

Approval Date: 4/29/05
Expiration Date: 9/30/05

INTERIM AGENCY SYSTEM LIFE CYCLE MANAGEMENT PROCEDURES

1. Purpose

The purpose of the System Life Cycle Management Procedures is to amplify the information provided in EPA's System Life Cycle Management Policy to aid those involved in developing and using Agency information systems.

2. Background

EPA is committed to managing its information systems in a cost-effective manner and ensuring its systems meet mission needs since such systems are the lifeblood of the Agency. EPA depends on information to accomplish its mission, and the Agency's data and associated information systems are among its most valuable assets and are critical to EPA's ability to provide reliable environmental information.

Information resources increasingly consume an ever larger share of the Federal Budget. New laws and regulations, in particular the Clinger-Cohen Act of 1996, the Federal Information Security Management Act of 2002, and OMB Circulars A-11 and A-130, require EPA to ensure that its life-cycle management procedures are comprehensive and up-to-date. Development of information systems is difficult, often complex, and expensive. Agency system life-cycle management requirements are designed to meet applicable Federal laws and regulations, ensure management involvement at key decision points, obtain and sustain Agency commitment, and coordinate information systems-related activities.

The System Life Cycle Management Procedures provides for the integration of system life-cycle management with IT Investment Management, specifically Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA), and information security procedures and practices. As information systems are increasingly interconnected over the Internet, security concerns have become of paramount importance. Security considerations, activities and documentation are *required at every phase* of the system life cycle.

3. Authorities

This Procedures document is issued under the authority of EPA's System Life Cycle Management Policy.

4. System Life Cycle Phases and Subphases

All EPA information system development or acquisition projects must be organized and managed as an ordered series of SLC phases. These phases must be documented in the System Management Plan (SMP) created specifically for each project by the System Manager. Any adjustments to these phases must be fully and completely documented in the SMP through appropriately approved waivers. Although discussed sequentially, it is *not* the intent that EPA systems must be managed in a linear fashion. Large or complex EPA systems must be organized and managed in a series of release cycles tailored from the following:

A) Definition Phase defines an EPA business problem and documents the purpose and scope of the proposed information system.

- **Initiation Subphase** establishes the existence of an EPA business problem that may be solved by the development of an information system.
- **Concept Definition Subphase** verifies the business problem, identifies high-level requirements that must be met to solve the problem, and outlines a feasible, timely, and cost-effective solution to the problem. This subphase should characterize or reassess any existing characterization of the information's and information system's sensitivity levels and identify any existing or potential management and operational controls for the business area. Prior to beginning any EPA information system development effort, existing systems and sources should be thoroughly researched for suitability to meet identified requirements.
- **Requirements Definition Subphase** determines the detailed functionality, standards, and security required of the proposed system based on business requirements and risk management principles.

B) Development or Acquisition Phase utilizes the information developed in the previous phase to assess and evaluate the development and/or acquisition of products and services. This phase will be repeated if the project requires multiple release cycles.

- **Design Subphase** begins the actual design of the intended system based on requirements and IT architectural consideration. The design specifies automated vs. manual functions and procedures, computer programs, data-storage techniques, and technical control mechanisms that address the sensitivity requirements of the system. The data standards are codified by OEI OIC. The conformity review is conducted during this subphase. This subphase may be optionally divided into High-Level Design and Detailed Design.
- **Construction Subphase** codes and tests the program modules that implement the design against the stated requirements and design specifications. System maintenance, operations and training documentation are developed.

C) Implementation Phase installs the system in the production environment. Data is converted

as needed, security features are configured and enabled, and sample testing is conducted to verify the system and its security. Written authorization to process must be completed during this phase prior to beginning operations.

- **Testing Subphase** tests the system to ensure that it works as specified in the requirements and design specifications (including revisions controlled through the configuration management processes) and that it meets applicable Federal, Agency and organization standards of performance, reliability, integrity, and security. Testing should also ensure that data names, definitions, and formats used in data exchange mechanisms conform to EPA data standards.
- **Implementation Subphase** releases and deploys the new system to all required users within the Agency and to external users, where required, and conducts training for all users, operations, and maintenance personnel.

D) Operations and Maintenance phase continues use of the new or modified system by the Agency, resolves problems not detected during testing, improves the performance of the product, and modifies the system to meet changing requirements. Significant new development or enhancement must be managed as a new development cycle. Any changes to the general support system on which an application resides need to be evaluated and may stimulate a new release cycle.

E) Termination Phase ends the operation of the system in a planned, secure, orderly manner. This phase is identified as an SLC phase but is not identified as a separate cost accounting phase. System components and data are archived or incorporated into other systems as required and hardware is disposed of.

5. System Life-Cycle Management Activities

All EPA information system development or acquisition projects must implement life-cycle management activities in tandem with the SLC phases:

A) Project Planning which establishes reasonable plans for building the system and controlling the project. It involves establishing a work breakdown structure, developing estimates of the planning parameters for the work to be performed, identifying project risks, establishing the necessary commitments, and developing the plan to perform the work.

B) Project Tracking which provides visibility into and control of the project progress to ensure that the project plan is being followed. It involves tracking project performance against the project plan, monitoring risks, taking corrective actions when there are significant discrepancies between performance and the plan. Progress is primarily determined by comparing actual system size, effort, cost, and schedule against those projected in the plan.

C) Component Management which manages the acquisition of software components from sources external to the project. It identifies software to be acquired, identifies and selects suppliers, establishes agreements with suppliers, accepts delivery of the acquired software, and ensures its maintenance and support. (This is required only for projects having separately acquired components.)

6. System Life-Cycle Support Activities

All EPA information system development or acquisition projects must implement life-cycle support activities in tandem with the SLC phases:

A) Configuration Management which establishes and maintains the integrity of the developmental and managerial products through the system life cycle. This involves identifying the configuration of the developmental products at given points in time (i.e., those products identified as configuration items), controlling changes to these products, and maintaining the integrity of these baselines through the system life cycle.

B) Quality Assurance which objectively reviews the project's activities and products for adherence to applicable requirements, processes, standards (including data standards), and procedures. It involves identifying and documenting non-compliance issues, providing feedback to project staff, development personnel, and managers, and ensuring that non-compliance issues are addressed.

C) Records Management which incorporates records management and archival functions into the design, development, and implementation of information systems. This involves establishing record schedules for both system development products and for the data contained in the system, if necessary.

