements of the plan as defined in the PAL template may be tailored out • Contact OIT Security Organization for assistance.
Security Risk Assessment	Documents security risks for the system and its data	Contact OIT Security Organization for assistance
System Test Plan	Identifies how the system shall be tested, criteria for success, and testing resource needs	Contact the Testing Organization for assistance.
Security Test Plan	Identifies the security tests required for certification.	Contact OIT Security Organization for assistance
System Acceptance Test Plan	Defines the testing activities to be performed, test data and acceptance criteria, and testing resource needs. Also includes security acceptance testing verifications as needed.	Developed by the Testing Organization.
Training Requirements	Identifies the training needs of the business organization and end-users.	Developed by the Training Organization.
Training Plan	Identifies the training that shall be developed and provided based on the approved Training Requirements.	Developed by the Training Organization.
User and Functional Requirements and Requirements Traceability Matrix	A precise description of the requirements of the system including detailed user, system, and support requirements.	• User and functional requirements documents may be combined • Requirements Certification/ signoff is necessary • Includes security, automation readiness, quality, and data requirements.
Infrastructure Plan	Defines the architecture, hardware, communications, and other infrastructure support needs of the project.	May be included in the Project Plan or form the basis of Acquisition Plans developed by the project.

Document	Description	Notes
Acquisition Plan(s)	Developed with the Acquisition Organization to define and acquire products and services for completing the project.	Forms the basis of the Statement of Work issued by OFPD.
System Design Document(s)	Provides a detailed description of how the system will work, including technical approach, databases, interfaces, components, and module specifications	May be combined
Security Design Document	Defines the security features of the system.	
Implementation Plan	Identifies the configuration items and sequence of work that needs to be performed to migrate an application to testing and production environments.	Documents the understandings between the Project and ISD Support Teams.
Deployment Plan	Describes the strategies and schedule to field test and roll-out the system.	Defines the agreements between the Project, Business Sponsor, users, and Support Organizations.
Test Cases/Scenarios	Describes the test cases and expected results.	May be combined
Test Results	Actual results from the unit, integration, security, systems, and acceptance testing performed.	
Documents to operate and maintain the system	As appropriate. Can Include: • Program specifications or modifications log • Operations Manual(s) for system and sites • User documentation and training materials • Test cases/scenarios for regression testing	
Risk Management Outputs	Includes: • Project risk management plan or strategy • Prioritized list or database of project risks (formally updated in every stage or more frequently)	The risk management strategy may be included in the Project Plan. Risk data (including prioritization and mitigation) may be maintained as part of a risk management plan or in a database for ease of update.
Lessons Learned	Documents the lessons learned, both good and bad, during the project's life.	Concerns technical, project, operational, and process-related issues.
Interconnection Security Agreements (ISA)	Identifies connectivity between internal systems and all non-Customs systems and networks. It supports a previously established business Memorandum of Understanding (MOU).	Each ISA must have a previously approved MOU. Signatories for the final agreement are the CIO and equivalent level in the non-Customs organization.

Document	Description	Notes
Security Certification and Security Accreditation Packages	Specific documents and signoffs are necessary before the system can move to production or use production data.	Includes Contingency Plan, Disaster Recovery Plan, and Trusted Facility Manual in addition to those Security documents listed previously.

Once a system moves into the Operations stage, the following are also mandatory:

Document	Description	Notes
A documented change control process	Defines the change control procedures to be used for application changes and for hardware/system change management.	For application changes, see the OIT CM Organization's SOP for Change Control/Change Management Overview for Non-Emergency and Emergency Projects.
Post-implementation security documents as required	Includes Contingency Test Plan and Test Reports, Application Security Audit Reports, System/Infrastructure Security Audit Reports, and Security Incident Reports.	Also includes updates as needed to the security documents created during the development project and listed above. Contact OIT Security Organization for assistance.
Operational System QA and CM Plans	OIT standard plans with updates as required for new/changed systems.	
Business Impact Analysis (BIA) priorities and Continuity of Operations Plan (COOP)	Sets restoration priority of all business functions compared to all others, and defines the procedures for restoring functions (both manual and automated) in case of a disaster.	This information is maintained by each business area in conjunction with ISD and IA. Each project will provide information for updates in their Disaster Recovery Plans.

