NIST Special Publication 800-64 Revision 2

Security Considerations in the System Development Life Cycle

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

October 2008

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

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy 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, 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 from NIST, 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 to the original authors, as well as our reviewers, Arnold Johnson, John Garguilo, Marianne Swanson, and Elizabeth Lennon from NIST who greatly contributed to the document's development. NIST also gratefully acknowledges and appreciates the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

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 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 life cycle (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. Early integration of security in the SDLC enables agencies to maximize return on investment in their security programs, through:

- 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; and
- Facilitation of 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 (a.k.a. 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 Life Cycle 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 life cycle 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. Also considered outside scope is an organization's information system governance process.

First, the guideline describes 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. Information security is a business enabler when applied through 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 life cycle 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;
- Facilitation of informed executive decision making through comprehensive risk management in a timely manner;
- Documentation of 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
- Improved systems interoperability and integration that would otherwise be hampered by securing systems at various system levels.

1.4 Document Organization

The remaining chapters of this guide discuss the following:

- Chapter 2, Overview of Information Security and the System Development Life Cycle, summarizes the relationship between the SDLC and other IT disciplines, establishes a common understanding of SDLC, and the discusses the roles and responsibilities involved in integrating information security into the SDLC.
- Chapter 3, Incorporating Security into the Information System Development Life Cycle**,** describes a number of security considerations that will help integrate Information security into each phase of the SDLC.
- Chapter 4, Additional Security Considerations, highlights security considerations for development scenarios, such as service-oriented architectures and virtualization, for which the approach to security integration varies somewhat from that of traditional system development efforts.

This guide contains seven appendices. Appendix A provides a glossary of terms. Appendix B presents a comprehensive list of acronyms. Appendix C lists references cited in this publication. Appendix D provides a mapping of relevant NIST publications to corresponding SDLC security activities. Appendix E gives an overview of other SDLC methodologies. Appendix F discusses additional planning considerations for the development / acquisition phase of the SDLC. Appendix G provides an additional graphical view of security integration in the SDLC.

CHAPTER TWO

OVERVIEW OF INFORMATION SECURITY AND THE SYSTEM DEVELOPMENT LIFE CYCLE FUNDAMENTALS

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[1] involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information 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.

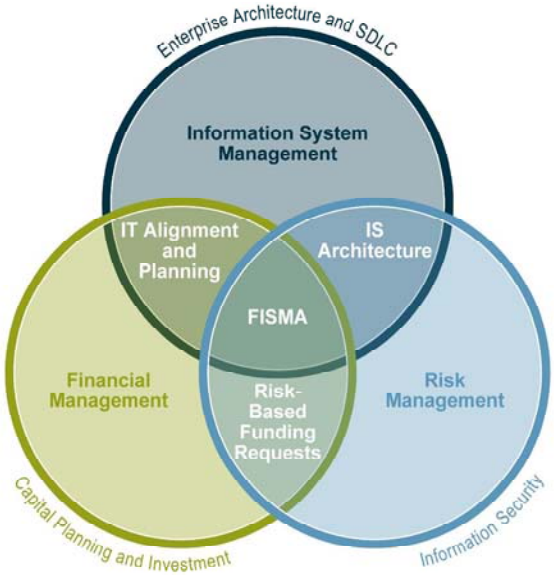


FIGURE 2-1. POSITIONING SECURITY CONSIDERATIONS

Executing a risk management-based approach for systems and projects means integrating security early and throughout the agency's established system and CPIC life cycles. 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 helps document security-relevant decisions and provides assurance to management that security was fully considered in all phases. System managers can 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 can

[1] NIST Draft Special Publication 800-39, *Managing Risk from Information Systems: An Organizational Perspective,* describes a framework for building an information system security risk management program.

use this information 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.

There are many SDLC methodologies that can be used by an organization to effectively develop an information system. A traditional SDLC, a linear sequential model (also known as waterfall method), 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 may 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 rapid application development (RAD) model, the joint application development (JAD) model, the prototyping model, and the spiral 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 the SDLC model will be defined by an organization's acquisition policy. Appendix E provides an overview of other SDLC methodologies.

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.

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. The 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. Procurement-centric operations have unique sets of vulnerabilities due to the potential unknowns and uncontrollable nature of supply chains. These vulnerabilities should be understood and factored into any risk-based decisions.

A typical SDLC includes five phases: initiation, development/acquisition,[2] 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 that phases may continue to be repeated throughout a system's life prior to disposal.

[2] This publication does not provide an exhaustive description of the acquisition processes. Organizations should refer to the appropriate Federal Acquisition Regulations (FAR) and organization-specific policies and procedures for detailed acquisition information.

- Initiation. During the initiation phase, the need for a system is expressed and the purpose of the system is documented.
- Development/Acquisition. During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed.
- Implementation/Assessment. After system acceptance 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.

The SDLC 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.