D) Security Management and Assurance which includes designating an accountable manager and security personnel; determining information sensitivity and associated threats; assessing and managing risk; developing a security plan, ensuring that information security requirements and controls are identified for the system to reduce the risks; ensuring that technical security controls are incorporated and tested (certified); specifying security implementation limitations (residual risks); and authorizing (accrediting) the information system in writing before operations commence. Security considerations, activities and documentation are *required at every phase* in the SLC.

7. Cost Accounting

EPA managers must account for information system costs according to the cost accounting phases defined in EPA's cost-accounting policy. Costs incurred in a given SLC phase or subphase must be reported under the corresponding cost-accounting phase.

Figure 1. Crosswalk Translation of System Life Cycle Phases to Cost Accounting Phases

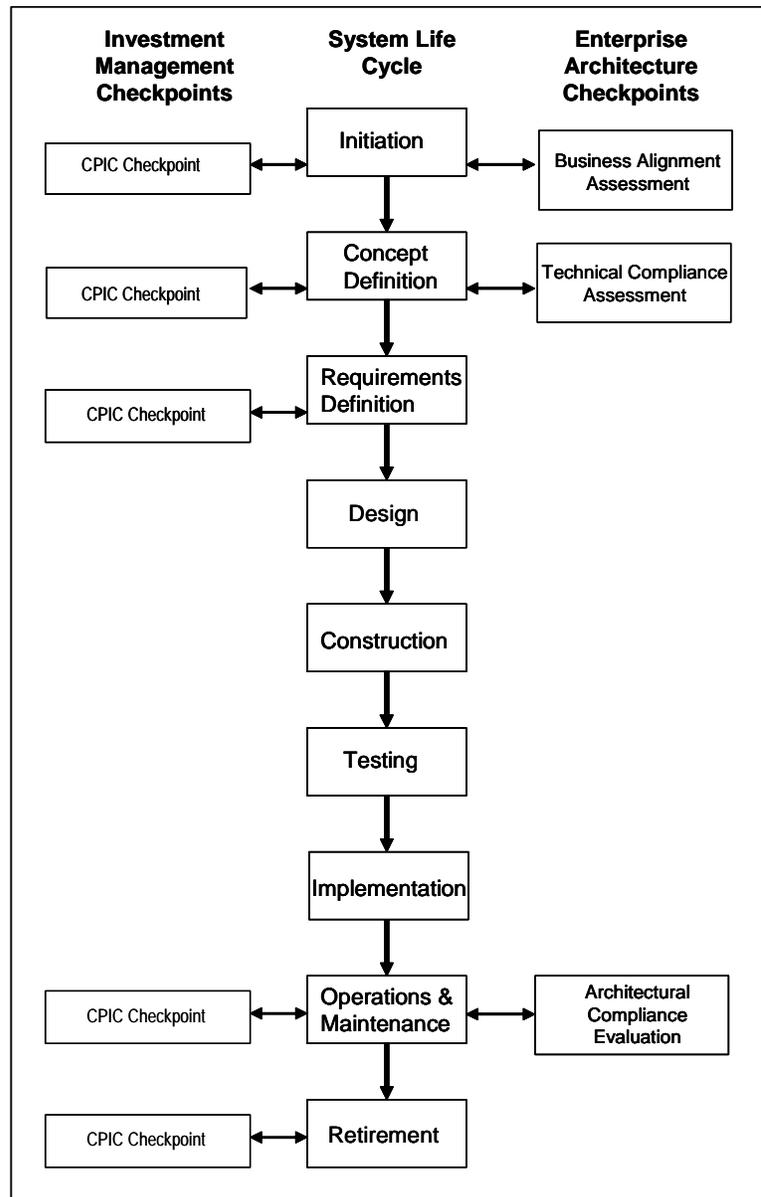
SLC Phase	Cost Accounting Phase
Definition	Preliminary Design
Development or Acquisition	Development
Implementation	Maintenance
Operation and Maintenance	
Termination	

8. IT Investment Management (CPIC and EA) Review

In accordance with the Clinger-Cohen Act (CCA), EPA information systems must be developed according to a structured process that includes planning, allocation, and management of funds, and must undergo quantitative and qualitative investment evaluation reviews. In addition to the SLC, EPA requires that two additional processes be followed to support the CCA: (1) the Capital Planning and Investment Control Process (CPIC), an annual process for agencies to report to OMB about IT performance, and (2) the Enterprise Architecture (EA) process, a process to align EPA IT architecture and investment management functions. Because these three processes are closely integrated, “checkpoints” are required to assure communication and a coordinated development effort.

System owners must ensure the necessary CPIC and architectural reviews take place. Figure 2 shows the required checkpoints as horizontal arrows between the SLC column and the CPIC and Enterprise Architecture columns. The System Manager must ensure the necessary documentation required by the CPIC and EA processes is prepared and submitted for review. These checkpoints help the System Manager determine if the system development is aligned with the business investment and technical architecture. Responsible offices involved in each of these areas must closely coordinate with each other prior to and during these checkpoints. CPIC and enterprise architectural checkpoints must be completed before an information system can advance.

Figure 2. CPIC, SLC, and Enterprise Architecture Relationships



9. System Management Plan

The System Management Plan (SMP) is the primary managerial document in the life of an information system and is required for all information system projects. The sections of the System Management Plan are listed below, although some may be waived with appropriate approval as specified in the System Life Cycle Management Policy:

- Change Tracking Log
- Mission Need Statement
- Business Case
- System Operations and Maintenance Concept
- Responsibilities
- Cost-Benefit Analysis Summary
- Schedule
- Project Risk Management Plan
- Security Plan
- Project Quality Assurance Plan
- Configuration Management Plan
- Review Sections
 - Data Standards
 - Enterprise Architecture (EA) Alignment
 - Capital Planning and Investment Control (CPIC)
- Approvals (Decision Papers)
- Waivers
- Application Deployment Checklist

SMP sections are defined at the end of the next section, along with the system life cycle products.

The SMP is a living document, created by the System Manager in the Initiation Subphase and continually updated and supplemented through the Operations and Maintenance Subphase. The level of detail of each section of the SMP should be consistent with the size of the system it documents. SMP requirements are the same for both general support/infrastructure systems and programmatic/administrative systems.

10. System Life Cycle Products

The System Manager is responsible for producing all required SLC products consistent with the SLC phases. Figure 3 shows the EPA system life-cycle phases and the major products for each phase. The two columns to the right indicate if the product is being developed for the first time (*Initial*), or if a previously developed product is being updated (*Updated*). The system life-cycle products are described at the end of this section.

