NIST Special Publication 800-64 Revision 2 (DRAFT)

National Institute of Standards and Technology
U.S. Department of Commerce

Security Considerations in the System Development Lifecycle (DRAFT)

Richard Kissel
Kevin Stine
Matthew Scholl
Hart Rossman
Jim Fahlsing
Jessica Gulick

I N F O R M A T I O N   S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

March 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Acting Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information security, and its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, and for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright regulations. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgements

The authors, Richard Kissel, Kevin Stine, and Matthew Scholl wish to thank their colleagues, Hart Rossman, Jim Fahlsing and Jessica Gulick from Science Applications International Corporation (SAIC), who helped update this document, prepare drafts, and review materials. In addition, special thanks are due our reviewers, Marianne Swanson and Elizabeth Lennon who greatly contributed to the document's development. A special note of thanks also goes to the original authors.

Table of Contents

Table of Figures

EXECUTIVE SUMMARY

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-64, *Security Considerations in the Information System Development Life Cycle,* has been developed to assist federal government agencies in integrating essential information technology (IT) security steps into their established IT system development lifecycle (SDLC). This guideline applies to all federal IT systems other than national security systems. The document is intended as a reference resource rather than as a tutorial and should be used in conjunction with other NIST publications as needed throughout the development of the system.

This publication serves a federal audience of information system and information security professionals, including information system owners, information owners, information system developers and program managers.

To be most effective, information security must be integrated into the SDLC from system inception. Agencies can then leverage increased return on investment in their security programs, such as.

- Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation;
- Awareness of potential engineering challenges caused by mandatory security controls;
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques;
- Facilitating informed executive decision making through comprehensive risk management in a timely manner;

This guide focuses on the information security components of the SDLC. First, descriptions of the key security roles and responsibilities that are needed in most information system developments are provided. Second, sufficient information about the SDLC is provided to allow a person who is unfamiliar with the SDLC process to understand the relationship between information security and the SDLC.

This document integrates the security steps into the linear, sequential (aka waterfall) SDLC. The five-step SDLC cited in this document is an example of one method of development and is not intended to mandate this methodology.

Lastly, SP 800-64 provides insight into IT projects and initiatives that are not as clearly defined as SDLC-based developments, such as service-oriented architectures, cross-organization projects, and IT facility developments.

CHAPTER ONE

INTRODUCTION

Consideration of security in the System Development Lifecycle is essential to implementing and integrating a comprehensive strategy for managing risk for all information technology assets in an organization. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-64 is intended to assist Federal government agencies to integrate essential security activities into their established system development lifecycle guidelines.

1.1 Purpose and Scope

The purpose of this guideline is to assist agencies in building security into their IT development processes. This should result in more cost effective, risk appropriate security control identification, development and testing. This guide focuses on the information security components of the SDLC. Overall system implementation and development is considered outside the scope of this document.

First, the guideline describes of the key security roles and responsibilities that are needed in development of most information systems. Second, sufficient information about the SDLC is provided to allow a person who is unfamiliar with the SDLC process to understand the relationship between information security and the SDLC.

The scope of this document is security activities that occur within a waterfall SDLC methodology. It is intended that this could be translated into any other SDLC methodology that an agency may have adopted.

1.2 Audience

This publication is intended to serve a diverse federal audience of information system and information security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, and authorizing officials); (ii) organizational officials having a vested interest in the accomplishment of organizational missions (e.g., mission and business area owners, information owners); (iii) individuals with information system development responsibilities (e.g., program and project managers, information system developers); and (iv) individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system security officers).

1.3 Value to Agency Missions, Security Programs and IT Management

Federal agencies are heavily dependent upon their information and information systems to successfully conduct critical missions. With an increasing reliability on and growing complexity of information systems as well as a constantly changing risk environment, information security has become a mission-essential function. This function must be conducted in a manner that reduces the risks to the information entrusted to the agency, its overall mission, and its ability to do business and to serve the American public. In the end, information security, as a function, becomes a business enabler through the proper and effective management of risks to information confidentiality, integrity, and availability.

Agencies may realize the value of integrating security into an established system development lifecycle in many ways, including:

- Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation;
- Awareness of potential engineering challenges caused by mandatory security controls;
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques;
- Facilitating informed executive decision making through comprehensive risk management in a timely manner;
- Documenting important security decisions made during development, ensuring management that security was fully considered during all phases;
- Improved organization and customer confidence to facilitate adoption and usage as well as governmental confidence to promote continued investment; and
- Improve systems interoperability and integration that would otherwise be hampered by securing systems at various system levels.

CHAPTER TWO

INFORMATION SYSTEM SECURITY AND THE SYSTEM DEVELOPMENT LIFE CYCLE OVERVIEW

Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete project and system development life cycle (see **figure 2-1**). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes to establish insight into the agency's vital business operations, their supporting assets and existing interdependencies and relationships. With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program's cost-effective performance as well as articulate its business impact and value to the agency.

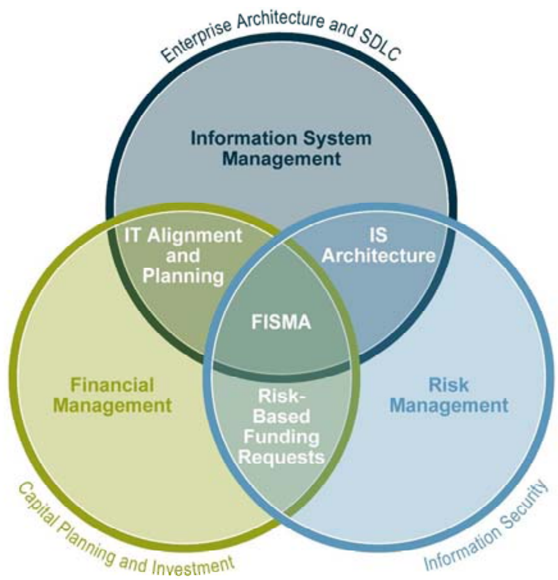

FIGURE 2-1. POSITIONING SECURITY CONSIDERATIONS

Executing a risk-management based approach for systems and projects means integrating security into the agency's established system and CPIC life cycles early and throughout. Integration enables security to be planned, acquired, built in and deployed as an integral part of a project or system. It plays a significant role in measuring and enforcing security requirements throughout the phases of the life cycle.

Life cycle management also helps document security-relevant decisions, in addition to helping assure management that security is fully considered in all phases. This documentation benefits system management officials as well as oversight and independent audit groups. System management personnel use this information as a self-check reminder of why decisions were made so that the impact of changes in the environment can be more readily assessed. Oversight and independent audit groups use the documentation in their reviews to verify that system management has done an adequate job and to highlight areas where security may have been overlooked. This includes examining whether the documentation accurately reflects how the system is actually being operated and maintained.

Many methods exist that can be used by an organization to effectively develop an information system. A traditional SDLC is called a linear sequential model (also known as waterfall method). This model assumes that the system will be delivered in its final stages of the development life cycle. Another SDLC method uses the prototyping model, which is often used to develop an understanding of system requirements without actually developing a final operational system. More complex systems require more iterative development models. More complex models have been developed and successfully used to address the evolving complexity of advanced and sometimes large information system designs. Examples of these more complex models are the: spiral model, component assembly model, and concurrent development model. The expected size and complexity of the system, development schedule, and length of a system's life will affect the choice of which SDLC model to use. In many cases, the choice of SDLC will be defined by an organization's acquisition policy.

This guide incorporates security into the linear sequential model of SDLC, because this model is the simplest of the various models, and it is an appropriate platform for this discussion. However, the concepts discussed can be adapted to any SDLC model.

Implementer's Tip

This guide does not provide an exhaustive description of the development and acquisition processes. (See the appropriate Federal Acquisition Regulations (FAR) and organization-specific policies and procedures for detailed acquisition information).

2.1 Establishing a Common Understanding

2.1.1 Agency SDLC Policy and Guideline

Each agency should have a documented and repeatable SDLC policy and guideline that supports its business needs and complements its unique culture. This agency SDLC guideline can be granular in nature or more objective in focus depending on the agency's IT management style, complexity of needs, and procurement preference. For example, some agencies maintain a development operation that builds and maintains systems while others outsource development and potentially maintenance as well. The former may require a more detailed procedure, while procurement-centric operations may need only objectives, service levels and deliverables detailed.

A general SDLC includes five phases: initiation, development, implementation/assessment, operations/maintenance, and disposal. Each phase includes a minimum set of security tasks needed to effectively incorporate security in the system development process. Note, phases may continue to be repeated throughout a system's life prior to disposal.

- Initiation. During the initiation phase, the need for a system is expressed and the purpose of the system is documented.

- Development. During this phase the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle.
- Implementation. After initial system testing, the system is installed or fielded.
- Operation/Maintenance. During this phase the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events.
- Disposal. Activities conducted during this phase ensure the orderly termination of the system, safeguarding vital system information, and migrating data processed by the system to a new system, or preserving it in accordance with applicable records management regulations and policies.

This SDLC related guideline provides utility by documenting:

- insight into the major activities and milestones;
- decision points or control gates;
- specified outputs that provide vital information into system design;
- project accomplishments; and
- system maintenance, security, and operational considerations.

This guideline should support, and be supported by, the agency's mission processes, enterprise architecture and financial processes.

2.1.2 Introduction to IT Security Integration

Executing a risk-management based approach for systems and projects means integrating security into the agency's established, system development and CPIC lifecycles. An integrated, security component (composed of milestones, deliverables, control gates, and interdependencies) that specifically addresses risk management (discussed in the next section) enables security to be planned, acquired, built in, and deployed as an integral part of a project or system. It also plays a significant role in measuring and enforcing security requirements throughout the lifecycle. Integrated security within the SDLC does not mean CPIC, IT and EA representatives consider security aspects but that they team with a security professional that informs, educates, and evaluates the appropriate levels of risk and protection levels. This separation of roles promotes security considerations and the training of personnel but should be reinforced by appropriate access for senior decision makers whom are outside the system developer chain.

Implementing information security early in the project allows the requirements to mature as needed and in an integrated and cost-effective manner. Engineering security into a product's initiation phase typically costs less than acquiring technologies later that may need to be reconfigured, customized or may provide more or fewer security controls than required. Security should be included during the requirements generation of any project. Designing a solution with consideration for security could substantially reduce the need for additive security controls (e.g., designing a house with two doors versus four requires less point-of-entry security and wiring the house for a security system and electricity at the same time precludes tearing holes in the walls later). This also allows for security planning at an enterprise level that allows reuse, decreases cost and schedule development, and promotes security reliability.

> *Implementer's Tip*
> Security activities should be physically and logically integrated into the agency's SDLC policy and guidelines versus maintaining them in a separate, complementary document or security lifecycle. This ensures a wider audience and decreases the need for the reader to reference multiple documents unnecessarily. Of course, security integration can and should reference supplemental process documents that provide further details.

The most effective way to accomplish the integration of security within the system development lifecycle is to plan and implement a comprehensive risk management program, also known as risk management framework (see section 2.1.5). This results in integrated security costs and requirements as well as an embedded, repeated, authorization process that provides risk information to IT stakeholders and developers throughout the agency.

2.1.3 Capital Planning & Investment Control Process

Each agency has an established and documented CPIC process in line with OMB A-11. NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, further articulates the integration and value of security. This guideline seeks to continue this discussion with a focus on security integration within the SDLC.

Key concepts from NIST SP 800-65 that should be considered when reading this guideline include:

- The CPIC process is defined by OMB Circular A-130 as "a management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes." Integrating security into this process ensures that information resources are planned and provided in a thorough, disciplined manner, enabling improved security for IT investments.
- Integrating security into the CPIC process consists of a seven-step methodology to ensure that mission and security requirements are met throughout the investment life cycle.
- While specific roles and responsibilities will vary from agency to agency, involvement at the enterprise and operating unit levels throughout the process allow agencies to ensure that capital planning and IT security goals and objectives are met.
- In concert with the OMB capital planning and NIST guidelines, agencies are required to adhere to the Government Accountability Office's (GAO) best practices, three-phase, investment life-cycle model for federal IT investments.
- Costs associated with implementing and assessing IT security controls and ensuring effective protection of federal IT resources should be accounted for in the capital planning process.

2.1.4 Security Architectures

Some agencies have established and documented security architectures in line with NIST guidelines consisting of security control families outlined in SP 800-53 with regard to protecting the confidentiality, integrity, and availability of federal information and information systems. A comprehensive security architecture acknowledges current security services, tools and expertise, outlines forecasted business needs and requirements, and clearly articulates an implementation plan aligned with the agency's culture and strategic plans. Usually, the security architecture is supplemented with an integrated schedule of tasks that identifies expected outcomes (indications and triggers for further review/alignment), establishes project timelines, provides estimates of resource requirements, and identifies key project dependencies.

2.1.5 Role in the NIST Risk Management Framework

NIST SP 800-64 complements the Risk Management Framework by providing a sample road map for integrating minimal but vital security milestones into an agency's SDLC. In addition, this publication provides further detail on additional activities that are valuable for consideration given that each system and agency culture varies. These additional activities supplement the risk management framework. A more detailed description of the NIST Risk Management Framework is presented in NIST Draft SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective.*

2.2 Legacy System Considerations

In many cases, organizations will be applying information security to legacy information systems that have been in operation for some extended period of time with a set of security controls already in place. Some legacy systems may have excellent security plans that provide comprehensive documentation of the risk management decisions that have been made, to include identifying the security controls currently employed. However, other systems may have little, if any, documentation available. For legacy information systems, although the system is in the operations and maintenance phase of the SDLC, the security considerations still apply and can be thought of as a potential system upgrade that represents a full SDLC from requirements identification and necessary development to implementation of the upgrade and back into operations and maintenance.