C.5 Mandatory Metrics Summary

When a project begins, metrics must be defined for the system's contribution to Customs mission performance and business improvement. The project must also document metrics for expected systems performance and acceptance criteria. These metrics are documented in the project's Business Case, and the acceptance criteria are documented in the User Requirements.

Once the project has been approved, the following Project Management Performance Data must be collected, documented, and used throughout the project's life cycle (as identified in Chapter 2, Section 2.4.4):

- Effort for both product development and review activities
- Cost
- Work Product Size(s) and changes
- Schedule (based on Effort and Size estimates plus staff availability)
- Requirements (i.e., number of requirements) and Number of Changes
- Product Quality (i.e., number of defects, severity, and status)

- Critical Computer Resources (e.g., memory, storage, bandwidth, hardware, tools) needed both for development and for deployment and operation.

Each of these items must be estimated during initial planning. Also, the assumptions and constraints upon which the estimates are based should be documented. Then data for each of these metrics must be collected regularly during the project's life cycle.

The project compares actual accomplishments and effort with the estimates to provide objective information on project status and trends. Corrective actions will be taken as required and documented. These measurements shall not be used to evaluate individual performance.

Once the system is in operation, Performance Measures must be collected:

- To demonstrate the systems' contribution and efficiency; and
- For comparison with the gains projected in the Business Case.

C.6 Mandatory Supporting Process Summary

All projects must document and effectively perform these key processes. See Chapter 2, Customs Life Cycle Policies, for details relating to the processes listed below. Also see the Customs Standard Life Cycle stages in Chapter 4, Section 4.3 for the development life cycle processes also required to be performed by each project.

Process	Definition	Reference
Quality Assurance	Define and Measure Success	Section 2.5
Configuration Management	Ensure Interoperability and Consistency	Section 2.6
Requirements Change Management	• Define Impacts • Prevent Scope Creep	Sections 2.2 and 2.7
Project Management	• Define Duties • Report Progress • Coordinate Activities	Sections 2.3, 2.4, and 2.8
Development Life Cycle	• Define High-level Conceptual Processes (e.g., Design) • Identify Required Activities and Outputs within Life Cycle	Section 4.3

C.7 Projects Already Underway and Systems in Operation

This handbook applies not only to new projects, but also to projects already underway, and to systems in operation.

Senior Management shall weigh the costs and benefits, then determine and document the appropriate level of effort to be expended for each underway project and system in operation to bring them into compliance with this Handbook.

Managers of all underway projects and systems in operation shall determine in which stage of the Customs Standard Life Cycle they fall. Underway projects and systems in operation shall commence SDLC activities, reviews, and deliverables from that point forward. Deliverables and reviews from Life Cycle stages prior to that point, which are necessary precursors to future activities, shall be completed. Other deliverables must be completed to the maximum extent practicable.

The tailoring and approval process, described in Chapter 4, Stage 2 – Initiation and Authorization, provides the mechanism for underway projects and systems in operation along with their Senior Management to account for and document SDLC compliance, along with rationale for the level of effort to be expended.

Appendix D
SDLC Changes

D.1 High Level Change Process

Changes to the SDLC may be suggested by anyone who uses the document. The following describes the high level process for SDLC Changes. The SDLC Change Procedures document contains detailed procedures and responsibilities.

- Suggestor submits a change request
- The SLC Organization maintains a change request catalog
- The SLC Organization routes change requests to the cognizant subject matter group for staffing and research if needed.
- The SLC Organization collates the change requests for review by the Process Coordination Board and/or the Management Steering Committee as appropriate
- The PCB and/or MSC determines priority and schedule of suggested revisions. At a minimum, the PCB will review suggested revisions quarterly.
- The SLC Organization coordinates hard copy and electronic interim revisions.
- The SLC Organization collates all low priority or editorial items for the next full re-write of the SDLC.