Figure 3. System Life Cycle Products

<u>SLC Phase/ Subphase</u>	Products	
	Initial	Updated
Initiation	Initiation Decision Paper System Management Plan Assignment of Responsibility for Security	
Concept Definition	System Concept Document Security Concept Security Risk Assessment Cost-Benefit Analysis	System Management Plan
Requirements Definition	Requirements Decision Paper Functional Requirements Specification Requirements Traceability Matrix System Test Plan Security Plan	System Management Plan Cost Benefit Analysis Security Risk Assessment
Design	Development Decision Paper System Design Document Data Conversion Plan	System Management Plan Functional Requirements Specification Requirements Traceability Matrix System Test Plan Security Plan
Construction	System Modules (code) User/System Documentation	System Management Plan Functional Requirements Specification Requirements Traceability Matrix System Test Plan Security Plan Security Risk Assessment Data Conversion Plan
Testing	System Implementation Plan User Training Plan Authorized Processing Document Technical Vulnerability Assessment Cottingency Plan/COOP Security Test & Evaluation (ST&E) Report Certifier's Statement	System Modules (test) Security Risk Assessment System Management Plan Functional Requirements Specification Requirements Traceability Matrix System Test Plan Security Plan Data Conversion Plan User/System Documentation

Implementation	Implementation Decision Paper Authorization to Process	System Modules (implement) System Management Plan Functional Requirements Specification Requirements Traceability Matrix Security Plan Security Risk Assessment User Training Plan User/System Documentation System Implementation Plan
Operations & Maintenance	Customer Feedback Evaluation Re-authorization to Process Security Controls Review	System Modules (operational) Technical Vulnerability Assessment System Management Plan Security Plan Security Risk Assessment
Termination	Retirement Decision Paper System Disposition Report Archived/Incorporated Data Archived/Incorporated Software Archived Life-cycle Products	Security Plan Security Risk Assessment

Products may be in the form of written documents, graphics, electronic files, or system modules. Many of these products will be started in one life-cycle phase and updated periodically in subsequent phases to reflect the progress achieved during the project. They may vary in length and amount of detail, but collectively they document key decisions and approvals for the continuation and direction of the project and provide necessary system definition information to the project team and end users of the system.

Deviations from prescribed project deliverables must be documented in the System Management Plan with an explanation of how project risk will not be elevated if a product is not produced.

Description of EPA SLC Products

Archived/Incorporated Data - Stored data in archive locations designated by the System Disposition Report.

Archived/Incorporated Software - Stored software in archive locations designated by the System Disposition Report.

Archived Life-Cycle Products - Stored life-cycle products, including system documentation, in archive locations designated by the System Disposition Report.

Application Deployment Checklist - A checklist of activities/requirements that applies to applications and systems being deployed on National Technology Services Division managed platforms. It aids in a smooth deployment by identifying the activities that should take place

during implementation. Depending on the type and size of the system, the activities on the checklist will vary but may include delivery of hardware, delivery of communications equipment, coordination of commercial software with suppliers and the deployment team, and site preparation. Deployment is particularly challenging when a system is fielded incrementally; during the transition, newly installed systems must be able to interface with legacy systems or exchange data with other sites. This product is a component of the SMP.

Assignment of Responsibilities for Security - A document that officially assigns an individual the responsibility for the security of a general support system or major application.

Authorization to Process - A management control, consisting of a document signed by the management official responsible for a general support system or major application. (This management official is sometimes referred to as the “Designated Approving Authority.”) It authorizes an information system to operate, prior to beginning processing or use of the system. Authorization is equivalent to the term “accreditation.” For a system, the authorization is based on implementing the system security plan. For an application, the authorization is based on confirming that the security plan(s) implemented for the systems on which the application operates, adequately secure the application. Results of the most recent tests and/or assessments are factored into management authorizations. Management authorization implies accepting the risk of each system used by the application (derived from Appendix III, OMB Cir. A-130).

Authorized Processing Document - Produced during the testing subphase prior to implementation, either at the very end of testing or very beginning of implementation. Developed by the management official authorizing the use of each general support system and major application. This official cannot be the person assigned the responsibility for the security of the general support system or major application. Authorization must be based on the Security Plan because the plan defines the security controls for the general support system or major application. The manager must determine if the plan, as implemented, provides adequate security. Management's signature means that they accept the risk associated with processing and they agree that the general support system or major application is at an acceptable risk level. Authorization to process must be obtained prior to operation or upon significant modification. **General support systems and major applications must be re-authorized at least every three years.** For major applications, results of the most recent review or audit of controls shall be a factor in management authorizations. This could be as little as one page or multiple pages.

Business Case - The compelling business rationale and justification for developing or modernizing a system. It describes current business processes, possibly using activity and data models. Current costs and performance are also associated with the models. Gaps between current and desired outcomes are identified and analyzed. Alternatives for improving the business are developed and evaluated based on readily available information. This product is a component of the SMP.

CPIC Review - Includes the analysis of how the conceptual system will address Capital Planning and Investment Control (CPIC) requirements. Any CPIC documents that might need to

be generated in the Select Phase are identified. It includes a determination as to where the project falls within CPIC thresholds. It also includes development and submission of CPIC Select Phase documents. This product is a component of the SMP.

Certifier's Statement - Provides an overview of the security status of the system and brings together all of the information necessary for the Designated Approving Authority to make an informed, risk-based decision. The statement documents that the security controls are correctly implemented and effective in their application. The report also documents security controls not implemented and provides corrective actions.

Change Tracking Log - documents changes to the SMP, and is the first section of the SMP.

Configuration Management (CM) Plan - Identifies configuration items, specifying which configuration items are placed under CM control. It contains the baseline for the CM activities for the project and defines the starting point at which the project CM activities are monitored and tracked. It contains the procedure used to apply technical and administrative direction and oversight to identify and document the functional and physical characteristics of an item or system, control any changes to the characteristics, record and report the changes and their implementation status, and audit the item or system to verify conformity to requirements. The plan comprises four major areas of effort: configuration identification, configuration status accounting, configuration change control, and configuration audits. This product is a component of the SMP.

Contingency Plan/Contingency of Support Plan - A plan to ensure the capability to perform an Agency function supported by an application in the event of failure of its automated support. **An untested plan is not considered a viable plan** (derived from Appendix III, OMB Cir. A-130).

Cost-Benefit Analysis - Documents costs and proposed benefits of alternatives. Time-phased costs and both tangible and intangible benefits are estimated. Financial and decision analysis techniques are used to evaluate the alternatives and make a recommendation. Evaluation metrics promulgated by OMB may include discounted life-cycle costs and benefits, net present value, discounted return on investment, discounted payback period, and internal rate of return.