Implementer's Tip

Effective communication of security requirements and expectations is a vital and challenging step. The key is to document the security requirement in specific and measurable terms so that it clearly identifies who has the responsibility and accountability. The medium (memorandum, agreement or expectation document) as well as the granularity and complexity should be manageable and cost effective. This is a topic discussed throughout this publication.

2.3 Key Roles and Responsibilities in the SDLC

Many participants have a role in information system development. The names for the roles and titles will vary among organizations. Not every participant works on every activity within a phase. The determination of which participants need to be consulted in each phase is as unique to the organization as the development. With any development project, it is important to involve appropriate information security personnel as early as possible, preferably in the initiation phase.

A list of key roles is provided below. In some organizations, a single individual may hold multiple roles.

TABLE 2-1. KEY SECURITY ROLES AND RESPONSIBILITIES IN SDLC

Role	Responsibilities
Authorizing Official (AO)	An AO relies primarily on: (i) the completed security plan; (ii) the security test and evaluation results; and (iii) the plan of action and milestones for reducing or eliminating information system vulnerabilities, in making the security accreditation decision on whether to authorize operation of the information system and to accept explicitly the residual risk to agency assets or operations.
Chief Information Officer (CIO)	The CIO is responsible for the organization's information system planning, budgeting, investment, performance and acquisition. As such, the CIO provides advice and assistance to senior organization personnel in acquiring the most efficient and effective information system to fit the organization's enterprise architecture.
Configuration Management (CM) Manager	The CM manager is responsible for managing the effects of changes or differences in configurations on an information system or network. Thus, the CM manager assists in streamlining change management processes and prevents changes that could detrimentally affect the security posture of a system before they happen.
Contracting Officer	The Contracting Officer is the person who has the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.
Contracting Officer's Technical Representative	The COTR is a qualified employee appointed by the Contracting Officer to act as their technical representative in managing the technical aspects of a contract.
Information System Security Officer	The Information System Security Officer is responsible for ensuring the security of an information system throughout its life cycle.
Information Technology Investment Board (or equivalent)	The Information Technology (IT) Investment Board, or its equivalent, is responsible for managing the CPIC process defined by the Clinger-Cohen Act of 1996 (Section 5)
Legal Advisor/Contract Attorney	The legal advisor is responsible for advising the team on legal issues during the acquisition process.
Other Participants	The list of SDLC roles in an information system development can grow as the complexity increases. It is vital that all development team members work together to ensure that a successful development is achieved. Because the system certifier and accreditor, as well as the Information Security Officials must make critical decisions throughout the development process, they should be included as early as possible in the process. System users may assist in the development by helping the program manager to determine the need, refine the requirements, and inspect and accept the delivered system. Participants may also include personnel who represent IT, configuration management, design and engineering, and facilities groups.
Privacy Officer	The privacy officer is responsible for ensuring that the services or system being procured meet existing privacy policies regarding protection, dissemination (information sharing and exchange) and information disclosure.
Program Manager / Official (Information Owner)	This person represents programmatic interests during the SDLC process. The program manager, who has been involved in strategic planning initiatives of the SDLC, plays an essential role in security and is, ideally, intimately aware of functional system requirements.
QA/Test Director	The QA/Test Director is responsible for system evaluation and testing and functions as a resource across a variety of programs by assisting in the development and execution of test plans in conjunction with Program Managers and customers. Reviews system specifications and determines test needs, work with Program Managers to plan activities leading up to field test activities.
Senior Agency Information Security Officer (SAISO)	The SAISO, also known as Chief Information Security Officer, is responsible for developing enterprise standards for information security. This individual plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize information security risks to the organization. Information security program managers coordinate and perform system risk analyses, analyze risk mitigation alternatives, and build the business case

Role	Responsibilities
	for the acquisition of appropriate security solutions that help ensure mission accomplishment in the face of real-world threats. They also support senior management in ensuring that security management activities are conducted as required to meet the organization's needs.
Software Developer	The developer is responsible for programmatic coding regarding applications, software, and Internet/intranet sites, including "secure coding", as well as coordinating and working with the Configuration Management (CM) manager to identify, resolve, and implement controls and other CM issues.
System Architect	As the overall designer and integrator of the application, the system architect is responsible for creating the overall design architecture and for maintaining the conceptual integrity of the architecture throughout the project life cycle. The System Architect is also responsible for ensuring the quality of technical work products delivered by the project team, including designs, specifications, procedures and documentation.
System Owner	The system owner serves as the authority for all matters of security for the system. The system owner is responsible for developing functional requirements and verifying that the requirements are implemented securely.

CHAPTER THREE

INCORPORATING SECURITY INTO THE INFORMATION SYSTEM DEVELOPMENT LIFE CYCLE

This section describes a number of security considerations that will help integrate IT security into the SDLC. Security considerations are approached in each SDLC phase thus advancing the technical and security requirements together to ensure a balanced approach during development. **Figure 3-1**, organized by development phase, provides an overall view of the process.

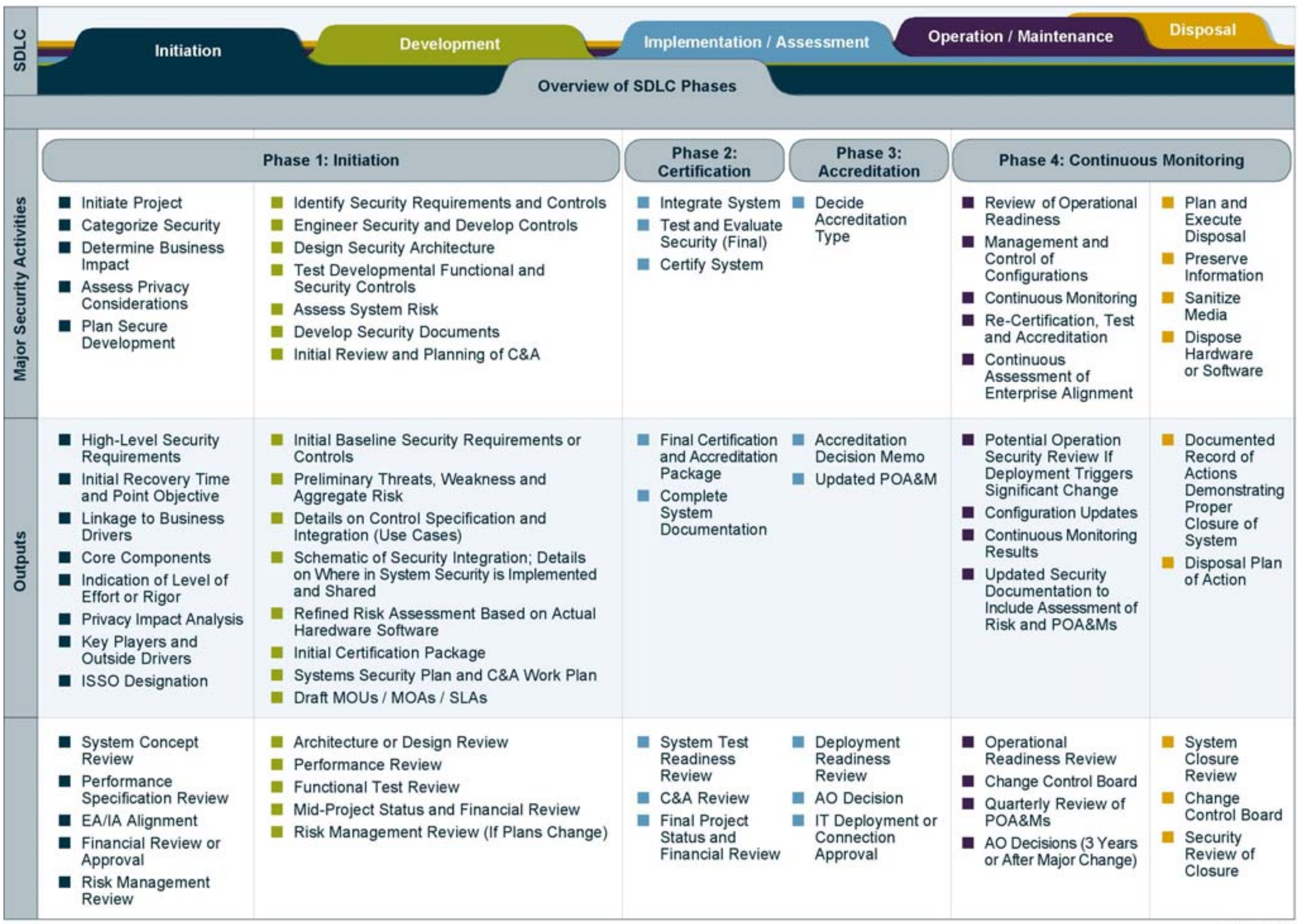

FIGURE 3-1.SECURITY IN SDLC – A CONCEPTUAL VIEW

In order to provide clear, concise guidance to the reader, each lifecycle phase is described in a section below that has been organized in this manner:

- Provide a brief description of the SDLC phase;
- Identify general control gates, or established points in the life cycle when the system will be evaluated and when management will determine whether the project should continue as is,

change direction, or be discontinued. Control gates should be flexible and tailored to the specific organization.

- Identify and describe major security activities in each phase that have security implications. Each activity is then further decomposed in the following areas:
  - Description. The description provides a detailed overview of the activity and highlights specific considerations necessary to address the task.
  - Expected Outputs. Common task deliverables and artifacts are listed along with suggestions for forward/backward integration of these work products into the SDLC.
  - Synchronization. A feedback loop that provides opportunities to ensure that the SDLC is implemented as a flexible approach that allows for appropriate and consistent communication and the adaptation of tasks and deliverables as the system is developed.
  - Interdependencies. This section identifies key interdependencies with other tasks to ensure that security integration activities are not negatively impacted by other IT processes.

3.1 SDLC Phase: Initiation

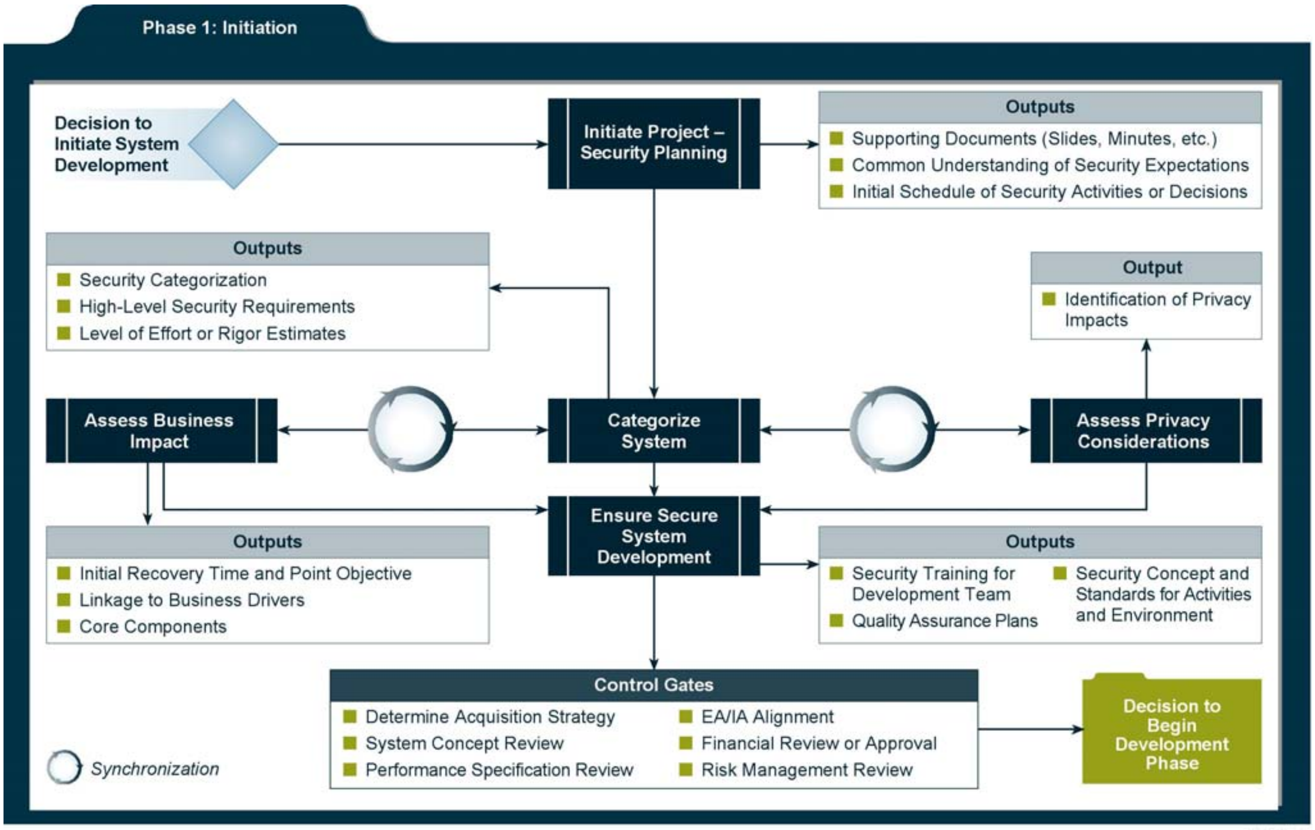

FIGURE 3-2.RELATING SECURITY CONSIDERATIONS IN INITIATION PHASE

3.1.1 Description

During this first phase of the development life cycle, security considerations are key to diligent and early integration thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered. At this point, security is looked at more in terms of business risks with input from the IT security office. For example, an agency may identify a political risk resulting from a prominent website being modified or made unavailable during a critical business period resulting in decreased trust by citizens. Key security objectives for this phase include:

- Initial delineation of business requirements in terms of confidentiality, integrity, and availability
- Determination of information categorization and identification of known special handling requirements to transmit, store or create information such as personally identifiable information
- Determination of any privacy requirements.