D.2 Change Request Instructions

The form on page D-3 should be used when suggesting changes to this handbook. The following explains the fields on the form and the information required in each field:

Field	Required Information
Date	The date this suggestions is being submitted
Change Request Number	None. *This field to be used by the SLC Team*
Chapter/Page to Be Changed	Please identify the chapter, page, and if possible paragraph containing the text or figure to be changed. **Example**: Page D-1, second paragraph, fifth line
Name of Submitting Office	Please identify the Office/Branch/team within Customs

Field	Required Information
Phone	The suggestor's phone number. In the case of a group suggestion, this should be the phone number of the POC.
Address	Please provide full business mailing address and/or e-mail name.
Proposed Change	Explain WHAT material should be changed. Identify the page number and existing text or figure. Show the new material or changed wording that you recommend. **Example**: Page 7-1, Change "Pre-deployment Review" to "Operational Readiness Review".
Rationale for Change	Explain WHY this change should be made.

This form is available electronically in the OIT Toolbox and by e-mail request to "SDLCMAIL"
Send to: USCS, SLC Team, 7681 Boston Blvd., 2C42, Springfield, VA 22153 or
E-mail to "SDLCMAIL"

Note: If the suggestion is being submitted without using the form, the suggestor should provide all the above information in the body of the message.

Change Request

Date:_____ Change Request Number *(SLC Team Use Only)*

Chapter/Page to Be Changed:_____

Name of Submitting Office_____

Point of Contact_____Phone_____

Address _____

_____

_____

Proposed Change:

Rationale for Change:

This form is available electronically in the OIT Toolbox and by e-mail request to "SDLCMAIL"

Note: For the SLC Team to take appropriate action on a change request, please provide a clear description of the recommended change along with supporting rationale.

Send to: USCS, SLC Team, 7681 Boston Blvd., 2C42, Springfield, VA 22153 or
E-mail to "SDLCMAIL

Appendix E
Governing Directives

E.1 Introduction

This appendix summarizes the directives, standards, and other publications applicable to Customs systems development whose requirements are referred to or embedded in this Handbook.

If a project is highly complex or specialized, additional standards may be applicable. A good source for determining if standards exist for all or part of the project in question is the FIPS Index, published by the National Technical Information Service (NTIS). A copy of this directory and the Code of Federal Regulations are located in the reference section of the Customs library at Headquarters.

E.2 OIT Standards

The following Customs architecture, data, and software development standards and policies apply to projects and systems development. This list was current at the time of printing. However, these undergo continuing evaluation and refinement. The current list of OIT Standards and Policies should be obtained from the Technology and Architecture Group's Policy Team. In addition, processes, procedures, operating manuals and the like will be posted in the Customs Process Asset Library.

- Investment Management Process System Description;
  - U.S. Customs Service Enterprise Architecture Blueprint;
  - U.S. Customs Service Enterprise Architecture Technical Reference Model;
  - Maintenance Projects and Enhancements Requirements Specification Document;
  - United States Customs Data Object Definition and Naming Standards

- Post-Implementation Review Handbook;
- U.S. Customs Modernization Acquisition Policies;
- Infrastructure Services Division's Infrastructure Support Process (ISP);
- Policy and Procedures for Requesting Testing Services;
- Policies and Procedures for Mainframe Applications;
- Standard Operating Procedures for Operating System Support;
- Customs OIT Software Configuration Management (CM) Plan;
- Systems Operations Branch CM Team's Standard Operating Procedure "Change Control/Change Management Overview for Non-Emergency and Emergency Projects";
- Automation Standards Definition;
- Graphical User Interface (GUI) and Programming Standards as applicable.

E.3 Customs Directives

Availability: Customs Directives are available on-line from the mainframe through the Customs Issuance System (CIS). All directives in the CIS are prefixed with "099". A directory of applicable directives will be displayed if you enter "IM" in the data field labeled "Issuing Office".