Cost-Benefit Analysis Summary - Highlights of significant information included in the Cost-Benefit Analysis. This product is a component of the SMP.

Customer Feedback Evaluation - Document used by the customer or user to indicate satisfaction, dissatisfaction, or recommended changes to a system and its performance.

Data Conversion Plan - Describes the specific data preparation requirements and the data that must be available for the system conversion. If data are to be transported from the original existing system, a detailed description of the data handling, conversion, and loading procedures is included. If the data are to be transported using machine-readable media, the characteristics of

those media are described.

Data Standard Review - A process for evaluating Agency program systems for conformity with existing EPA data standards and any standards under development. Standards conformity reviews should take place during system design to ensure that new and reengineered applications meet EPA data standards. Conformity reviews can be performed at any time during the system life cycle, potentially necessitating system requirements modification. This product is a component of the SMP.

Decision Papers - A decision document presented to management. It summarizes those aspects of the analysis and decisions of a given phase or subphase that are important to program management and requests approval to continue the project. The EPA life-cycle model provides for decision papers to be prepared at the beginning of the Definition, Development or Acquisition, Implementation, and Termination Phases and at the end of the Requirements Definition Subphase. The level of detail for decision papers should be appropriate to the category of the system. All decision papers are included in the SMP as attachments.

Enterprise Architecture Alignment Review - Includes the cumulative results of all Enterprise Architecture system reviews. It documents technical, data, or business areas in which the system being developed must align with EPA's Enterprise Architecture and includes discussion and guidance on how to make the system compliant. It may also include acceptance of new architectural components not previously part of the EPA's architecture. This product is a component of the SMP.

Functional Requirements Specification (FRS) - Identifies and describes functional requirements, non-functional (system) requirements, data requirements/data dictionary, information (data) quality requirements, Section 508 compliance requirements, and user support/system help requirements.

Mission Need Statement - Documents the results of a mission analysis, serves as the decision document for the mission need decision, and after final approval, serves as the basis for investment analysis. It provides a clear, unambiguous, and quantitative description of the mission area, current capability, capability shortfall or technological opportunity, required operational capability, impact of disapproval, benefits, time frame, criticality, and resource estimate. This product is a component of the SMP.

Project Quality Assurance Plan - Provides guidance on the development of products created during the life-cycle process to ensure they are substantively accurate and conform to a standard project management structure and meet certain quality factors. Quality factors present general goals for developing a high-quality system. Quality assurance is accomplished through the

efforts of designated quality assurance personnel on the project team, usually through a series of independent formal reviews and auditing activities. This product is a component of the SMP.

Project Risk Management Plan - Identifies and categorizes risks to the successful completion of the project. Lists each identified risk, describing its probability of occurrence, potential consequences, and degree to which it can be controlled. Strategies for eliminating or mitigating each risk are documented. Risks and the effectiveness of risk management actions are continually monitored and the plan changed accordingly throughout the life of the project. This product is a component of the SMP.

Re-authorization to process - The same as authorization to process except re-authorizations occur subsequent to the initial authorization. **Re-authorizations occur at least every three years or prior to significantly changing the use or processing of the information system.** It should be done more often where there is a high risk and potential magnitude of harm. Results of the most recent review or audit of controls must be factored into management re-authorizations (derived from Appendix III, OMB Cir. A-130).

Requirements Traceability Matrix (RTM) - Closely linked to the System Test Plan, this matrix lists user requirements, as documented in the Functional Requirements Specification, and tracks how they are addressed across the life cycle. In the Design and Construction subphases, each requirement is mapped to a design or construction element. In testing, the RTM identifies which test script will test each requirement and may be used to track testing completion. The RTM assists maintenance personnel by tracking each requirement to the appropriate document and section.

Responsibilities - Located in the SMP, this product describes the roles and responsibilities of the key participants in the system life-cycle development process. It identifies, by name, the System Sponsor, System Owner, System Manager, and other points-of-contact. It lists the organization(s) supporting the system and delineates organizational responsibilities.

Schedule - A time frame for system development activities to occur based on the estimates developed in the previous phases, as well as task dependencies, organization priorities, and resource availability. Adjustments are made throughout the life cycle based on enterprise goals, objectives, and priorities. Schedule adjustments also take into account task dependencies and resource availability. This product is a component of the SMP.

Security Concept - A preliminary analysis of security considerations for the new system. It provides the first look at the information that might be included in the Security Plan. Areas considered include risks from theft, disclosure, unauthorized access, eavesdropping, programmed attacks, incorrect routing, misplacement, erasure, and accidental damage. Includes an analysis of the sensitivity of data stored in the system.

Security Controls Review - A review or audit of the security controls in each information system. **Required at least every three years or when significant modifications are made to the system.** Systems may have self reviews; applications require independent reviews or audits. The scope and frequency of the review should be commensurate with the acceptable level of risk

for the system. **A deficiency pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act is identified if there is no assignment of responsibility for security, no security plan, or no authorization to process controls.**

Security Plan - Describes the plan to meet security and privacy requirements. It addresses risks, including those from theft, disclosure, unauthorized access, eavesdropping, programmed attacks, incorrect routing, misplacement, erasure, and accidental damage. This product is a component of the SMP.

Security Risk Assessment - Qualitative determination of risk to a collection of sensitive data and the people, information systems, and installations involved in storing and processing that data. Its purpose is to determine how protective techniques can be effectively applied to minimize potential loss (derived from EPA Order 2195.1A4, Agency Network Security Policy, and EPA Directive 2195A1, EPA Information Security Manual). It is the test to determine if the system meets the required security and privacy requirements as described in the Security Plan. Security system testing includes addressing risks from theft, disclosure, unauthorized access, eavesdropping, programmed attacks, incorrect routing, misplacement, erasure, and accidental damage. The Security Plan is updated, as necessary, based on findings and vulnerabilities associated with the Security Risk Assessment. A formal or comprehensive security risk assessment would typically include a Technical Vulnerability Assessment (TVA). A formal risk assessment, which includes a TVA, must be implemented on any new system during the testing subphase. The results of this formal risk assessment must be fully reflected and addressed in that system's security plan prior to implementation.

Security Test and Evaluation (ST&E) Report - Documents the initial ST&E of a system under development. The developmental ST&E is conducted at a central integration and test facility or at one of the intended operating sites if a test facility is not available.