Early planning and awareness will result in cost and timesaving through proper risk management planning. Security discussions should be performed as part of (not separately from) the development project to ensure solid understandings among project personnel of business decisions and their risk implications to the overall development project.

3.1.2 Control Gates

General types of control gates for this phase may include:

- An information system security categorization review of identified information types, resulting impact levels, and final Security Categorization.
- A System concept review that verifies that the concept is viable, complete, achievable, and in line with organizational mission objectives and budgetary constraints.
- An enterprise architecture alignment that harmonizes IT vision, standards, business requirements, as well as security alignment with current and imminent security services.
- A performance specification review that ensures the initial system design has addressed all currently identified specified security requirements.
- A risk management review that conforms to the recommended NIST risk management framework guidelines to reduce ambiguity in managing system risk.
- A financial review that verifies the system will be aligned with CPIC artifacts and guidance while balancing the cost implications associated with risk management.

3.1.3 Major Tasks with Significant Security Integration Activities

3.1.3.1 Initiate Project – Security Planning

Description:	Security Planning should begin in the project initiation phase by: • Identifying key security roles for the system development • Ensuring all key stakeholders have a common understanding, including security implications, considerations, and requirements. • Outlining initial thoughts on key security milestones including time frames or development triggers that signal a security step is approaching. This early involvement will enable the developers to plan security requirements and associated constraints into the project. It also reminds project leaders that many decisions being made have security implications that should be weighed appropriately, as the project continues. Identification of Security Roles Identification of the ISSO is an important step that should take into consideration the amount of time the individual will devote to this task, the skills needed to perform the duties, and the capability the individual has to effectively carryout the responsibilities. Identifying the ISSO provides the individual key insights into risk associated decisions early in the process and provides the other team members access to the security office for support in integrating security into the system development. Stakeholder Security Integration Awareness The ISSO, with the assistance of the security office, provides the business owner and developer with an early understanding of the security steps, requirements, and expectations so security can

	be planned in from the beginning. Topics may include: • Security Responsibilities • Security Reporting Metrics • Common Security Controls Provided (if applicable) • Certification & Accreditation Process • Security Assessment Techniques • Security Document & Requirement Deliverables • Major activities with development schedule and resource impact such as active testing, accreditation, and training Initial Project Planning Developing an initial project outline for security milestones that is integrated into the development project schedule will allow proper planning as changes occur. At this stage, activities may be more in terms of decisions followed by security activities.
Expected Outputs:	• Meeting minutes or supporting documentation, such as slides. • Common understanding of security expectations. • Initial schedule of security activities or decisions.
Synchronization:	A series of milestones or security meetings should be planned to discuss each of the security considerations throughout the system development.
Interdependencies:	A project schedule should integrate security activities to ensure proper planning of any future decisions associated with schedules and resources.

Implementer's Tips
• Many of the project initiation artifacts (meeting minutes, briefings, role identification) can be standardized and provided to developers for proper level-of-effort planning. • An in-person meeting allows attendees an important opportunity to gauge understanding and awareness • If the agency identified the same individual for multiple systems, a planned approach will increase their ability to multi-process, such as assigning common systems or common organizations with ownership.

3.1.3.2 Categorize the Information System

Description:	Security categorization provides a vital step towards integrating security into the government agencies' business and information technology management functions and establishes the foundation for security standardization among information systems. Security categorization starts with the identification of what information supports which government lines of business, as defined by the EA. Subsequent steps focus on the evaluation of security in terms of confidentiality, integrity, and availability. The result is strong linkage between mission, information, and information systems with cost-effective information security. FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, provides a standardized approach for establishing security categories for an organization's information and information systems. NIST SP 800-60, the companion guideline to FIPS 199, provides a process roadmap and information taxonomy to categorize agency information systems. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization by operating an information system. FIPS Publication 199 defines three levels (i.e., low, moderate, or high) of potential impact on organizations or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability). The security categorization standards assist organizations in making the appropriate selection of security controls for their information

	systems.
Expected Outputs:	• Essential to the security categorization process is documenting the research, key decisions, and supporting rationale driving the information system, security categorization (this is included in the System Security Plan). • Initial level of rigor can be derived from applying the resulting security categorization to the minimal security controls in NIST SP 800-53.
Synchronization:	The security categorization should be revisited if major scope change occurs or when the business impact analysis is updated.
Interdependencies:	• Business Impact Analysis: Agency personnel should consider the cross-utilization of security categorization and Business Impact Analysis (BIA) information in the performance of each task activity. Since these activities have common objectives, agencies should mutually draw on these activities for each information system and use the results to ensure accuracy. • CPIC and EA: Just as no IT investment should be made without a business-approved architecture[1], the security categorization at the start of the security life cycle is a business-enabling activity directly feeding the EA and CPIC processes as well as migration and upgrade decisions. • System Design: Understanding and designing the system architecture with varying impact levels in mind may assist in achieving economies of scale with security services and protection through common security zones within the enterprise. This type of approach requires a solid understanding of an agency's information and data types gained through the security categorization process. • Contingency and Disaster Recovery Planning: Contingency and disaster recovery planning personnel should review information systems that have multiple data types of varying impact levels and consider grouping applications with similar, system-impact levels with sufficiently protected infrastructures. This ensures efficient application of the correct contingency and disaster protection security controls and avoids the over protection of lower-impact systems. • Information Sharing and System Interconnection Agreements: Agency personnel should utilize aggregated and individual security categorization information when assessing interagency connections.

Implementer's Tips

- To enable an appropriate level of mission support and the diligent implementation of current and future information security requirements, each agency should establish a formal process to validate system level categorizations in terms of agency priorities. This will not only promote comparable evaluation of systems, but also yield added benefits to include leveraging common security controls and establishing defense-in-depth.
- Agency personnel should review the appropriateness of the provisional impact levels in the context of the organization, environment, mission, use, and connectivity associated with the information system under review, to include: the agency's mission importance; lifecycle and timeliness implications; configuration and security policy related information; special handling requirements; etc.
- Even though information system security categorization may result in moderate or high impact system identification, the individual 800-53 security controls prescribed for confidentiality, integrity, and/or availability may be set at the high water mark identified for the individual security objective if the controls are truly independent and if cost or other concerns are a significant driver. For the latter, a risk management approach to the selection of security controls should be followed and any justifiable variances documented in the information systems security plan.
- Agency personnel should be aware that there are several factors that should be considered during the aggregation of system information types. When considering these factors, previously unforeseen concerns may surface affecting the confidentiality, integrity, and/or availability impact categorization at the system level. These factors include data aggregation, critical system functionality, extenuating circumstances, and other system factors.

[1] FEA Consolidated Reference Model Document, Version 2.1, December 2006

3.1.3.3 Assess Business Impact

Description:	An assessment of system impact on the agency lines of business correlates specific system components with the critical business services that are provided. That information is then used to characterize the business and mission consequences of a disruption to the system's components. An initial draft of this product early in the lifecycle alerts system stakeholders to key IT and security decisions. This task should also take into account the availability impact level identified during the security categorization task. Refer to NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, for a business impact assessment template.
Expected Outputs:	• Identification of lines of business this system supports and how they will be impacted? • What core system components are needed to maintain minimal functionality? • How long can the system be down before the business is impacted? (Initial idea of the needed Recovery Time Objective) • What is the business tolerance for loss of data? (Initial idea of the needed Recovery Point Objective)
Synchronization:	• This should be reviewed periodically and updated as major development decisions (such as new functionalities) occur or system's purpose and scope change significantly. • As the system matures, the BIA should be augmented with more detail on major IT components.
Interdependencies:	• The BIA is a key step in the contingency planning process. The BIA enables improved characterization of the system requirements, processes, and interdependencies and uses this information to determine contingency requirements and mitigating solutions. • The FIPS 199 Security Categorization activity's similarity in terms of inputs and purpose positions it as a complimentary activity that provides checks and balances to ensure all business drivers are adequately addressed.
Implementer's Tips	
• Some of this information can be derived from the original business case for the initiative. • For larger and more complex developments, consider holding a stakeholders meeting to brainstorm possible linkages and impacts. • Reuse data and information for multiple purposes when applicable. Categorization decisions can be reused for BIA, DR, CP, and COOP decisions. Categorization should be reflective of DR priorities. If not, there is potential that categorization was not conducted at an appropriate level or DR priorities are incorrect. • The results of a BIA can be used to develop requirements or objectives for service level agreements (SLAs) with supporting service providers.	

3.1.3.4 Assess Privacy Considerations

Description:	When developing a new system it is important to directly consider if the system will transmit, store, or create information that may be considered privacy information. This typically is identified during the security categorization process when identifying data types. Once identified as a system under development that will likely handle privacy information, the system owner should work towards identifying and implementing the necessary steps to enable proper safeguards and security controls. Many agency's have employed either a one or two-step model to address privacy considerations. The one-step model requires all systems on the agency's system inventory develop a privacy impact assessment that outlines criteria for privacy information determination and documents security controls employed to properly protect the information. In contrast, the two step model differentiates by processing all systems through a threshold analysis, which is focused on whether a privacy impact assessment should be performed. A positive answer would then result in the execution of a more detailed evaluation of privacy data and proper security controls in the form of a privacy impact assessment. The resulting document of either process would then be incorporated into the system security

	plan and maintained appropriately.
Expected Outputs:	Privacy Impact Assessment providing details on where and to what degree privacy information is collected, stored or created within the system.
Synchronization:	Should continue to be reviewed and updated as major decisions occur or system purpose and scope change significantly.
Interdependencies:	• A FIPS 199 Security Categorization is the initial step in identifying types of information such as privacy information. • Security controls identification and assessment would reflect whether additional controls are needed to protect the privacy information. • System Security Plan, Contingency Plan, Business Impact and Privacy Impact Assessments
Implementer's Tips	
• Governance for Privacy Information: Privacy Act of 1974, 5 U.S.C. § 552A • The E-Government Act of 2002 strengthened privacy protection requirements of the Privacy Act of 1974. Under the terms of these public laws, Federal government agencies have specific responsibilities regarding collection, dissemination or disclosure of information regarding individuals. • The September 29, 2003 OMB Memorandum, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" puts the privacy provisions of the E-Government Act of 2002 into effect. The guidance applies to information that identifies individuals in a recognizable form, including name, address, telephone number, Social Security Number, and e-mail addresses.	

3.1.3.5 Ensure Use of Secure Information System Development Processes

Description:	Primary responsibility for application security, during early phases, lies in the hands of the development team who has the most in-depth understanding of the detailed workings of the application and ability to identify security flaws in functional behavior and business process logic. This means that they are the first level of defense and opportunity to build in security. It is important that their role not be assumed or diminished. Communicating and providing expectations is key to planning and enabling an environment that protects down to the code level. Considerations to plan for include: *Secure Concept of Operations (CONOPS) for Development.* A concept of operations document for secure development should be established for the environment and a continuity of operations plan should be in place for the code repository as source code is the predominant work product of software and system development and should be preserved in the event of interruption to the development environment. *Standards and Processes.* System development should occur with standard processes that consider secure practices and are documented and repeatable. To accomplish this, system developers should determine and document appropriate secured processes for the assurance level required by the system they are developing. Thus, systems with a high assurance requirement may need additional security controls built into the development process. *Security Training for development team.* Additional security training may be needed for key developers to understand the current threats and potential exploitations of their products. This enables the developers to create more secure designs and empowers them to address key issues early in the development processes. *Quality Management.* Quality management, which includes planning, assurance and control, is key to ensuring minimal defects within and proper execution of the information system. This reduces gaps or holes that are sometimes left open for exploitation or misuse (whether intentionally or not) causing vulnerabilities in the

	system. *Secure Environment.* The system development environment should meet minimum FISMA compliance criteria as expressed in 800-53. This is to include workstations, servers, network devices, and code repositories. Development environments must be accredited as would any other operational system or environment. A secure development environment lends itself to developing secure software and systems. *Secure Code Practices and Repositories.* Special attention should be placed upon code repositories with an emphasis on systems that support distributed code contribution with check-in/check-out functionality. Role based access should apply to accessing the code repository and logs should be reviewed regularly as part of the secure development process. Code should be developed in accordance with standard practices. A necessary part of the aforementioned CONOPS is the establishment and retention of secure coding patterns and components. Secure coding patterns embody code level examples and accompanying documentation that illustrate how to meet specific functional requirements while simultaneously achieving security mandates. These patterns can then be re-used by developers to ensure that all software components are developed in an assured fashion having been vetted and adopted by the organization. When possible, completed software components that have passed security certification should be retained as reusable components for future software development and system integration. As a team, system developers and security representatives should agree on what steps can and should be taken to ensure valuable and cost effective contributions.
Expected Outputs:	• Plans for development phase security training. • Planned quality assurance techniques, deliverables and milestones. • Development and coding standards including development environment.
Synchronization:	Lessons learned from completed products and security testing should be evaluated for appropriateness in adjusting development processes and standards to prevent embedding weaknesses.
Interdependencies:	• IT development standards should contain appropriate methodologies that add value to the process and do not detract from security • System development training and orientation should include basic and specialized (to environment) security awareness, training, and education.

Implementer's Tips

- Understanding modern, application, security flaws and attack methods is essential to protecting the system against them. Providing application security training to the development and testing teams and will increase understanding of the issues and techniques and should enable the development of more secure systems. If developers are aware of what to look for and what to test during the development phase, the number of security defects released to QA should be reduced. In addition, if the QA test team is well educated in the area of application security, they are more likely to identify a security issue before the product is moved on to the next phase of testing. Such training should result in greater confidence in the overall security of the production system. Providing training in application security will also emphasize the importance of application security to the team.
- Any weakness known by the development team should be addressed as soon as possible. It is unwise to assume that complicated attacks requiring significant knowledge of the internal workings of the system are unlikely from malicious attackers. On more than one occasion, system owners have been surprised to find that attackers were able to “discover” information that the system owners assumed to be hidden.
- To reduce the possibility of security flaws in the system, security-focused additions should be investigated and incorporated into the existing coding standards or development guideline document. These standards should account for all types of software development languages used, such as C++, Java, HTML, JavaScript, and SQL.