Directive HB 1400-05A: *Information System Security Policy and Procedures Handbook*: This manual provides general security procedures and policies to be used with Customs automated information systems.

Directive 5510-023: *U.S. Customs Information Resource Management (IRM) Review Program*: This directive establishes the requirement and methodology for conducting reviews of Customs information resources to ensure that the resources are being utilized efficiently and effectively. This directive requires quarterly status reports for the current fiscal year reviews, and also annual review reports must be provided to Treasury for subsequent reporting to GSA, GAO, OMB, etc.

Directive 5510-024: *Local Management Information Systems (MIS)*: This directive establishes policy to upgrade the national inventory of local MIS, and establishes criteria covering the development of a local MIS is not appropriate.

Directive 5510-026: *Customs Electronic Data Retention and Schedules*: This directive establishes a service wide policy for the storage of Customs electronic data. This policy provides storage life-cycle schedules for keeping historical data on-line, archiving the data for long-term storage, destroying the data or transferring it to the National Archives Records Administration Federal Records Center for permanent retention.

E.4 Treasury Directives

Directive TD 25-04: *Implementation of the Privacy Act of 1974, as Amended*: This directive restates policy and procedures and assigns responsibilities for carrying out the requirements of the Privacy Act and authorizes TD P 25-04, "Privacy Act Handbook".

Publication TD P 25-04: *Privacy Act Handbook*: Contains detailed definitions of and procedures for Privacy Act Systems of records. Includes the text of the Privacy Act, Treasury Disclosure regulations and TD 25-04 as Appendices.

Publication TD P 71-10: *Department of the Treasury Security Manual*: The primary purpose of this manual is to establish comprehensive, uniform security policies, procedures, and guidelines to be followed by each bureau in developing its own specific policies and operating directives.

Publication TD P 81-01: *Treasury Information Technology (IT) Programs*: The IT manual provides uniform policies and general procedures for use by the bureaus and offices in carrying out their IT responsibilities in several areas including IT planning, IT architecture, telecommunications programs and services, information resources management, IT training, and IT standards, in accordance with the standards and guidelines issued by OMB, GSA, GAO and NIST.

Publication TD P 84-01: *Information System Life Cycle Manual (ISLC)*: Describes the procedures applicable to managing the full system development life cycle for Treasury ADP systems and/or applications. It addresses the aspects of requesting, identifying, defining, testing and implementing ADP systems and applications in varying levels of detail.

Publication TD P 85-03: *Risk Assessment Guideline, Vol 1 & 2*: This directive provides guidelines for identifying and quantifying potential areas of risk for ADP hardware and application software. It also provides a methodology for determining how to establish baselines for risk exposure and to minimize damage due to compromise, natural disaster, and system failure.

E.5 Laws Impacting Federal Technology Acquisition and Usage

Privacy Act of 1974 as amended: The act requires Federal agencies to adopt minimum standards for the collection and processing of personal information and to publish detailed descriptions of these procedures. It also limits the making of such records available to other public and private agencies or parties and requires agencies to make records on individuals available to them upon request, subject to certain conditions and exclusions.

Computer Security Act of 1987: The Act requires that agencies must ensure the security and privacy of sensitive information in Federal computer systems. It calls for the establishment of Security Plans and requires mandatory training for all persons involved in management, use or operation of Federal computer systems that contain sensitive information.

Americans with Disabilities Act of 1990: This act requires that federal agencies shall ensure that IT systems allow ready access to information or services normally provided by individuals with disabilities.

Chief Financial Officers Act of 1990: The purpose of this act is to bring more effective general and financial management practices to the Federal Government through statutory provisions. The goal is to improve the systems of accounting, financial management, and internal controls to assure the issuance of reliable financial information and to deter fraud, waste, and abuse of Government resources. In addition, it requires agencies to provide complete, reliable, timely, and consistent financial information to the executive branch of the Government and the Congress in the financing, management, and evaluation of Federal programs.

Government Performance and Results Act (GPRA) of 1993: The intent of GPRA was to shift the focus of government managers from expending resources to producing results. It stresses improvement of program effectiveness and public accountability.