System Concept Document - Key document of the Concept Definition Subphase. The functional portion describes the results of all significant functional analyses conducted during this subphase, including definition of high level requirements, assessment of pertinent existing information processing capabilities, complete formulation of alternative system functional concepts, assessment of the alternatives, and rationale for the selection of the recommended concept. The data portion describes high-level data requirements for the recommended system concept, provides definitions of these requirements, charts the logical structure of the data requirements, and describes sources, uses, and distribution of data. It defines the system concept, and includes, if applicable, a feasibility study, alternatives analysis, and acquisition strategy.

System Design Document - Describes the external and internal requirements of the system. Externally, it describes the operating environment and design characteristics of the system. It is used with the Functional Requirements Specification to provide a complete system specification of all user requirements. Internally, it presents the detailed system and subsystem designs that

will be used in developing the system. It contains the database design, file structures, input formats, output layouts, and design unit processing logic to be used by the system. It may contain the context diagram, object class diagrams, data flow diagrams, interface design, logical data model, metadata definitions, physical database design (a database file), Section 508 compliance design, and user support/system help design.

System Disposition Report - Describes the rationale for ceasing system operations, documents the plan for ceasing operations and effectively archiving the various components of the system, including hardware, and provides information about the location of archived materials. This report is vital to ensure that information about the system can be accessed to support reactivation of the system, or future reuse of portions of the current system by other systems.

System Implementation Plan - Describes how the system is to be installed and implemented as an operational system. It contains an overview of the system, a brief description of the major tasks involved in the implementation, the overall resources needed to support implementation effort (such as hardware, software, facilities, materials, and personnel), and any site-specific implementation requirements. The System Implementation Plan is first developed during the Testing Subphase and is updated during the Implementation Subphase.

System Management Plan - The core document that provides the overall framework for the management of the system development. It is created during the Initiation Subphase and updated in the next seven subphases of the system life cycle. Additional documentation is added as the life cycle progresses.

System Modules (code, test, implementation, operational) - Development units that include the source code modules, object code modules, load modules, and job control streams developed to automate the required business functions. Although these modules are not typically documents but files that reside on the developed system, source code and job control listings can be printed and included in system documentation for each unit/module. System modules are created during the Construction, Testing, Implementation, and Operations and Maintenance Subphases.

System Operations and Management Concept - It describes the general manner in which the system will be managed to include the level of operational support required. It identifies whether the system will be distributed to the Regions or operated from a central location. It describes how the system will be extended to a user's desktop, i.e., whether it requires a support person to install a client component or the system is Web-based with no client footprint required. It identifies the number and locations of required servers. It estimates the number of operational support personnel and provides an estimate of the number of hours per user required to support the system annually. It identifies the number of users expected by organization and location. This product is a component of the SMP.

System Test Plan - Defines all aspects of system testing. It is created in the Requirements Definition Subphase and refined through the Design, Construction and Testing Subphases.

Designed to ensure that all aspects of the system are adequately tested and that the system can be successfully implemented, the System Test Plan documents the scope, content, methodology, sequence, responsibility for, and management of test activities. It describes the various levels of testing (Unit/Module, Integration, System Qualification (including stress and external interface testing), System Acceptance, and Security) in progressively greater levels of detail as the system is developed. Test scripts may be included in the System Test Plan or maintained separately. The System Test Plan is closely associated with the Requirement Traceability Matrix.

Technical Vulnerability Assessment (TVA) - Implemented using automated proprietary or public domain software tools to scan a network or system for security vulnerabilities. These software tools contain checks for recently released vulnerabilities and custom attacks. Typically, these tools generate a report that identifies the vulnerabilities, specifies the level of severity, and provides the required remediation actions. A TVA is usually included as part of a formal or “comprehensive” security risk assessment. Depending on the sensitivity of the system these tools may also be used routinely.

User/System Documentation - User documentation is prepared for the system user and describes functionality and operation of the system. System documentation describes the behind-the-scenes functions required of system operators and documents the internal design and construction of the system.

User Training Plan - A detailed plan to ensure that each user has the necessary skills and knowledge to interact with the developed system in the user’s specific role.

Waivers - Written justification for deviating from the system life cycle process or for omitting sections of the SMP. Waivers may be considered based on the requirements of the system and needs of the developing office. Any waivers for Major Applications and General Support Systems and systems considered to be Major Investments in the Capital Planning and Investment Control (CPIC) process must be concurred with by the System Owner and applicable Senior Information Resources Management Official and approved by the Director of the Office of Environmental Information’s Office of Technology Operations and Planning. Waivers for any other applications and/or systems must be concurred with by the System Owner and approved by the applicable Senior Information Resources Management Official. Waivers must be documented as an attachment to the SMP.

11. COTS/GOTS Tailoring

EPA information system requirements should be met by COTS information systems or by systems developed in other government agencies whenever possible. Described below are potential ways a COTS or GOTS acquisition life cycle may be tailored through appropriate waivers. With further research the Agency may adopt a designated COTS/GOTS process, and, if

so, such a process will be documented in these procedures.

A) Definition Phase defines an EPA business problem and documents the purpose and scope of the proposed information system.

- **Initiation Subphase** establishes the existence of an EPA business problem that may be solved by the development of an information system.

Potential COTS/GOTS Tailoring: None necessary.

- **Concept Definition Subphase** verifies the business problem, identifies high-level requirements that must be met to solve the problem, and outlines a feasible, timely, and cost-effective solution to the problem. This subphase should characterize or reassess any existing characterization of the information's and information system's sensitivity levels and identify any existing or potential management and operational controls for the business area. Prior to beginning any EPA information system development effort, existing systems and sources should be thoroughly researched for suitability to meet identified requirements.

Potential COTS/GOTS Tailoring: Investigates COTS product alternatives or other government agency solutions applicable to the business area prior to system development, conducting an alternatives analysis and preliminary cost-benefit analysis, if necessary, to determine the best approach to meet the mission need.

- **Requirements Definition Subphase** determines the detailed functionality, standards, and security required of the proposed system based on business requirements and risk management principles.

Potential COTS/GOTS Tailoring: Identifies functional features that can be met by commercial or government products. The specified requirements must be sufficiently flexible or prioritized to assist in evaluating a variety of available commercial products and their associated fluctuations over time.

B) Development or Acquisition Phase utilizes the information developed in the previous phase to assess and evaluate the development and/or acquisition of products and services. This phase will be repeated if the project requires multiple release cycles.

- **Design Subphase** begins the actual design of the intended system based on requirements and IT architectural consideration. The design specifies automated vs. manual functions and procedures, computer programs, data-storage techniques, and technical control mechanisms that address the sensitivity requirements of the system. The data standard conformity review is conducted during this subphase. This subphase may be optionally divided into High-Level Design and Detailed Design.