3.2 SDLC Phase: Development

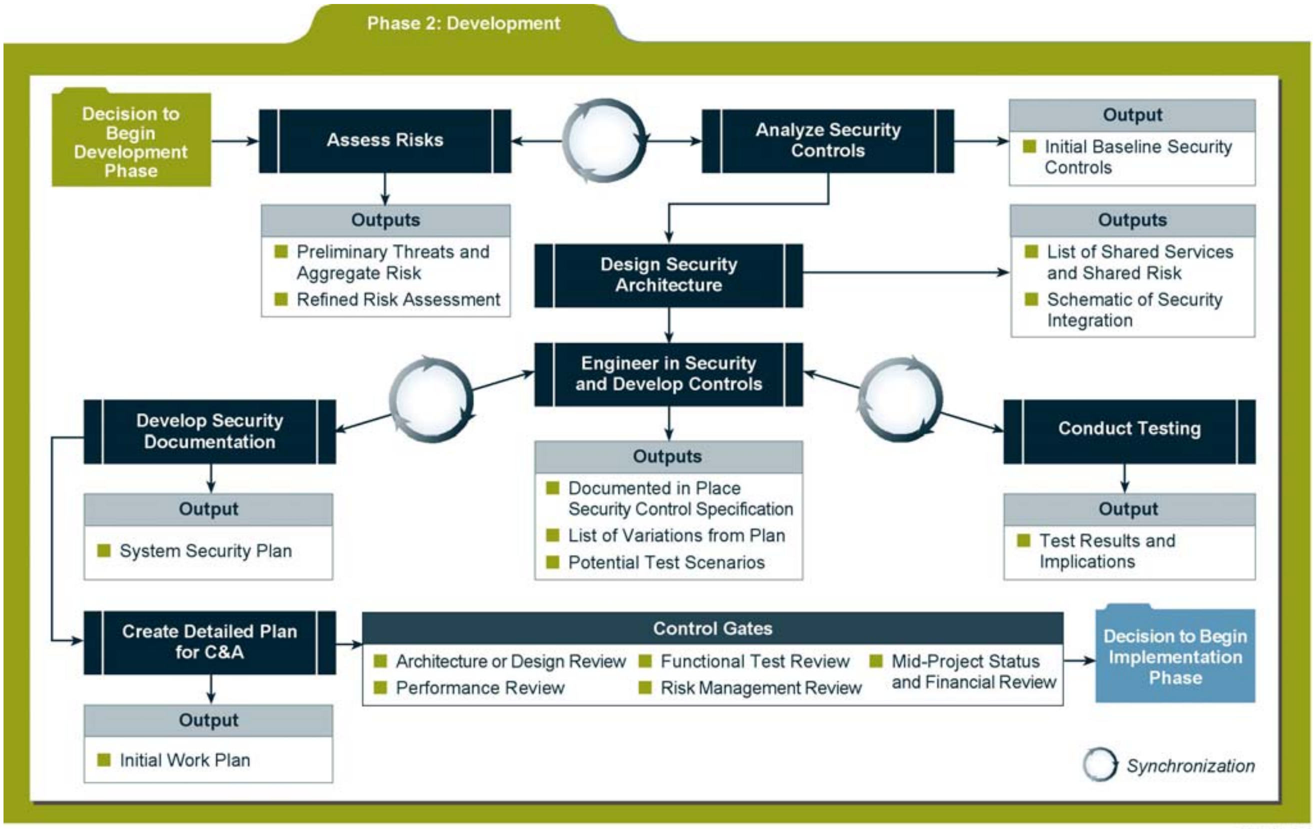

FIGURE 3-3. RELATING SECURITY CONSIDERATIONS IN THE DEVELOPMENT PHASE

3.2.1 Description

This section addresses security considerations unique to the second SDLC phase. Key security objectives for this phase include:

- Supplement the risk assessment
- Analyze security requirements
- Perform functional and security testing
- Prepare initial documents for system certification and accreditation

Although this section presents the information security components in a sequential top-down manner, the order of completion is not necessarily fixed. Security analysis of complex systems will need to be iterated until consistency and completeness is achieved.

3.2.2 Control Gates

General types of control gates for this phase may include:

- An Architecture/Design Review that evaluates the planned system design and potential integration with other systems as well as incorporation of shared services and common security controls, such as authentication, disaster recovery, intrusion detection, or incident reporting.
- A system Performance Review would evaluate whether the system is delivering or capable of delivering to the documented expectation of the owner. For example, the ability of the system to maintain availability and data integrity at the expected extreme resource loads.
- A system Functional Review that ensures functional requirements identified are sufficiently detailed and are testable.
- Mid-Project Status & Financial Review is important to detect major shifts in planned level of effort to ensure cost benefit ratios are monitored and effective decisions are continued.
- A follow-on review of risk management decisions may be needed if, due to the aforementioned reviews, the system and/or its security controls and/or its requirements change.

3.2.3 Major Tasks with Significant Security Integration Activities

3.2.3.1 Assess Risk to System

Description:	Agencies should consult NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, for guidance on conducting risk assessments. The purpose of this risk assessment is to evaluate current knowledge of the system's design, stated requirements and minimal security requirements derived from the security categorization process to determine their effectiveness to mitigate anticipated risks. Results should show that specified security controls provide appropriate protections or highlight areas where further planning is needed. To be successful, participation is needed from people who are knowledgeable in the disciplines within the system domain (e.g., users, technology experts, operations experts). The security risk assessment should be conducted before the approval of design specifications as it may result in additional specifications or provide further justification for specifications. In addition to considering the security perspective of the system being developed/ acquired, organizations should also consider how the system might affect other systems to which it will be directly or indirectly connected. This may mean that there are inherited common controls to leverage or additional risks that need to be mitigated. In these cases, an enterprise review may be needed to provide a more comprehensive view.
Expected Outputs:	A refined risk assessment based on a more mature system design that more accurately reflects the potential risk to the system, known weaknesses in the design, identified project constraints, and known threats to both business and IT components. In addition, previous requirements are now transitioning into system specific controls.
Synchronization:	Since this risk assessment is completed at a more mature stage of system development, there may be a need to revisit previously completed security steps, such as BIA or Security Categorization. Development rarely goes as planned and requirements have a way of changing.
Interdependencies:	• Security categorization provides the initial risk assessment information based on information types. • Additional security controls or compensating controls may be planned or modified based on the risk assessment to ensure effectiveness.
Implementer's Tips	

• Within any organization, the threat from internal sources remains the highest probability of occurrence. Improprieties by employees [system developers] who are also privileged system users are a real threat, especially since such employees may have active accounts within the system. Practices should include independent audits of the system and its supporting processes. Continuous monitoring and integrity based tools to ensure configuration audit and control may be of use by providing an automated, central, audit log collection, correlation, and analysis tool. • It is a good idea to monitor the National Vulnerability Database (http://nvd.nist.gov) for known component vulnerabilities and build in controls to mitigate them. These would then need to be tested. • When dealing with a system having multiple owners (sometimes across different domains), it is important to identify shared and inherited risks. • Depending on the rigor needed and the complexity of the system, it may be important to follow the data flow/information sharing beyond the first interface. Failure to do so may result in inheriting unknown risks. • Other inherited risks may be evaluated through the supply of materials for the system. Supply chain risk should be understood and evaluated to mitigate potential use of fraudulent, pirated, un-licensed or intentionally compromised material.

3.2.3.2 Analyze Security Control

Description:	The analysis of security controls is separate and more granular than the risk assessment but a highly linked activity. While the risk assessment defines what and why, the security requirements analysis seeks to determine how, when, where, and to what extent for the planned security controls. This process should include an analysis of laws and regulations, such as FISMA, OMB circulars, agency-enabling acts, agency specific governance, FIPS and NIST Special Publications, and other legislation and federal regulations that define applicable specifics to the established baseline security requirements. After a review of mandated requirements, agencies should consider functional and other security requirements. *Analysis of Functional Security Requirements:* This may include two sources of system security requirements: (1) system security environment, (i.e., enterprise information security policy and enterprise security architecture) and (2) functional requirements from security operations or services as well as security related business rules as appropriate. This is the primary source of actual requirements that are specific enough for implementation and test. NIST FIPS and SPs can be used to derive high-level requirements but must be specified through local security policies for effective implementation. *Analysis and Assurance of Security Requirements:* The correct and effective use of information security control requirements is a fundamental building block of information security. Assurance is the grounds for confidence that an entity will meet its security objectives. Assurance supports the confidence that the security controls being acquired will operate correctly and will be effective in the operational environment. This analysis should address the developmental activities required and assurance evidence needed to produce the desired level of assurance that the information security controls will work correctly and effectively. As with other aspects of security, the goal should be cost-effective implementation that meets the requirements for protection of an organization's information assets. In each situation, a balance should exist between the system security benefits to mission performance and the risks associated with operation of the system.
Expected Outputs:	• Initial Baseline Security Controls and Requirements –identification beyond the minimal security requirements that specifies where controls will be applied and how. • The formation of the building blocks for preliminary system-level security architecture.
Synchronization:	• Security controls and associated specifications should reflect appropriate levels of protection to the system in line with the security categorization. • Significant decisions should consider any possible secondary risks that may result should the decision influence previously considered security controls and protections identified during the risk assessment.

Interdependencies:	• Once formulated, security requirements will be incorporated into the System Security Plan. • The Risk Assessment is a primary tool to identify if required baseline security requirements are effective to address security assurance needs. If not, then additional control requirements must be selected until an acceptable level of security assurance is reached.
Implementer's Tips	
• Addressing security requirements in a matrix format that allows the developers and security engineers to review implementation per major system component can facilitate gap analysis and proper planning. • IT security requirements should be stated in specific terms. For complex systems, iterations of the requirements analysis may be needed. If so, planned reviews should occur at major SDLC milestones. • Any new functional requirement may have security implications. Introducing additional risk or weakening existing security controls is more likely if a specific security analysis is not performed. If security is not addressed specifically during requirements specification, then it would be possible for undocumented risk to enter the system. • More detailed "attack prevention" requirements will also help ensure security controls and methods are tested prior to release. If a documented requirement exists, then it is assumed that a test case will need to be developed and executed. • Security controls are not one-dimensional and should be addressed as appropriately on multiple components throughout the system. For example, if your system is composed of SQL servers, Web Sphere and a mainframe, then auditing may need to be planned for all, some or none depending on the system. Documenting this during this stage decreases the level of effort during testing.	

3.2.3.3 Design Security Architecture

Description:	With the increase in shared service providers and the centralization of some key security services within agencies, it is becoming more important to plan these services and understand how they will integrate into the system. An enterprise alignment of the system should ensure the initiative fits the agencies' future plans and does not conflict or unnecessarily provide redundant services. In addition, as the system matures and more decisions are made as to services utilized, the EA should be reviewed for optimal integration. At the system level, security should be architected and then engineered into the design of the system. This may be accomplished by zoning or clustering services either together or distributed for either redundancy or additional layers of protection. Security designing at the system level should take into consideration services obtained externally, planned system interconnections, and the different orientations of system users (e.g., customer service versus system administrators). Another example would be a system auditing strategy that should be developed to enable an accurate trace or reconstruction of all priority and high-risk work flows. The audit strategy should include various audit records from several different components including (but not limited to) the Web application, databases, mainframe, and Web servers. The goal should not be to capture as much audit information as possible but to capture only what is needed to provide enough information to investigate potential security breaches and system failures. This activity may be performed when reviewing from an IT development view the known bottlenecks and single points of failures. Minimal security requirements as well as requirements and constraints determined early in the process should provide the architects with a set of assumptions and constraints to build around. This activity can provide the most value for the system in lowering the total cost of ownership by planning the systems core components in a secure way.
Expected Outputs:	• Schematic of security integration; details on where, within the system, security is implemented & shared. • Security architectures should be graphically depicted and detailed to the extent the reader can see where the core security controls are applied and how. • Matured listing of shared services and resulting shared risk. • Identification of common controls used by the system.
Synchronization:	• The security architecture becomes a key component of the system documentation that should be reviewed and maintained as major changes or significant control gates (milestones) are

	reached. • Significant results from assessments, security testing, and reviews should be examined for potential feedback on effectiveness.
Interdependencies:	• Enterprise Architecture should provide insights into other like systems or services where integration is optimal. • System Security Plans will document the summary of the security architecture approach or strategy. • Security Requirements Analysis will provide the majority of the information at the detailed level. This will enable the architect to review the information, apply it theoretically at the system level, and determine if the controls will work as intended or if there are gaps or unnecessary redundancy.
Implementer's Tips	
• Security architecting can provide effective compensating controls when there are issues with implementing minimal security requirements with the system's design specification. Security architectures will also identify common controls that the system will inherit as well as who has responsibility for those common controls. • Demonstrating the logic behind the security of this system will help in determining the need for additional controls. • Risks accepted by the system that may have downstream, adverse affects on the enterprise can be identified and raised as issues during the architectural review. Enterprise risk culminating from all individual system risk should be expressed and tracked through the agency Enterprise Architecture process.	