Federal Acquisition Streamlining Act (FASA) of 1994 (Title V): In this legislation, Congress extended the affirmative action authority, granted to the Department of Defense, to all agencies of the federal government. The intent was to simplify acquisition of Federal procurements. FASA provided the executive branch with tools to improve the process for acquiring goods and services. FASA's changes were implemented in revisions to federal acquisition regulations, directives, and instructions

Paperwork Reduction Act of 1995: This act laid the foundation for electronic interface between the public and the federal government, by requiring federal agencies to reduce the amount of documentation required from the public to complete various government processes and procedures.

Federal Financial Management Improvement Act of 1996: In general the act requires each agency to implement and maintain financial management systems that comply substantially with Federal financial management systems requirements, applicable Federal accounting standards, and the United States Government Standard General Ledger at the transaction level.

Information Technology (IT) Management Reform Act of 1996 (ITMRFA): Transfers the responsibility for overseeing government I&T acquisitions from GSA to OMB. It also established the position of CIO for each agency.

Federal Acquisition Reform Act of 1996 (FARA): This law supports the simplification of the federal acquisition process by simplifying the competition process for acquisition, allowing more flexibility in obtaining commercial items (i.e., purchase card), and revising the personnel aspects of the acquisition process (procurement integrity and acquisition workforce management)

Government Paperwork Elimination Act of 1998: This legislation requires agencies to pursue acquisitions and use of information technology, including alternative information technologies that provide for electronic submission, maintenance, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures.

Rehabilitation Act Amendments of 1998, Section 508: This requires that when Federal departments or agencies develop, procure, maintain or use electronic and information technology, they shall ensure that the technology is accessible to people with disabilities, unless an undue burden would be imposed on the department or agency.

E.6 OMB Circulars and Memoranda

Circular A-11: *Preparation and Submission of Budget Estimates*: Prescribes policies and procedures for preparing and submitting agency budgets to the Executive Branch.

Circular A-34: *Budget Execution*: Prescribes policies and procedures for executing budgets once approved and authorized by Congress and the Executive Branch.

Circular A-76: *Performance of Commercial Activities - Sections I and III*: These sections describe criteria to consider when performing a management study to determine whether an ADP system is needed.

Circular A-94: *Discount Rates to be Used in Evaluating Time-Distributed Costs and Benefits*: This circular establishes policy and sets guidelines for calculating depreciation and amortization of Federal tangible assets when evaluating costs and benefits. This circular is re-issued annually.

Circular A-109: *Major Systems Acquisitions*: Establishes guidelines for the acquisition of major IT systems, including any required support services and/or personnel.

Circular A-120: *Guidelines for the Use of Advisory and Assistance Services*: This circular establishes policy and sets guidelines for the appropriate use of advisory and assistance services obtained by contracts. It specifically identifies the types of services allowed to be contracted as well as delineating those actions prohibited from being contracted.

Circular A-123: *Management Accountability and Control*: This circular provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls.

Circular A-127: *Financial Management Systems*: This circular identifies policies and procedures that must be followed when developing, operating, evaluating, or reporting on financial management ADP applications. It also provides specific objectives that financial management systems must meet to comply with applicable law and guidelines from GAO, Treasury and OMB.

Circular A-130 *Management of Federal Information Resources* : This circular provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35.

Circular A-130, Appendix III: ***Security of Federal Automated Information Systems***: This appendix requires that appropriate security procedures be put in place for any automated information system and that the procedures will comply with all applicable security standards. It further requires that the procedures be adequately documented and that security awareness and training be conducted. It divides security functions into four categories: applications, personnel, information technology, and installation.

The primary action required is management certification that the procedures implemented comply with all regulations and standards. This creates a chain of accountability for all security measures in place. As part of this accountability, periodic reviews and re-certification of the security measures in use must be performed, although no intervals are specified.

OMB Memorandum M-97-02, dated October 25, 1996: *Funding Information Systems Investments*.