Potential COTS/GOTS Tailoring: Adapts COTS/GOTS products through the use of “wrappers,” “bridges,” or other “middleware.” Adaptation and integration must take into account the interactions among custom components, COTS/GOTS products, any non-developmental item components, any legacy code, and the architecture, including infrastructure and middleware elements. For COTS/GOTS acquisitions, the Design and Construction Subphases may be combined.

- **Construction Subphase** codes and tests the program modules that implement the design against the stated requirements and design specifications. System maintenance, operations and training documentation are developed.

Potential COTS/GOTS Tailoring: Adapts, integrates and customizes the COTS/GOTS product without modifying it. If the selected COTS/GOTS product is not sufficiently “mature,” the system may require some manual (non-automated) action to perform the desired business process. The agency, contractor, COTS vendor, or system integrator also may need to perform some development work.

C) Implementation Phase installs the system in the production environment. Data is converted as needed, security features are configured and enabled, and sample and security testing is conducted to verify the system and its security.

- **Testing Subphase** tests the system to ensure that it works as specified in the requirements and design specifications (including revisions controlled through the configuration management processes) and that it meets applicable Federal, Agency and organization standards of performance, reliability, integrity, and security. Testing should also ensure that data names, definitions, and formats used in data exchange mechanisms conform to EPA data standards.

Potential COTS/GOTS Tailoring: Develops and implements test strategy and test plans that identify which features of the system are to be tested, i.e., only the COTS/GOTS features, or all features. It also identifies how one tests for failures in features that may have abnormal behavior due to unknown dependencies between the used and unused features of the COTS/GOTS product.

- **Implementation Subphase** releases and deploys the new system to all required users within the Agency and to external users, where required. Conducts training for all users, operations, and maintenance personnel.

Potential COTS/GOTS Tailoring: None necessary.

D) Operations and Maintenance Phase continues use of the new or modified system by the Agency, resolves problems not detected during testing, improves the performance of the product,

and modifies the system to meet changing requirements. Significant new development or enhancement must be managed as a new development cycle. Any changes to the general support system on which an application resides need to be evaluated and may stimulate a new release cycle.

Potential COTS/GOTS Tailoring: Updates by vendors of their COTS products or agencies of their GOTS products on their schedules and at differing intervals. Updates include elimination, change, addition, or combining of features for a release. COTS/GOTS must also consider general support system changes as well.

E) Termination Phase ends the operation of the system in a planned, secure, orderly manner, by archiving system components and data or incorporating them into other systems as required, and disposing of hardware. This phase is identified as a SLC phase but is not identified as a separate cost accounting phase.

Potential COTS/GOTS Tailoring: None necessary.

12. Quality Management System Development

The Systems Life Cycle Management Policy requires that all systems be developed in a rigorous manner that lessens and manages risk. In order to reduce the risk of failed systems, all *new* Major Applications and General Support Systems and systems considered to be Major Investments in the Capital Planning and Investment Control (CPIC) process will be developed using a methodology equivalent to at least the Software Engineering Institutes's (SEI) Capability Maturity Model (CMM) Level 3.¹ All such *existing* applications and systems, *not currently* compliant with CMM Level 3 (or equivalent) methodology, must develop and implement a plan ensuring that within four (4) years from the date of the Agency's System Life Cycle Management Policy, (December 29, 2003), they are being developed using a methodology equivalent to at least the SEI's CMM Level 3.

A) CMM Levels

SEI has defined five levels of software process maturity through which public and private organizations should progress from lowest to highest: Initial, Repeatable, Defined, Managed, and Optimizing. Each level is focused on and characterized by different elements of the development process, and sets higher standards as the process approaches the Optimizing level of maturity. Each level is associated with Key Process Areas (KPAs) that need to be

¹ The CMM was developed by the software community with stewardship by SEI, a federally funded research and development center established in 1984 by the U.S. Department of Defense. The program is operated through Carnegie Mellon University and is sponsored by the U.S. Office of the Under Secretary of Defense for Acquisition and Technology.

implemented for a project to meet that CMM level's standards.²

B) CMM Key Process Areas

Each CMM level is defined by the KPAs making up the level:

- Except for Level 1, each maturity level is decomposed into several KPAs that indicate the areas on which an organization should focus to improve its system development process. All KPAs for a given level must be addressed for an organization to achieve that maturity level.
- Each KPA identifies a cluster of related activities that, when performed collectively, achieves a set of goals considered important for enhancing process development capability. All the goals of a KPA must be achieved for the organization to meet the requirements of that maturity level.
- An organization is said to have reached a certain level if the organization has fully institutionalized every KPA at that level.

Figure 4 describes the focus, characteristics, and key processes that define each level of maturity.

Figure 4. CMM Levels and Related Key Process Areas

Level	Name	Focus	Characteristics	Key Process Areas
1	Initial	None	Unpredictable and poorly controlled	<ul style="list-style-type: none"> • None
2	Repeatable	Project management	Disciplined processes	<ul style="list-style-type: none"> • System configuration management • System quality assurance • System subcontract management • System project tracking and oversight • System project planning • Requirements management

²Although SEI developed the CMM for *software* development processes, the methodology is aptly applied to *system* development processes for EPA.

Level	Name	Focus	Characteristics	Key Process Areas
3	Defined	Engineering process	Standard, consistent processes	<ul style="list-style-type: none"> • Peer reviews • Inter-group coordination • System product management • Integrated system management • Training program • Organization process definition • Organization process focus
4	Managed	Product and process quality	Predictable processes that are measured and controlled	<ul style="list-style-type: none"> • System quality management • Quantitative process management
5	Optimizing	Continuous process improvement	Continuously improving processes	<ul style="list-style-type: none"> • Process change management • Technology change management • Defect prevention

13. Alternate Life Cycle Models

Development of EPA systems does not have to be through one life cycle model, variations are possible. Five Software Engineering Institute life cycle models appropriate for use are described below.

A) Waterfall Life Cycle Model

The waterfall approach has been in use for decades to develop commercial business applications such as payroll, general ledger, accounts payable, and others. During the Waterfall Life Cycle, the work is divided into well-defined stages and progress is controlled and managed by formal project management methods. Work progress is linear, meaning when the first stage is complete, work continues on the next, with no rework or iteration of the preceding stages.

This model is most effective in the development of systems with requirements that are well understood and can be fully specified before any detail design or coding of programs begins.