3.2.3.4 Engineer in Security and Develop Controls

Description:	During this stage, security controls are implemented and become part of the system rather than applied at completion. Applying security controls in development should be considered carefully and planned logically. The intent is to integrate the controls so that challenges with system performance are known early. Additionally, some security controls may limit or hinder efficient development. For new information systems, the security requirements identified and described in the respective system security plans are now designed, developed, and implemented. The system security plans for operational information systems may require the development of additional security controls to supplement in place controls or the modification of controls that are deemed to be less than effective. During this task, decisions are made based on integration challenges and trade-offs. It is important to document the major decisions and their business drivers. In cases where the application of a planned control is not possible or advisable, compensating controls should be considered and documented.
Expected Outputs:	• Implemented controls with documented specification for inclusion into the security plan. • List of variations resulting from development decisions and trade offs. • Potential assessment scenarios to test known vulnerabilities or limitations
Synchronization:	Security control application may undergo changes as a result of functional and user testing. Changes should be documented.
Interdependencies:	• Security Requirements Analysis should be reviewed and updated if change is needed. • Security Architecture Strategy should be reviewed and updated if change is needed. • Specific configurations should be documented or reference in the System Security Plan.
Implementer's Tips	
Documenting security deviations at this stage will encourage solid risk planning and reduce time later in backtracking business justifications. In addition, it demonstrates evidence of risk planning.	

3.2.3.5 Develop Security Documentation

<table>
<tr><td>Description:</td><td>At this point in the SDLC, security documentation should begin taking form. The prominent document is the System Security Plan [NIST SP 800-18]. Supplements to it may include:
Configuration Management Plan
Contingency Plan (including a Business Impact Assessment)
Continuous Monitoring Plan
Security Awareness, Training and Education (SATE) Plan
Incident Reporting Plan
Privacy Impact Analysis
Development of these documents should consider how mature the security services being documented are. In some cases, these documents may contain only known requirements, common controls, and templates. Filling in these documents should begin as early as possible during the project.
At this stage, it is important to solidify the security approach, the proper scope, and an understanding of responsibilities. For example, the Disaster Recovery Plan may be covered by the connected General Support System, and SATE may be outsourced to a shared-service provider. In this case, the plans may focus on the system specifics and may reference key points from an in-place service-level agreement.
Documenting as you go provides cost savings and better decision making through a comprehensive approach that allows early detection of gaps. Perfection in documenting may cause unneeded iteration development and thus increase cost. Managing the expectation of details available is critical. For example, much time may be taken to write up a particular security control and then, due to functional testing, the control is replaced or discontinued.</td></tr>
<tr><td>Expected Outputs:</td><td>Security documentation supporting the system development and providing the foundation of the initial certification package.
Document the intended security approach to management and operational security controls that may not be clearly identified in the security architecture.</td></tr>
<tr><td>Synchronization:</td><td>These documents will need to be updated toward the end of user acceptance testing to ensure they are accurate.</td></tr>
<tr><td>Interdependencies:</td><td>Documentation should align with:
Security Requirements Analysis
Security Architecture
Business Impact Assessment, and
Security Categorization.</td></tr>
<tr><td colspan="2">Implementer’s Tips</td></tr>
<tr><td colspan="2">Security operations should not be driven by documentation of compliance but based on system need and described in compliance with security guidance.
Focus first on the SSP until it’s somewhat complete, and then begin scoping out documents.
For systems developed over long periods of time, it may be best to track security in terms of control application and then apply security to the SSP. If this approach is used, the controls should specify which core component is providing the control coverage (may be multiple).
On major systems that are large in size, complex in design, or politically sensitive, it is best to assign a POC to each document and initiate development with a meeting of the minds on the document’s scope, expectations, and level of granularity.</td></tr>
</table>

3.2.3.6 Conduct Developmental, Functional and Security Testing

Description:	Systems being developed or undergoing software, hardware, and/or communication modification(s) must be formally tested and evaluated prior to being granted formal accreditation. The objective of the test and evaluation process is to validate that the system complies with the functional and security requirements and will operate within an acceptable level of residual security risk. Testing of security controls is based on the assessment procedures detailed in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*. The process focuses on specificity, repeatability, and iteration. For repeatability, the testing process must be capable of the execution of a series of tests against an information system more than once (or against similar systems in parallel) and yield similar results each time. For iteration, each system will be required to execute functional tests in whole or in part a number of successive times in order to achieve an acceptable level of compliance with the requirements of the system. To achieve this, functional testing will be automated to the degree possible and the test cases will be published, in detail, to ensure the test process is repeatable and iterative. For specificity, the testing must be scoped to test the relevant security requirement as it is intended for use in its environment. The use of automated testing tools and integration of the NIST ISAP/SCAP should be accomplished prior to the commencement of security control test and evaluation activities. Any security functionality not tested during the functional or automated testing will be carefully examined to ensure compliance with the requirements during the explicit, security control test and evaluation. Only test or “stub” data should be used during system development. Absolutely no operational, security relevant, or PII data should reside within any system or software during development.
Expected Outputs:	Documentation of any variations in security testing as a result of challenges discovered during functional testing.
Synchronization:	All test results are returned to developers for configuration-managed updates. Erroneous results may require the customer to clarify the nature of the requirement.
Interdependencies:	• Security Requirements Analysis may be impacted and require updating. • Changes may impact the Security Architecture and require updating.

Implementer’s Tips

- In an effort to reduce redundant, functional and security, testing activities, it is recommended that functional test plans include general security features testing (to the greatest extent possible).
- Preliminary testing of basic security controls during functional testing may reduce or eliminate development issues earlier in the development cycle (ex., mandatory access controls, secure code development, and firewalls). Preliminary testing is considered development level testing, not C&A testing but, if no changes occur, re-use test results to maximum extent possible in the C&A.
- For systems of high visibility and sensitivity, independent development testing may be recommended.
- Preliminary testing enables cost and schedule risk mitigation.
- Preliminary testing may be done at component or security zone level to ensure each component or security zone is secure as an entity.
- Capture the process and results of all security testing that occurs throughout the lifecycle for evaluation, issue identification and potential reuse.
- Source code should be periodically reviewed using automated tools or manual spot check for common programming errors that have a detrimental impact on system security including: Cross-site scripting vulnerabilities, buffer overflows, race conditions, object model violations, poor user input validation, poor error handling, exposed security parameters, passwords in the clear, and violations of stated security policy, models, or architecture as part of the software development QA process.

3.2.3.7 Perform Initial Review of and Planning for C&A

<table>
<tr><td>Description:</td><td>Because the Authorizing Official (AO) is responsible for accepting the risk of operating the system, the AO can advise the development team if the risks associated with eventual operation of the system appear to be unacceptable. Specifications can impose excessive burden and costs if the acceptable residual risks are not known. The involvement of the accrediting official is required for this determination of acceptable residual risks. It is easier to incorporate requirement changes during the planning stage of a system acquisition than during the solicitation, source selection, or contract administration stages.

The development team and the AO should also discuss the forms of evidence that the accrediting official needs to make a decision. This evidence may include system test results and other data. In addition, the acquisition initiator and the accrediting official should discuss how changes to the system and its environment would be addressed. The possibility of establishing a security-working group should be discussed. Such a group may consist of personnel, such as users, program managers, and application sponsors; system, security, or database administrators; security officers or specialists, including the C&A representatives; and system or application analysts.

To ensure proper testing and reduce the likelihood of scope creep during testing, the security accreditation boundary should be clearly delineated. This will form the basis for the test plan to be created and approved prior to implementation performance.

At this point, the certification package should be close to completion, and any agency-specified, initial review for conformance has commenced.</td></tr>
<tr><td>Expected Outputs:</td><td>• A planning document that identifies key players, project constraints, core components, scope of testing, and level of expected rigor.
• The certification package should be close to completion, and any initial agency-specified conformance reviews initiated.</td></tr>
<tr><td>Synchronization:</td><td>ISSO provides the system owner with completed documentation required to initiate and conduct C&A. The AO is notified.</td></tr>
<tr><td>Interdependencies:</td><td>Security Controls Assessment Plan will derive the foundational information from this planning document/session.</td></tr>
<tr><td colspan="2">Implementer's Tips</td></tr>
<tr><td colspan="2">• Holding a planning session or completing a preliminary project plan four - six weeks prior to testing will allow enough time to obtain resources and plan appropriately.
• Holding a quick initial review of the certification package will help bring to light potential challenges.
• Active testing will impact development and should be planned well ahead of this meeting.
• Involving the AO in the planning process as early as possible [even in phase 1] will establish expectations for C&A and eliminate surprises prior to reaching C&A control gate.</td></tr>
</table>

3.3 SDLC Phase: Implementation

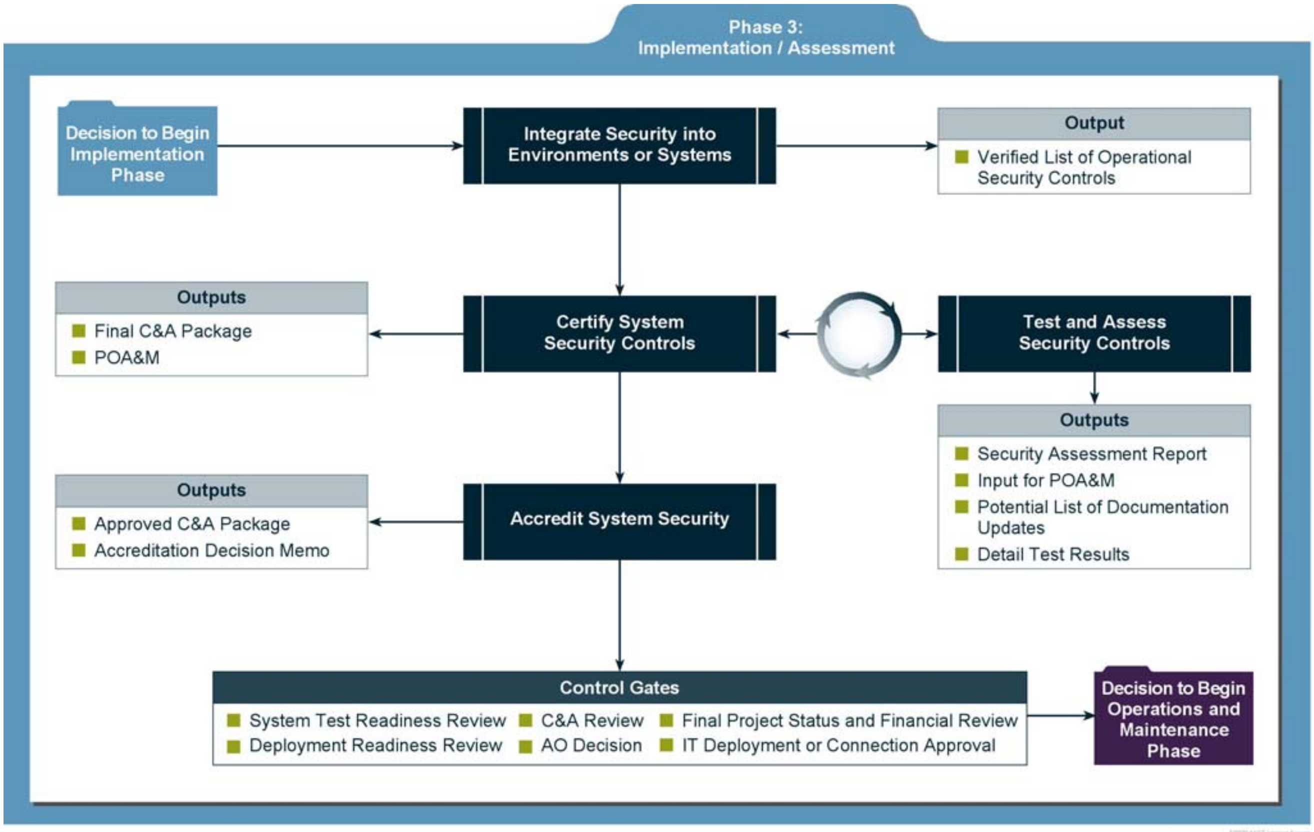

FIGURE 3-4. RELATING SECURITY CONSIDERATIONS IN THE IMPLEMENTATION/ASSESSMENT PHASE

3.3.1 Description

Implementation/ Assessment is the third phase of the SDLC. During this phase, the system will be installed and evaluated in the organization's operational environment.

Key security objectives for this phase include:

- Integrate the information system into its environment
- Conduct system certification activities
- Complete system accreditation activities

3.3.2 Control Gates

General types of control gates for this phase may include:

- System Test Readiness Review
- C&A Review

- Final Project Status and Financial Review
- Deployment Readiness Review
- AO Decision
- IT Deployment or Connection Approval

3.3.3 Major Tasks with Significant Security Integration Activities

3.3.3.1 Integrate Security into Established Environments or Systems

Description:	System integration occurs at the operational site when the information system is to be deployed for operation. Integration and acceptance testing occur after information system delivery and installation. Security control settings and switches are enabled in accordance with manufacturers' instructions, available security implementation guidance, and documented security specification.
Expected Outputs:	• Verified list of operational security controls. • Completed System Documentation.
Synchronization:	• Issues encountered during installation should be evaluated for inclusion into the contingency plan based on the potential for re-occurrence. • ISSO should review installed system to ensure controls are in place and properly configured and provide the verified list to system owner and AO.
Interdependencies:	Changes should be updated to the core security documents.
Implementer's Tips	
• Clean out test and development environment to ensure all test data is removed. • Extreme care should be exercised when integrating information systems into operational environments or systems such that critical operations are not disrupted.	

3.3.3.2 Test & Assess Security Controls

Description:	During this step, security controls are assessed for compliance and effectiveness using the most recently approved security requirements baseline (usually expressed in the system security plan). Assuming proper planning and security integration occurred during development, this task then becomes more focused on the verification of security controls and active testing. Whenever possible, automation and SCAP protocols should be leveraged to minimize level of effort and optimize resources. Test plans should be developed and approved to ensure alignment with the system's design and security approach, federal and agency compliance, and proper level of rigor. Once performed and documented, results should be discussed and addressed with residual vulnerabilities entered into the Plan of Action and Milestones (POA&M) process. Additional updates to security documents may be needed. Agencies should consult NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, or other similar publications for guidance on the evaluation of security controls.
Expected Outputs:	• Security Assessment Report. • Up-to-date POA&M. • Potential list of document updates.