OMB Memorandum M-00-07, dated February 28, 2000: *Incorporating and Funding Security in Information Systems Investments*.

OMB Memorandum-M-00-13, dated June 22, 2000: *Privacy Policies and Data Collection on Federal Web Sites.*

E.7 Code of Federal Regulations (CFR), Federal Information Resources Management Regulations (FIRMR)

CFR 41, Chapter 201-1.000-1 — 201-33.012: ***Federal Information Resources Management Regulations***: Identifies aspects of ADP functions and operation, including hardware acquisition and disposal, software development (internal vs. external), and security measures (physical and software), etc. These subject descriptions are general in nature, leaving compliance procedures to the individual agencies. Current Treasury directives and Customs handbook already comply with applicable CFR guidelines.

FIRMR Bulletin 90-3: ***Replacement of, and Screening For, Federal Information Processing (FIPS) Equipment Under Exchange/Sale Authority***: This bulletin outlines procedures to be used in conjunction with exchange/resale of Federal Information Processing equipment no longer required by a Federal office or agency.

E.8 Federal Information Processing Standards (FIPS) Publications

FIPS Publication 73: ***Guidelines for Security of Computer Applications***: Describes the categories of security that must be considered when developing an ADP system or application. Identifies decisions that should be made at each point in development, and describes some control measures that can be used.

FIPS Publication 87: ***Guidelines for ADP Contingency Planning***: Although this document is fairly old (March 1981), it remains the primary document on this topic from NIST.

FIPS Publication 102: *Guidelines for Computer Security Certification and Accreditation*: Sets forth the methods for establishing security certification and accreditation. Technically, a system or applications dealing with confidential data must be tested and approved by an appropriate security validation procedure before it can be activated.

FIPS Publication 113: *Computer Data Authentication*: Specifies a cryptographic authentication algorithm for use in ADP systems and networks where cryptographic authentication is necessary.

FIPS Publication 140: *General Security Requirements for Equipment Using the Data Encryption Standard*: Adopts Federal Standard (Fed-Std) 1027 as FIPS.

FIPS Publication 161-1: *Electronic Data Interchange (EDI)*: Adopts as a FIP the recognized national and international standards for Electronic Data Interchange (EDI) (X.12 and EDIFACT). In EDI data normally transmitted via paper documents is transmitted electronically according to established rules and formats. The data associated with each type of document (such as purchase orders or invoices) are transmitted with the document as an electronic message. Electronic transmission can be by means of telecommunication or by use of some electronic storage medium (such as magnetic disk or tape). The standard requires that any deviation from the standard document content or format must be submitted to NIST for approval along with a timetable for adopting the standard format. Also asks that documents not currently standardized by the study groups be submitted for evaluation and standardization.

E.9 National Computer Security Center Guidelines

NCSC-TG-015: *A Guide to Understanding Trusted Facility Management*: This technical guide provides compute security manufacturers, system evaluators, accreditors, auditors, developers, and end-users with concepts, relevant procedures, methods, and processes for trusted facilities management.

NCSC-TG-016: *A Guide to Writing Trusted Facility Management*: This technical guide provides computer security manufacturers, system evaluators, accreditors, auditors, developers, and end-users guidance for writing, evaluating, and using a trusted facility manual.

NCSC-TG-026: *A Guide to Writing the Security Features User's Guide (SFUG) for Trusted Systems*: This guide expands on the Trusted Computer System Evaluation Criteria by providing guidance on the development and evaluation of SFUG.

E.10 Other Guidelines

GAO/AIMD - 10.1.23: *Information Technology Investment Management*: A framework for assessing and improving process maturity of the investment management process.

***The Capability Maturity Model: Guidelines for Improving the Software Process*:** The Capability Maturity Model for Software (CMM) developed by the Software Engineering Institute® is a framework that describes the key elements of an effective software process. The

CMM describes an evolutionary improvement path for software organizations from an ad hoc, immature process to a mature, disciplined one.

Index

A

B

C

D

E

F

G

H

I

L

M

O

P

Q

R

S

T

U

V

W