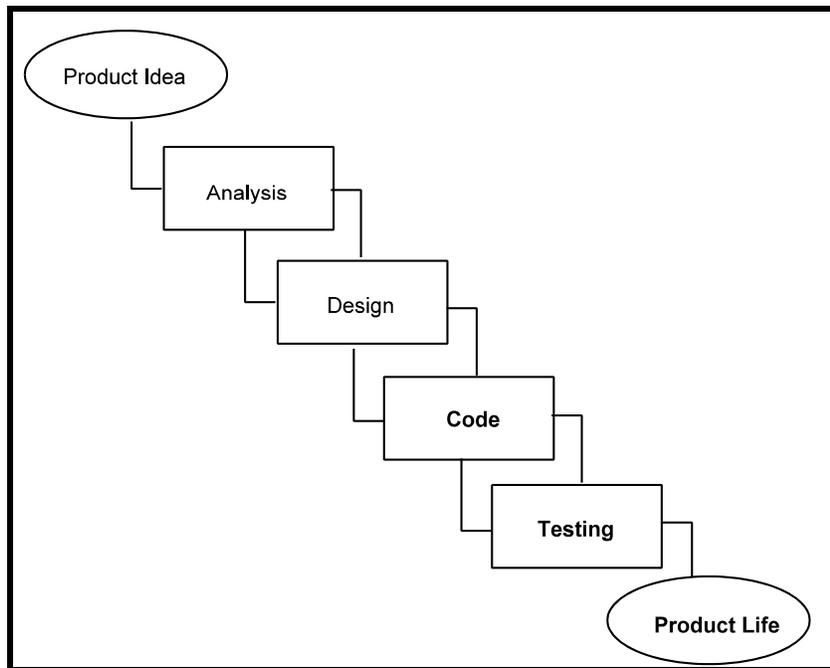


Figure 5. Waterfall Life Cycle Model

B) Rapid Prototype Life Cycle Model

Using a Rapid Prototype Life Cycle Model allows visualization of concepts and introduces the feasibility of the selected technical approach for the further development of the production system. Prototyping is a highly iterative process of building, using, evaluating, and refining a system to improve mutual understanding of the system between system developers and system users. This approach is appropriate when users cannot specify exactly what they want the system to do, or they need to explore alternative user interfaces to a system (e.g., input formats, screen displays, report formats, etc.).

Prototyping may also be used to develop a working version of a key subsystem to support testing to see if stringent performance requirements can be met.

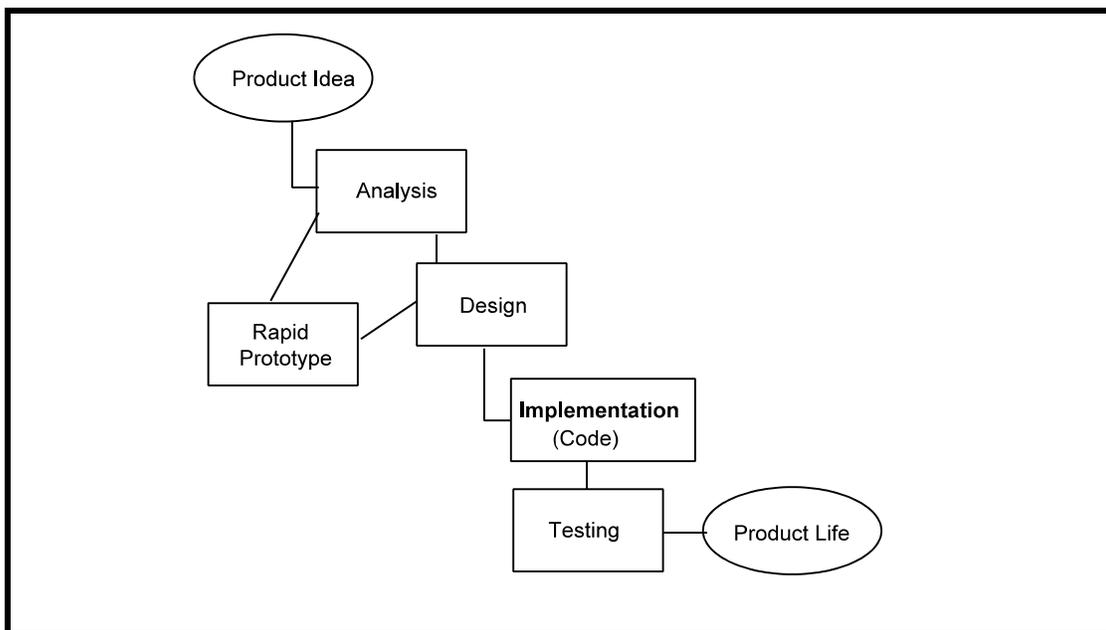


Figure 6. Rapid Prototype Life Cycle Model

C) Incremental Life Cycle Model

An Incremental Life Cycle Model is characterized by development of discrete modules of the system. Each module is developed following a selected software life cycle (e.g., Waterfall) and undergoes unit, integration, and system (acceptance) level testing before the next module is developed. Modules may be implemented independently as completed, or integrated at selected points in the life cycle.