Synchronization:	Assessment/test results from assessors to system owner, ISSO, system administrator, and developers.
Interdependencies:	• Continuous Monitoring Plan may provide reusable test plans for easier testing. • The testing of security controls may be reusable for continuous monitoring if documented well.

Implementer's Tips

- Assigning a core team of representatives from the major stakeholders to meet throughout testing will assist in communication and reduce surprises.
- The use of work plans for this subproject is very useful in tracking logistics, scope, and milestones.
- Clearly re-articulating the C&A process to all parties and agreeing on the testing's level of rigor and scope are very important in ensuring a smooth completion.
- Prioritize continuous monitoring by risk and cost effectiveness.
- Re-use as many prior testing results that are still relevant as possible.

3.3.3.3 Certify System Security

Description:	Prior to initial operations, a security certification must be conducted to assess the extent to which the controls are implemented, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In addition, periodic testing and evaluation of the security controls in an information system must be done to ensure that the controls are effectively maintained. In addition to verifying security control effectiveness, security certification also may uncover and describe actual vulnerabilities in the information system. The determination of security control effectiveness and information system vulnerabilities provides essential information to authorizing officials to facilitate credible, risk-based, security accreditation decisions.
Expected Outputs:	• Complete final Certification Package ready for assessment. • Certification Letter.
Synchronization:	Certifier provides written Certification Package results to System Owner, ISSO, and system administrator.
Interdependencies:	All previous steps.

Implementer's Tips

- All documents should be in final state and frozen for review to ensure an accurate picture of status at the time of review.
- Copying Certification Package to CD also helps ensure configuration control and a current archive.

3.3.3.4 Accredit System Security

Description:	OMB Circular A-130 requires the security authorization of an information system to process, store, or transmit information. This authorization (also known as security accreditation), granted by a senior agency official, is based on the verified effectiveness of security controls to some agreed-upon level of assurance and an identified residual risk to agency assets or operations (including mission, function, image, or reputation). The security accreditation decision is a risk-based decision that depends heavily, but not exclusively, on the security testing and evaluation results produced during the security control verification process. An accrediting official relies primarily on: (i) the completed system security plan; (ii) the security test and evaluation results; and (iii) the POA&M for reducing or eliminating information system vulnerabilities, in making the security accreditation decision to authorize operation of the information system and to accept explicitly the residual risk to agency assets or operations.

Expected Outputs:	• Decision on whether to approve for operation or wait until vulnerabilities are adequately addressed. • Copy of ATO, IATO, or denial from Authorizing Official to System Owner and ISSO.
Synchronization:	• System inventories and reporting statistics should be updated to reflect the accredited status. • CPIC activities should also reflect if the system is accredited.
Interdependencies:	• Update security and budget documentation with resulting status. • Certification statement for the information system.
Implementer's Tips	
Accrediting officials need to make risk decisions not only for the system under accreditation but for the risk extended to the organization as a whole by placing the system into operation.	

3.4 SDLC Phase: Operations and Maintenance

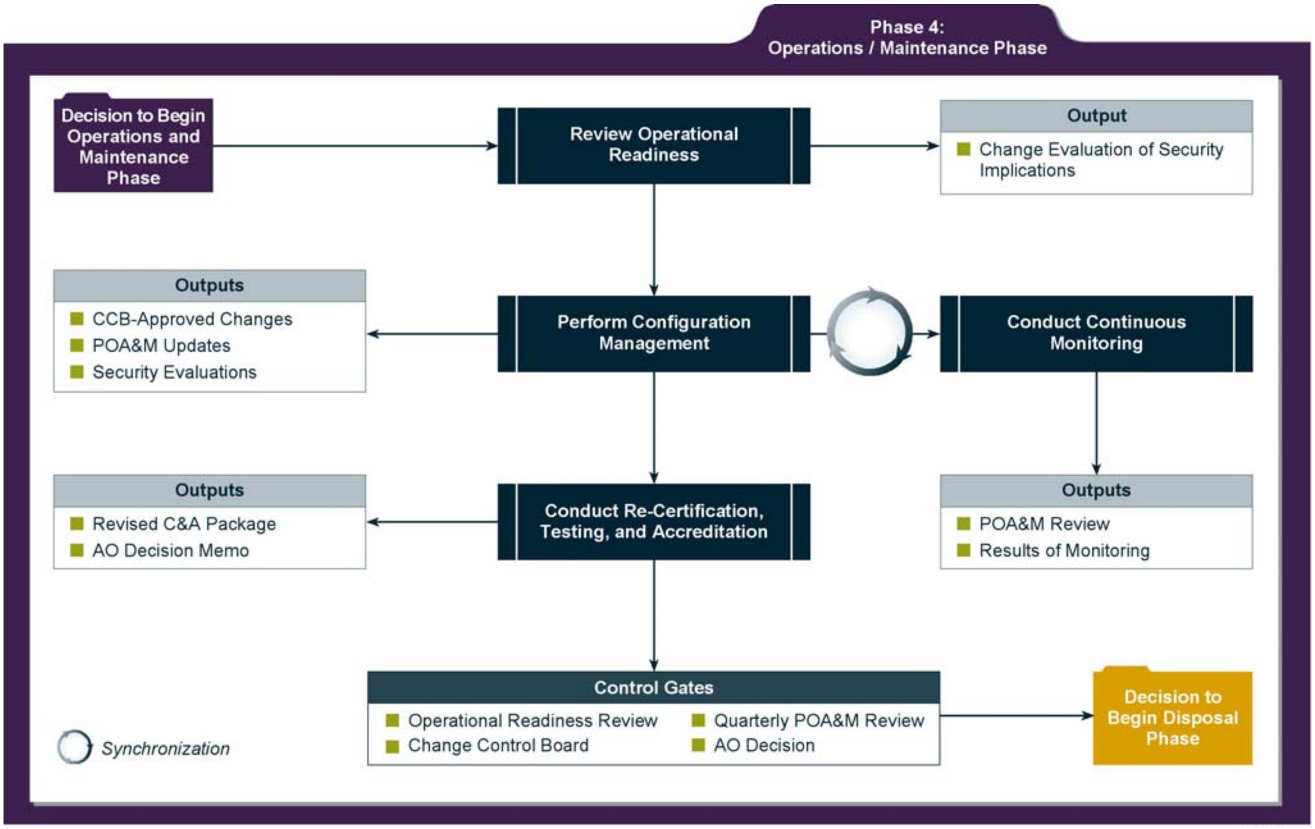

FIGURE 3-5. SECURITY CONSIDERATIONS IN THE OPERATIONS/MAINTENANCE PHASE

3.4.1 Description

Operations and Maintenance is the fourth phase of the SDLC. In this phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced. The system is monitored for continued performance in accordance with security requirements and needed system modifications are incorporated. The operational system is periodically assessed to determine how the system can be made more effective, secure, and efficient. Operations continue as long as the system can be effectively adapted to respond to an organization's needs while maintaining an agreed upon risk level. When necessary modifications or changes are identified, the system may re-enter a previous phase of the SDLC.

Key security objectives for this phase include:

- Conduct an operational readiness review;
- Manage the configuration of the system ;
- Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls; and

- Perform re-authorization as required.

3.4.2 Control Gates

General types of control gates for this phase may include:

- Operational Readiness Review
- Change Control Board Review of Proposed Changes
- Review of POA&Ms
- Accreditation Decisions (Every 3 years or after a major system change)

3.4.3 Major Tasks with Significant Security Integration Activities

3.4.3.1 Review Operational Readiness

Description:	Many times when a system transitions to a production environment, unplanned modifications to the application occur. If changes are significant, a modified (shorter) test of security controls, such as configurations, may be needed to ensure the integrity of the security controls. This step is not always needed; however, it should be considered to help mitigate risk and efficiently address last minute surprises.
Expected Outputs:	Evaluation of change to system in terms of potential security implications.
Synchronization:	• System Administrator and ISSO confirmation to System Owner that system is operating normally. • Should a last minute change occur that fundamentally changes the level of risk to the system, the system owner should consider re-certification - this is rare.
Interdependencies:	• An operational readiness review supplements the C&A process to ensure changes reviewed for risk potential. • Any change to security controls should be updated in the security documentation.
Implementer's Tips	
• When an application is enhanced or changed, regression testing helps to ensure that additional vulnerabilities have not been introduced. For example, adding source code can often introduce errors in other areas and may negatively impact existing and stable functions along with the new ones. • Changes that include additional data fields should be noted and analyzed to determine if the security posture of the system has degraded or introduced a need for additional controls.	

3.4.3.2 Manage Security Control Configuration due to System Changes

Description:	An effective agency configuration management and control policy and associated procedures are essential to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently for controlling and maintaining an accurate inventory of any changes to the system. Changes to the hardware, software, or firmware of a system can have a significant security impact. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.

	These steps, when implemented effectively, provide vital input into the system's continuous monitoring capability. As such, it facilitates the agency's ability to identify significant changes that alter a system's security posture and control effectiveness to ensure proper assessment and testing occurs. Note: The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). Agency Configuration Management procedures should integrate this activity to ensure repeatability and consistency. This is an iterative process that requires periodic review of profile changes.
Expected Outputs:	Full range of SDLC documents impacted by system change.
Synchronization:	• System updates should be included into the system security documentation at least annually or with significant change. • CM system documents should provide input into the Continuous Monitoring plan for the system.
Interdependencies:	• Inputs into the security activities and acts as a potential trigger to identifying when the system's posture has changed and requires additional security attention. • Security Architecture should provide key details on component level security service, which in turn provides a benchmark to evaluate the impact of the planned change. For example, if you are upgrading database software to a new version that has less auditing capability, the security architecture or security control documentation should provide insight into whether that component needs that level of auditing capability. Resulting analysis would identify whether further review is needed before implementing.
Implementer's Tips	
• Security significance is not always easy to identify when looking at CM artifacts. The reviewer should keep in mind any changes that would directly or indirectly (meaning allow exploit by a hacker to impair system) impact confidentiality, integrity and availability. • Some system enhancements that add new data may require a review of impact to the system security categorization and associated security controls. For example, data may be considered privacy. • Abbreviated CM processes that allow for unique emergency "break the glass" situations should be identified for emergency purposes. These situations should always be followed up with a full review when time permits.	

3.4.3.3 Monitor Security Controls Continuously

Description:	The ultimate objective of continuous monitoring is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the system operates. A well-designed and well-managed continuous monitoring process can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status information to appropriate organizational officials. This information can be used to take appropriate risk mitigation actions and make credible, risk-based authorization decisions regarding the continued operation of the information system and the explicit acceptance of risk that results from that decision. The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways, including security reviews, self-assessments, configuration management, antivirus management, patch management, security testing and evaluation, or audits. As mentioned when discussing security testing and configuration management, automation and SCAP should be leveraged to reduce level of effort and ensure repeatability.
Expected Outputs:	System artifacts demonstrating evidence of effective security control implementation.

Synchronization:	Continuous monitoring should be adjusted as risk levels fluctuate significantly and security controls are modified, added and discontinued.
Interdependencies:	Continuous monitoring provides system owners with an effective tool for producing ongoing updates to information system security plans, security assessment reports, and plans of action and milestones documents.
Implementer's Tips	
• Agencies should strive to implement a cost effective continuous monitoring program. Where available, a continuous monitoring program should make use of common services for more frequent monitoring, as well as system specific monitoring for critical security controls. • Realizing that it is neither feasible nor cost-effective to monitor all of the security controls in any information system on a continuous basis, agencies should consider establishing a schedule for security control monitoring to ensure that all controls requiring more frequent monitoring are adequately covered and that all controls are covered at least once between each accreditation decision. • Continuous monitoring processes should be evaluated periodically to review changes in threats and how this could affect the ability of controls to protect a system. These threat updates may result in updated risk decisions and changes to existing controls. • Take credit for activities already underway that count for continuous monitoring. AV DAT file updates, routine maintenance, physical security fire drills, log reviews etc should all be identified and captured in the continuous monitoring phase. • Prioritize continuous monitoring by importance of control to mitigating risk, validation of POA&M items that become closed and single control points of failure. • Look at a monitoring cycle that will coincide with the system certification life span and capture test procedures and results for re-use upon re-certification.	

3.4.3.4 Conduct Re-Authorization

Description:	Reaccreditation occurs when there are significant changes to the information system affecting the security of the system or when a specified time period has elapsed in accordance with federal or agency policy. The optimal goal is for re-accreditation to be another full review of existing artifacts and a new authorization letter.
Expected Outputs:	Updated system security certification package with associated accreditation artifacts.
Synchronization:	Re-authorization may be triggered by any continuous monitoring activities.
Interdependencies:	• Re-authorization may result in a short term, but planned for, spike in needed funding for the system. • Re-authorization may be a needed step prior to additional funding to ensure risk mitigation of investment.
Implementer's Tips	
• Plan re-authorizations for all operational systems with proper leveling of security staff resources to ensure morale and quality reviews. This may require offering short periods of waivers to distribute workload over the man-year. • Defining agency specific criteria for triggering a re-authorization helps to ensure decision makers are informed and all stakeholders have a common understanding. Some latitude should be given in criteria to allow for unique situations.	