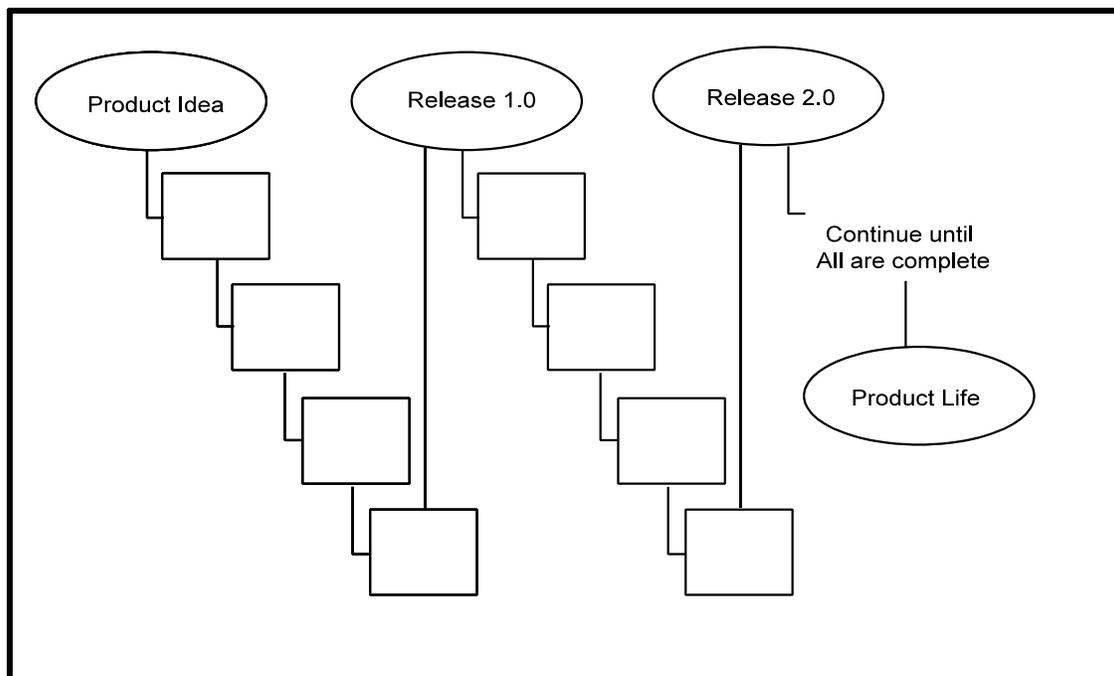


Figure 7. Incremental Life Cycle Model

D) Evolutionary Life Cycle Model

The Evolutionary Life Cycle Model maintains the step approach suggested by the Waterfall Life Cycle Model, but incorporates it into an iterative framework that more realistically reflects the real world. Developers and the customer can understand and react to risks at each evolutionary level. Prototyping is used as a risk reduction mechanism and enables the developer to apply the prototype approach at any stage in the evolution of the product.

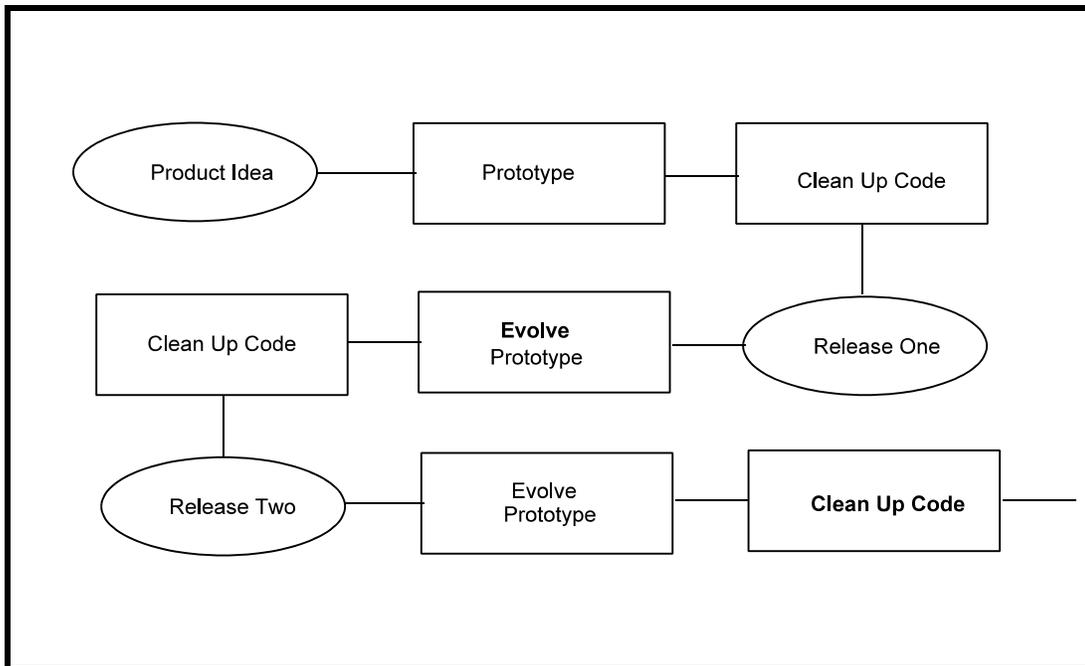


Figure 8. Evolutionary Life Cycle Model

E) Spiral Life Cycle Model

The Spiral Life Cycle Model encompasses the best features of both the Waterfall Life Cycle and prototyping models, while simultaneously adding a new element: risk analysis. The model divides the software engineering space into four quadrants: planning, risk analysis, engineering, and customer evaluation. Definitions of these quadrants are as follows:

- Planning: Determination of objectives, alternatives, and constraints.
- Risk Analysis: Analysis of alternatives and identification/resolution of risks.
- Engineering: Development of the “next-level” product.
- Customer Evaluation: Assessment of the results of engineering.

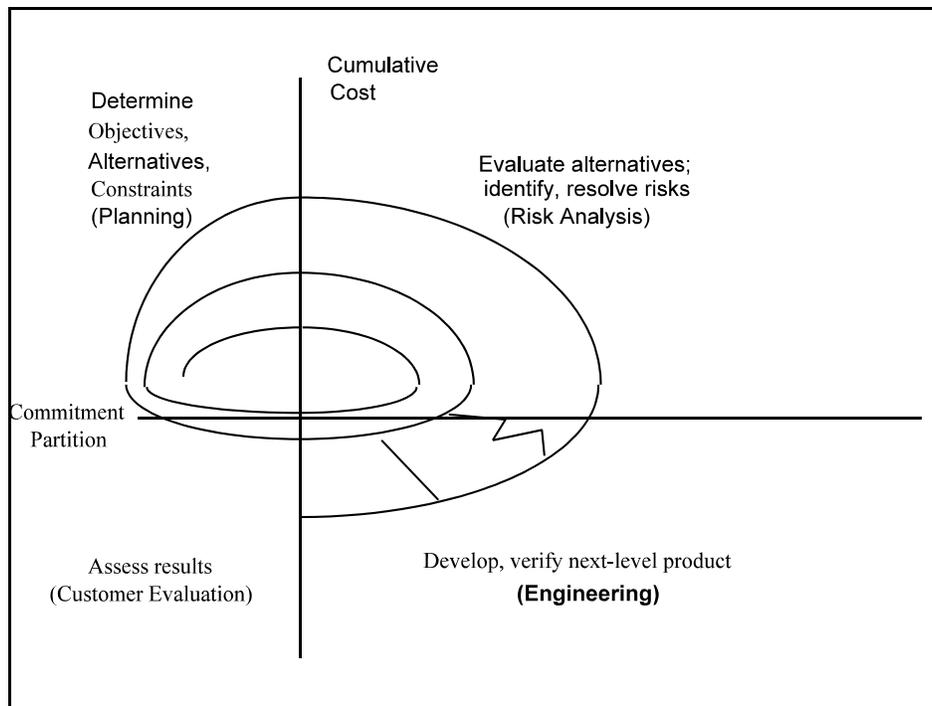


Figure 9. Spiral Life Cycle Model

Approve: _____/s/

Date: 4/29/05

Mark Day, Director
Office of Technology Operations and Planning