3.5 SDLC Phase: Disposal

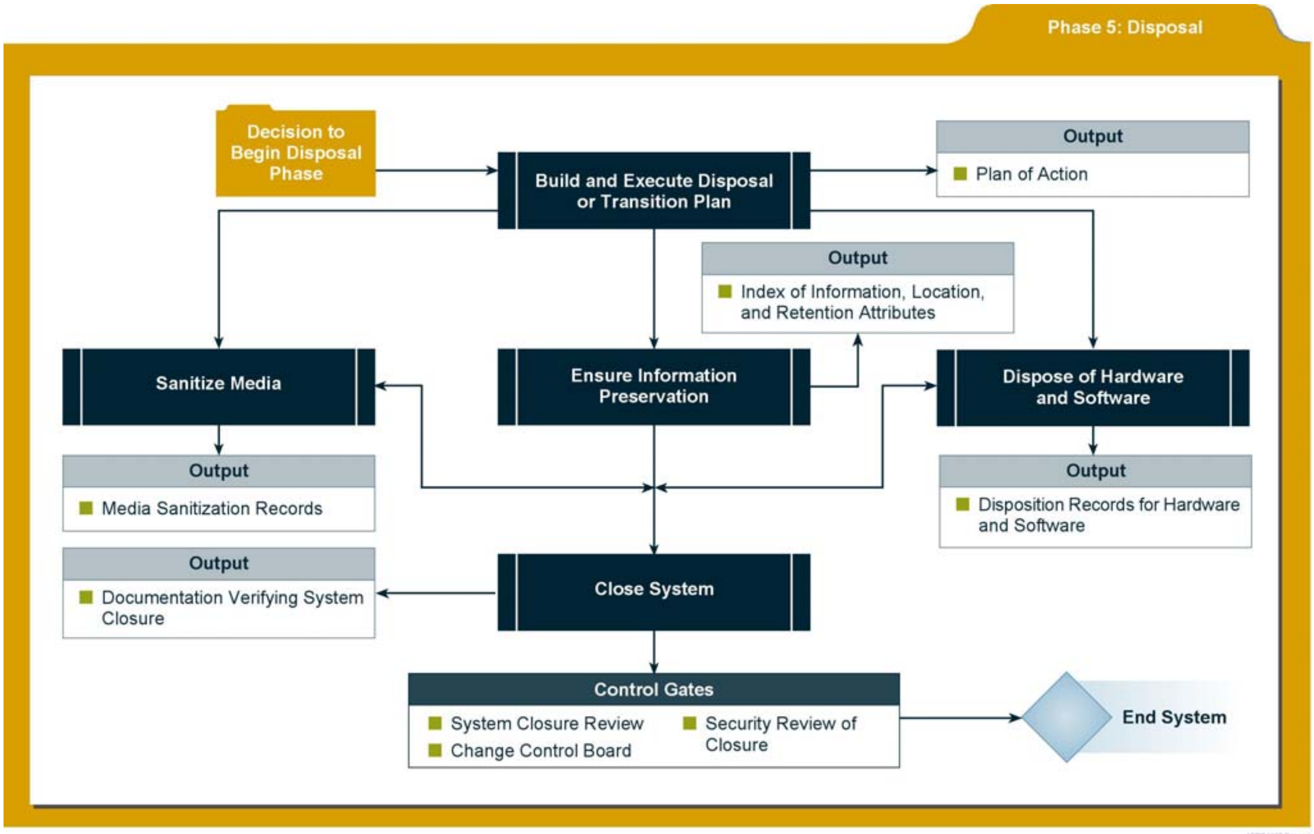

FIGURE 3-6. SECURITY CONSIDERATIONS IN THE DISPOSAL PHASE

3.5.1 Description

Disposal, the final phase in the SDLC, provides for disposal of a system and closeout of any contracts in place. Information security issues associated with information and system disposal should be addressed explicitly. When information systems are transferred, become obsolete, or are no longer usable, it is important to ensure that government resources and assets are protected.

Usually, there is no definitive end to an SDLC. Systems normally evolve or transition to the next generation because of changing requirements or improvements in technology. System security plans should continually evolve with the system. Much of the environmental, management, and operational information should still be relevant and useful in developing the security plan for the follow-on system.

The disposal activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future, if necessary. Particular emphasis is given to proper preservation of the data processed by the system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access.

Key security objectives for this phase include:

- Build and Execute a Disposal/Transition Plan
- Archive of critical information
- Sanitization of media
- Disposal of hardware and software

3.5.2 Control Gates

General types of control gates for this phase may include:

- System Closure Review
- Change Control Board
- Security Review of Closure

3.5.3 Major Tasks with Significant Security Integration Activities

3.5.3.1 Build and Execute a Disposal/Transition Plan

Description:	Building a disposal / transition plan ensures that all stakeholders are aware of the future plan for the system and its information. This plan should account for the disposal / transition status for all critical components, services, and information. Much like a work plan, this plan identifies necessary steps, decisions, and milestones needed to properly close down, transition, or migrate a system or its information. In many cases, disposed systems or system components have remained dormant but still connected to the infrastructure. As a result, these components are often overlooked, unaccounted for or maintained at suboptimal security protection levels, thus, providing additional and unnecessary risk to the infrastructure and all connected systems. A transition plan assists in mitigating these possible outcomes.
Expected Outputs:	Documented artifact outlining the plan of action for closing or transitioning the system and/or its information.
Synchronization:	Security documentation should reflect pending plans if security decisions and funding are reallocated or otherwise impacted because of the disposal decision.
Interdependencies:	Security documentation such as the security plan, security categorization and control requirements may need updating.
Implementer's Tips	
• Consult with agency Records Management, Privacy, and Freedom of Information Act (FOIA) officials prior to disposal to ensure compliance with these laws and applicable agency policy. • If you can help it, do not wait for the disposal phase to make a transition plan. Plan for disposal/transition throughout all phases of the lifecycle. This is best done as part of the requirements phase so full resource requirements for disposal/transition are understood and planned for. Throughout the lifecycle, this can be done as hardware and software becomes obsolete or damaged in other phases it will require tasks outlined in this phase.	

3.5.3.2 Ensure Information Preservation

Description:	When preserving information, organizations should consider the methods that will be required for retrieving information in the future. The technology used to retrieve the records may not be readily available in the future (particularly if encrypted). Legal requirements for records retention must be considered when disposing of systems.
Expected Outputs:	May include an indexing of preserved information, location and retention attributes.
Synchronization:	Records management, Privacy Act, and FOIA requirements should be considered.
Interdependencies:	Privacy considerations or activities may be important for FOIA reasons.
Implementer's Tips	
• Close coordination with the organization Freedom of Information Act (FOIA) Office will assist in planning for this activity. • Organizations can also get practical tips from the National Archives and Records Administration Information System Security Oversight Office.	

3.5.3.3 Sanitize Media

Description:	Based on the results of security categorization, the system owner should refer to NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, which specifies that, "the organization sanitizes information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization and destruction actions and periodically tests sanitization equipment/procedures to ensure correct performance. The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media." NIST 800-88, Guidelines for Media Sanitization, divides media sanitization into four categories: disposal, clearing, purging and destroying. It further suggests that the system owner categorize the information, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then, decide on the appropriate sanitization process. The selected process should be assessed as to cost, environmental impact, etc., and a decision made that best mitigates the risk to confidentiality and best satisfies other constraints imposed on the process. Several factors should be considered along with the security categorization of the system confidentiality when making sanitization decisions. The cost versus benefit of a media sanitization process should be understood prior to a final decision. For instance, it may not be cost-effective to degauss inexpensive media such as diskettes.
Expected Outputs:	Artifacts documenting actions taken.
Synchronization:	None.
Interdependencies:	Security categorization provides the identification and associated risk level of system information.
Implementer's Tips	
• Even though clear or purge may be the recommended solution, it may be more cost-effective (considering training, tracking, and validation, etc) to destroy media rather than use one of the other options. • Organizations can always increase the level of sanitization applied if that is reasonable, and indicated by an assessment of the existing risk.	

3.5.3.4 Dispose of Hardware and Software

Description:	Hardware and software can be sold, given away, or discarded as provided by applicable law or regulation. The disposal of software should comply with license or other agreements with the developer and with government regulations. There is rarely a need to destroy hardware except for some storage media that contains sensitive information and that cannot be sanitized without destruction. In situations when the storage media cannot be sanitized appropriately, removal and physical destruction of the media may be possible so that the remaining hardware may be sold or given away. Some systems may contain sensitive information after the storage media is removed. If there is doubt whether sensitive information remains on a system, the ISSO should be consulted before disposing of the system. Also, the vendor maybe consulted for additional disposal options or verification of risk.
Expected Outputs:	• Lists of hardware and software released (sold, discarded or donated). • Lists of hardware and software redeployed to other projects or tasks.
Synchronization:	None.
Interdependencies:	System hardware and software inventory should be updated accordingly.
Implementer's Tips	
• Do not forget property accountability requirements when disposing of a system. When possible, consider donation of used IT and/or e-cycling of hazmat parts. • Title 40 USC advises system owners and custodians that excess equipment is "Educationally useful" and "Federal equipment is a vital national resource." Wherever possible, excess equipment and media should be made available to qualifying schools and non-profit organizations to the extent permitted by law. • For cost savings, some agencies maintain reasonably old parts for contingency operations. For example, utilizing retired laptops for a telecommuting scenario that requires only partial processing for vital internet or email communications.	

3.5.3.5 Closure of System

Description:	The information system is formally shut down, disassembled at this point.
Expected Outputs:	• Documentation verifying system shutdown and action taken. • Final notification closure to the accrediting and certifying officials, configuration management, system owner, ISSO, and program manger.
Synchronization:	None.
Interdependencies:	• Archival of security documentation as appropriate. • If continuous monitoring services are provided, notification to providers of closure is needed (may include CM, AV, IR, and CCB). • Inventory updates for FISMA reporting and enterprise architecture.
Implementer's Tips	
• A memorandum articulating formal system closure and proper action taken that includes in the distribution all key stakeholders provides the simplest approach to formal closure.	

CHAPTER FOUR

ADDITIONAL SECURITY CONSIDERATIONS

"Building security in" is a security management technique that implements specific security considerations during SDLC phases. However, IT projects and initiatives are not always as clearly scoped as system or application developments. Some initiatives are service based and cross IT platforms (and, in some cases, organizations) or are facility oriented, like the building of a data center or hot site. These projects must follow as much as possible, established review boards and recognize and address necessary security considerations. This section will highlight common examples and provide some security-oriented considerations. The core elements of integrating security into the SDLC remain the same for these areas. Communications and documentation of the stakeholder relationship in regards to securing the solution will be the key success factor.

4.1 Supply Chain and Software Assurance

Ensuring supply chain[2] and software assurance will require a public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in hardware and software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development. This area is maturing and future guidelines will likely be provided to provide more specifics. In general, these processes and procedures should target the three following goals:

- **Trustworthiness** - No exploitable vulnerabilities exist, either maliciously or unintentionally inserted and materials are what they claim to be without counterfeit, piracy or violation of intellectual rights.

- **Predictable Execution** - Justifiable confidence that hardware and software, when executed, functions as intended

- **Conformance** - Planned and systematic set of multi-disciplinary activities that ensure hardware and software processes and products conform to requirements, standards and procedures

Towards these goals, acquisition managers and information security managers should factor in risks posed by the supply chain as part of their risk mitigation efforts including:

- Information on suppliers' process capabilities (business practices) should be used to determine security risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the system.

[2] Supply chain refers to the distribution channel of a product from its sourcing to its delivery to the end consumer.

- Information about evaluated products should be made available and reviewed, along with responsive provisions for discovering exploitable vulnerabilities, and products would be securely configured in use.

4.2 Service Oriented Architectures

Service-oriented architecture (SOA) is an information system architectural style where existing or new functionalities are packaged as services. These services communicate with each other by passing data from one service to another, or by coordinating an activity between one or more services. NIST SP 800-95: *Guide to Secure Web Services* provides more information on SOA security considerations.

Primary security management challenges with SOA include scoping the security boundary, assigning an appropriate risk level, and managing security expectations and responsibilities across multiple stakeholders and agreements. Designing a strategy for accreditation can also pose a challenge in terms of schedule and resources. While the traditional SDLC process will likely not fit, the security considerations remain, for the most part, applicable. Agencies should plan their approach so that accreditation as well as continuous monitoring and re-accreditation is cost effective and manageable.

As many traditional analytic tools (scanners, IDS, packet crafting/analysis tools, etc.) are not able to effectively evaluate the aggregate security posture of a service oriented architecture it is left to the security analyst to utilize analytic tools, apply unique SOA test cases, and extrapolate a synthetic model of the security environment for vulnerability and risk analysis.

In addition to automated testing that may be available, the following reviews that focus on the unique aspects of SOA are suggested:

- Audit Trail Certification & Correlation
- Service Oriented Architecture Interaction Description (Portlets, Security Assertions Markup Language (SAML), Simple Object Access Protocol (SOAP), Universal Description, Discovery, and Integration (UDDI), Web Services Description Language (WSDL), XACML, as well as many of the WS-* standards emerging in the web services arena including WS-Security, WS-Policy, and WS-Interoperability; highlighting security features and benefits in each)
- Access Control (such as discretionary and role-based)
- Core enterprise services composition and utilization
- Creation, protection, and disposal of robust meta-data

4.3 Specific Accreditation of Security Modules for Reuse

As applications and information systems become more object-oriented and component-based it becomes necessary to consider the security implications as well as cost of reusing software modules across multiple projects and perhaps across multiple organizations. It is recommended that components and software modules be created with reuse in mind, particularly for code that must be relied upon to provide security functionality across a broad range of projects. The certification & accreditation of these modules, much like unit testing for functional evaluation, provides developers, architects, and engineers with a ready toolbox of trusted code that can be implemented as needed, at a reduced cost, to ensure security compliance and risk management during the development of an information system at a reduced cost.

Accredited modules should be well documented as to their features and functions, accreditation documentation should be stored along with the module, documentation for developers highlighting use cases and implementation practices that will not be likely to void the accreditation should also be made available. The module and documentation should be digitally signed by the developer (or development team) to preserve the integrity and authenticity of the accreditation. Sufficiently complex modules (likely to be considered applications in their own right) may warrant essentially the same process as described in NIST SP 800-37.

4.4 Cross-Organizational Solutions

Cross-organizational solutions seek to provide access to information applications pursuant to a memorandum of agreement or service level agreement which provides value and benefit to both (or multiple) organizations. The applications made available across organizations can be categorized into two cases based on intended consumers. In the first case, the intended group of consumers is the “Enterprise,” which refers to the organization considered in total and includes interdependent resources (i.e., people, organizations, and technology) that must coordinate functions and share information in support of a common mission (or a set of related missions). In the second case, the expected group of consumers is a Community of Interest (COI). A COI is a collection of people who exchange information using a common vocabulary in support of shared missions, business processes, and objectives. The community is made up of the users/operators that participate in information exchange, the developers of services, applications, capabilities and systems for these users, and the functional proponents that define requirements and obtain resources for acquisition on behalf of the users.

When developing cross-organizational solutions care must be taken to draft guiding documents (a memorandum of agreement or service level agreement) that categorically describe the security features, requirements, and expected performance levels to ensure all parties are adequately protected. Further, it is necessary to agree upon test & validation responsibilities, incident response procedures, and monitoring and operations policies that will provide sufficient management of risk going forward. Special emphasis will need to be placed upon user and code/application authentication and authorization, which includes planning for growth of the user base, the interdependency of authentication and authorization systems between organizations, common access environments, and enrollment/disenrollment procedures.

4.5 Technology Advancement & Major Migrations

With the fast pace of innovation and correspondingly selective obsolescence in the information technology space, consideration must be given not only to integrating security into the SDLC for new systems and the integration of systems, but also to the overhaul, upgrade, or migration of systems to address technology advancement. Advances in technology create both new challenges in enterprise security as well as running the risk of reintroducing well-known vulnerabilities through flawed implementation/integration practices. Synergy of technology creates a synergy of exposure compounding existing problems.

When grappling with the security implications of technology advancement or planning a major system migration, you are likely to experience the following organizational behavior regarding information system security:

- As the technology is first introduced to address the organization's mission (or change in mission) or to solve an acute business problem, the organization will often seek to relax or remove baseline security requirements in order to speed the process along.

- When the apparent production status of the information system can no longer be ignored, security is typically enforced through controls on the legacy infrastructure, which have been certified and accredited; the justification being that they provide adequate mitigation.

- Eventually the information system matures, adoption increases, or understanding of the vulnerabilities, risks, and mitigation strategies of the technology or its' environment improves to the point that the management team is at least as comfortable with the risk management plan for the new technology as with the legacy system; and perhaps more confident given the demonstrated advanced capabilities of the system.

Further, this pattern of behavior is not limited to technology that is truly advanced or new. It is not uncommon for technology developed 10 or more years ago to be thrust into the limelight, now en vogue with developers, but lacking the scrutiny over time due to its historical fringe nature necessary to be assured that the discovery of vulnerabilities and active patching of vulnerabilities discovered in similar/equivalent technologies has been conducted.

This pattern of behavior, at first glance, seems to paint a bleak picture. However, it can be quite the contrary if viewed from the perspective of capitalizing on the heightened need to integrate security into the SDLC. These anticipated organizational behaviors provide a wealth of opportunities to capitalize on the emergent nature of the technology and the ability to plan for migration from legacy systems in an assured manner.

4.6 Data Center or IT Facility development

Data center or IT Facility developmental security places a special emphasis on physical security solutions, and rightly so. Nonetheless, it is important to remember that data centers are the storehouse for vast quantities of computing power and storage upon which applications are built and special attention is required to ensure all customers utilizing the data center's facilities are adequately protected.

A typical large organization may have multiple data centers each charged with supporting a specific set of customers and missions; but inter-related in order to supply high availability, continuity of operations, and meet continuity of operations and disaster recovery requirements (often requiring the ability to store data off-site or provide for alternate sites for data processing) in a cost effective manner, the data centers must share the burden and provide a matrix of redundancy. Under these conditions, it is crucial that data separation be maintained for data at rest as well as in transit and that in particular, separation of duties and auditability of administrative functions for data center staff be strictly enforced. In many cases, this will justify the need for separate local area networks (LANs) or Virtual LAN (VLANs) for administrative traffic and applications.

This integration of security, both technical and operational, becomes even more important with the rise of virtualization in the data center and the ability to move entire virtualized operating system environments across independent and distinct hardware platforms within the data center.

One unique consideration of the data center is the security of the contextual environmental data. This data will result from the monitoring of the physical security systems (cameras, motion sensors, etc.) as well as the environmental systems necessary to keep the computing hardware in a temperate working environment. This data is increasingly stored on a digital medium that is network accessible and should be handled with care as it is sensitive in nature and may give an attacker access to core information systems. These systems should be adequately protected and the resulting data should be stored off-site or out of band (i.e. not on the same networks/information systems as the customer information systems housed within the data center).

4.7 Virtualization

Virtualization, the use of virtual machines and applications, is a growing trend that provides opportunity for cost savings. While it can provide additional security in terms of isolation and recovery, it requires additional security planning for unique security risks inherit in virtualization implementations such as data intercepting through the shared clipboard, keystroke logging within the virtual machine, and denial of service to the host's resources.

Security controls associated with traditional physical platforms common overlooked in implementing virtualization include:

- Anti-malware within the virtual machine and host;
- Segregation of administrative duties for host and versions;
- Audit logging as well as exporting and storing the logs outside the virtual environment;
- Configuration and patch management of the virtual machine and host;
- Encrypting network traffic between the virtual machine and host; and
- IDS and IPS monitoring.

Due to its distributed network and complexity, mobilizing virtualization (for example, when used on blackberries) can further exasperate common security concerns such as malware, data leaks, patch management and weak access controls.

For best results, agencies should plan security into their selection criteria, and, at a minimum, create and document a secure deployment and maintenance plan prior to implementing a virtual solution.

APPENDIX A

GLOSSARY

Term	Definition
Acceptance	The act of an authorized representative of the Government by which the Government, for itself or as agent of another, assumes control or ownership of existing identified supplies tendered or approves specific services rendered as partial or complete performance of the contract. It is the final determination whether or not a facility or system meets the specified technical and performance standards.
Acquisition	Includes all stages of the process of acquiring property or services, beginning with the process for determining the need for the property or services and ending with contract completion and closeout.
Business Impact Analysis (BIA)	An analysis of an information technology (IT) system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. SOURCE: SP 800-34
Certification and Accreditation – (C&A)	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. *Accreditation* is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. *SOURCE: SP 800-37*
Clinger-Cohen Act of 1996	Also known as Information Technology Management Reform Act. A statute that substantially revised the way that IT resources are managed and procured, including a requirement that each agency design and implement a process for maximizing the value and assessing and managing the risks of IT investments.
Closeout	Includes all final contract activities (e.g., ensuring completion of all requirements, making final payment).
Commercial off-the-shelf (COTS)	Software and hardware that already exists and is available from commercial sources. It is also referred to as off-the-shelf.

Term	Definition
Contract administration	Government management of a contract to ensure that the Government receives the quality of products and services specified in the contract within established costs and schedules.
Contracting Officer	A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.
Contracting Officer's Technical Representative	An individual to whom the CO delegates certain contract administration responsibilities, usually related to technical direction and acceptance issues.
Control Gate	A point in time when the system development effort will be evaluated and when management will determine whether the project should continue as is, change direction, or be discontinued.
Deliverable	A product or service that is prepared for and delivered to the Government under the terms of a contract.
Environment	Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system. *SOURCE: FIPS 200; CNSSI-4009*
Federal Acquisition Regulation (FAR)	The regulation that codifies uniform acquisition policies and procedures for Executive agencies.
Federal Information Processing Standards	A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability. *SOURCE: FIPS 201*
Federal Information Processing Standards Publications	FIPS publications are issued by NIST after approval by the Secretary of Commerce. Some FIPS Pubs are mandatory for use in federal acquisitions.
Federal Information Security Management Act (FISMA)	Requires agencies to integrate IT security into their capital planning and enterprise architecture processes at the agency, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to the Office of Management and Budget (OMB). *SOURCE: SP 800-65*
Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. *SOURCE: SP 800-53; CNSSI-4009*

Term	Definition
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology. *SOURCE: SP 800-53; 44 U.S.C., Sec. 3502* Information and related resources, such as personnel, equipment, funds, and information technology. *SOURCE: FIPS 200; FIPS 199*
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. *SOURCE: SP 800-53; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542* Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— 1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; 2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and 3) availability, which means ensuring timely and reliable access to and use of information. *SOURCE: SP 800-66; 44 U.S.C., Sec 3541*
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposal of information. *SOURCE: SP 800-53; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3502; OMB Circular A-130, App. III*
Information System Owner	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. *SOURCE: FIPS 200; CNSSI-4009 Adapted*
Information System Security Officer (ISSO)	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program. *SOURCE: SP 800-53; CNSSI-4009 Adapted*

Term	Definition
Information Technology (IT)	Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes computers, ancillary equipment, software, firmware, similar procedures, services, and related resources.
Plan of Action and Milestones (POA&M)	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. *SOURCE: SP 800-53; OMB Memorandum 02-01*
POA&M	See Plan of Action and Milestones
Privacy Impact Assessment	An analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. SOURCE: SP 800-53; OMB Memorandum 03-22
Residual Risk	The remaining, potential risk after all IT security measures are applied. There is a residual risk associated with each threat. *SOURCE: SP 800-33*

APPENDIX B

REFERENCES

Clinger-Cohen Act, 40 United States Code (U.S.C.) 1401 and following, 1996.

Computer Security Act of 1987, Public Law (P.L.) 100-235.

Federal Acquisition Regulation (FAR), Department of Defense, General Services Administration (GSA) and National Aeronautics and Space Administration.

Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES), October 1999.

FIPS 81, *DES Modes of Operation*, December 1980.

FIPS 113, *Computer Data Authentication*, May 1985.

FIPS 140-2, *Security Requirements for Cryptographic Modules*, June 2001.

FIPS 180-2, *Secure Hash Standard (SHS),* August 2002.

FIPS 185, *Escrowed Encryption Standard*, February 1994.

FIPS 186-2, *Digital Signature Standard (DSS)*, January 2000.

FIPS 197, *Advanced Encryption Standard*, November 2001.

FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 2002.

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, final public draft, December 2003.

Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. Chapter 35, Subchapter III, 2002.

GSA publication, *A Guide to Planning, Acquiring, and Managing Information Technology Systems*, Version 1, December 1998.

International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) International Standard 15408:1999 (parts 1 through 3), *Common Criteria for Information Technology Security Evaluation*, August 1999.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, November 1999.

NIST SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.

NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.

NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A*, June 2004.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.

NIST SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.

NIST SP 800-35, *Guide to Information Technology Security Services*, October 2003.

NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, October 2003.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

NIST SP 800-39 (Draft), *Managing Risk from Information Systems: An Organizational Perspective*, October 2007

NIST SP 800-40, *Procedures for Handling Security Patches*, September 2002.

NIST SP 800-42, *Guideline on Network Security Testing*, October 2003.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, draft.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

NIST SP 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*, draft.

NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categorization Levels (draft)*.

NIST SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process (draft)*.

NIST Interagency Report (NISTIR) 6462, *CSPP Guidance for COTS Security Protection Profiles*, December 1999.

National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, *National Information Assurance Acquisition Policy*, January 2000, http://www.nstissc.gov/Assets/pdf/nstissp_11.pdf

National Technology Transfer and Advancement Act of 1995 (P.L. 104-113).

Office of Management and Budget (OMB) Circular A-76, *Performance of Commercial Activities*, May 2003.

OMB Circular A-130, *Management of Federal Information Resources*, November 2000.

Paperwork Reduction Act of 1995, as amended, (44 U.S.C. 3501 (10) and 3506).

Pressman, Roger S., *Software Engineering: A Practitioner's Approach*, 4th Edition, McGraw-Hill, New York, 1997.

United States Code (U.S.C.), Title 5, Section 552a

U.S.C., Title 50, Section 781

U.S.C., Title 50, Sections 831 through 835

United States Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, http://www.cybercrime.gov/s&smanual2002.htm, January 2001.

APPENDIX C

NIST REFERENCE MATRIX AND WEBSITES

To assist in further research, the matrix below provides a cross-matrix.

Security Activity	Supporting NIST Pub(s)
Phase 1 – Initiation	
1. Project Initiation – Security Planning	SP 800-64, -100, -37, -53
2. Categorize Security for the System	SP 800-60, FIPS 199
3. Assess Business Impact	SP 800-34
4. Assess Privacy Considerations	SP 800-37
5. Ensure Secure Information System Development	SP 800-64, -16
Phase 2 – Development	
1. Assess Risk to System	SP 800-30
2. Analyze Security Requirements	SP 800-53
3. Design Security Architecture	SP 800-30
4. Engineer in Security and Develop Controls	SP 800-53, FIPS 200
5. Develop Security Documentation	SP 800-18
6. Conduct Developmental, Functional, and Security Testing	FIPS 140-2; SCAP website (see below)
7. Create Detailed Plan for C&A	SP 800-37
Phase 3 – Implementation	
1. Integrate Security into Established Environments or Systems	SP 800-64
2. Certify System Security	SP 800-37, -53A
3. Test & Assess Security Controls	SP 800-55, -53A
4. Accredit System Security	SP 800-37
Phase 4 – Operations and Maintenance	
1. Review Operational Readiness	SP 800-70, -53A
2. Perform Configuration Management	SP 800-53A, -100
3. Conduct Continuous Monitoring	SP 800-53A, -100
4. Conduct Re-Authorization	SP 800-37, -53A
Phase 5 – Disposal	
1. Build and Execute Disposal or Transition Plan	None.
2. Ensure Information Preservation	SP 800-12, -14
3. Sanitize Media	SP 800-88
4. Dispose of Hardware and Software	SP 800-35
5. Close System	None.

Additional information can be found at the following NIST websites.

- http://csrc.nist.gov/
- http://nvd.nist.gov/scap.cfm

APPENDIX D

ADDITIONAL GRAPHICAL VIEWS OF SECURITY WITHIN SDLC