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

2.1.2 Introduction to Security Integration

Executing a risk management-based approach for systems and projects means integrating security into the agency's established system development and CPIC life cycles. 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 life cycle. Full and effective integration within the SDLC enables information security professionals, partnered with CPIC, IT and EA representatives, to promote effective management and oversight of security considerations throughout the life cycle.

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 life cycle. 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 life cycle is to plan and implement a comprehensive risk management program (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 Circular 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 allows agencies to ensure that capital planning and information 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 information security controls and ensuring effective protection of federal IT resources should be accounted for in the capital planning process.

2.1.4 Security Architectures

Security architectures should be in line with NIST guidelines consisting of security control families outlined in NIST 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 roadmap for integrating security functionality and assurance into the 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 life cycle considerations to legacy information systems that have been in operation for some extended period of time. Some legacy systems may have excellent security plans that provide comprehensive documentation of the risk management decisions that have been made, including identifying the security controls currently employed. Other legacy systems may have limited documentation available. The security considerations, however, are still relevant to these legacy systems, and should be applied and documented to ensure security controls are in place and functioning effectively to provide adequate protections for the information and the information system.

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 is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organization operations and assets, individuals, other organizations, and the Nation. To do this, the AO relies primarily on: (i) the completed security plan; (ii) the security assessment report; and (iii) the plan of action and milestones for reducing or eliminating information system vulnerabilities.
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.
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 business and programmatic interests in the information system during the SDLC process. The program manager 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 test and evaluation, 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. This person reviews system specifications and determines test needs, and works 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 promulgating policies on security integration in the SDLC and 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.
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 is responsible for the procurement, development, integration, modification,

Role	Responsibilities
	operation, and maintenance of an information system.
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 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.

CHAPTER THREE

INCORPORATING SECURITY INTO THE SDLC

This section describes a number of security considerations that will help integrate information security into the SDLC. Security considerations are identified in each SDLC phase, thus advancing the business application 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. THE SDLC – A CONCEPTUAL VIEW

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

- Provides a brief description of the SDLC phase.
- Identifies 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. Control gates are valuable in that they provide the organization with the opportunity to verify that security considerations are being addressed, adequate security

is being built in, and identified risks are clearly understood before the system development advances to the next life cycle phase.

- Identifies and describes major security activities in each phase. Each activity is then further defined 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

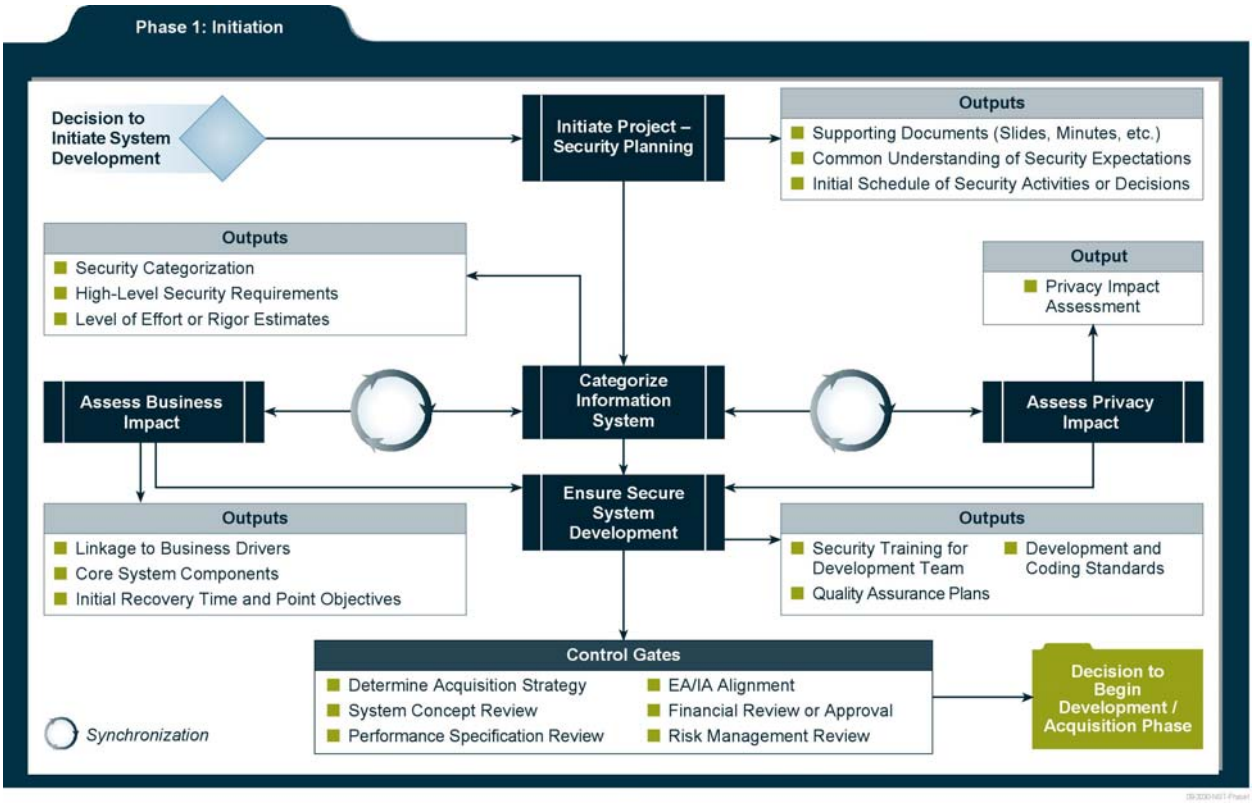


FIGURE 3-2. RELATING SECURITY CONSIDERATIONS IN INITIATION PHASE

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 information 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 activities 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; and
- 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:

- A determination of the acquisition strategy to be used throughout the remainder of the development process;
- A system concept review that verifies that the concept is viable, complete, achievable, and in line with organizational mission objectives and budgetary constraints;
- A performance specification review that ensures that the initial system design has addressed all currently identified specified security requirements;
- An enterprise architecture (EA) alignment that harmonizes IT vision, standards, and business requirements, as well as security alignment with current and imminent security services;
- A financial review that verifies that the system will be aligned with CPIC artifacts and guidance while balancing the cost implications associated with risk management; and
- A risk management review that conforms to the recommended NIST risk management framework guidelines to reduce ambiguity in managing system risk. Included in this risk management review is a review of the information system security categorization results, which include identified information types, resulting impact levels, and the final system security categorization.

3.1.3 Major Security Activities

3.1.3.1 Initiate Security Planning

Description:	Security planning should begin in the initiation phase by: • Identifying key security roles for the system development; • Identifying sources of security requirements, such as relevant laws, regulations, and standards; • Ensuring all key stakeholders have a common understanding, including security implications, considerations, and requirements; and • 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 carry out the responsibilities. Identifying the ISSO early in the process provides the individual key insights into risk-based decisions made early in the process and provides the other team members access to the ISSO for support in integrating security into the system development. Stakeholder Security Integration Awareness The ISSO provides the business owner and developer with an early understanding of the security steps, requirements, and expectations so security can be planned from the beginning. Topics may include:

	• Security Responsibilities • Security Reporting Metrics • Common Security Controls Provided (if applicable) • Certification & Accreditation Process • Security Testing and Assessment Techniques • Security Document & Requirement Deliverables • Secure Design, Architecture, and Coding Practices • Security Acquisition Considerations • 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:	• Supporting documents (slides, meeting minutes, etc.) • 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
• Security planning in the initiation phase should include preparations for the entire system life cycle, including the identification of key security milestones and deliverables, and tools and technologies. Special consideration should be given to items that may need to be procured (e.g., test/assessment tools). • 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 ISSO for multiple systems, a planned approach will increase their ability to multi-process, such as assigning common systems or common organizations with ownership. • Consult with agency Records Management, Privacy, and Freedom of Information Act (FOIA) officials early in the development life cycle to ensure compliance with applicable laws and agency policy.

3.1.3.2 Categorize the Information System

Description:	Security categorization, which corresponds to step 1 in the NIST Risk Management Framework, 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 and described in NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. 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. Federal Information Processing Standard (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 information and 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 and guidelines assist organizations in making the appropriate selection of security controls for their information systems.
Expected Outputs:	• Security Categorization - Essential to the security categorization process is documenting the research, key decisions, and supporting rationale for the information system security categorization (this is included in the System Security Plan). • High-Level Security Requirements • Level of Effort Estimates - Initial level of effort can be derived from applying the resulting security categorization to the minimal security controls in NIST SP 800-53, and assessment procedures in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.
Synchronization:	The security categorization should be revisited if there are significant changes to the information system 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,[3] 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	

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

agency's mission importance; life cycle and timeliness implications; configuration and security policy-related information; special handling requirements; etc., and make adjustments if necessary. • Even though information system security categorization may result in moderate- or high-impact system identification, the individual SP 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.

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 life cycle 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:	• Identify lines of business supported by this system and how those lines of business will be impacted; • Identify core system components needed to maintain minimal functionality; • Identify the length of time the system can be down before the business is impacted (initial idea of the needed Recovery Time Objective); and • Identify 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 the 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 complementary activity that provides checks and balances to ensure that 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 business impact assessments (BIA), disaster recovery (DR), contingency planning (CP), and continuity of operations (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 Impact

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 information types. Once identified as a system under development that will likely handle privacy information, the system owner should work towards identifying and implementing proper safeguards and security controls, including processes to address privacy information incident handling and reporting requirements. Many agencies 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 to 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. • This will have an impact on the System Security Plan, Contingency Plan, and Business Impact Assessment that may need to be captured in these documents.
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. • OMB M-06-16 and OMB M-07-17.	

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 defects in functional behavior and business process logic. 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 contingency 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, appropriate security processes for the assurance level required by the system should be determined and documented. 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 as well as training for secure design and coding techniques. 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 intentional or not) causing vulnerabilities in the system. *Secure Environment.* The system development environment should meet minimum FISMA compliance criteria as expressed in SP 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 reused 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 to a secure development environment.
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 defects and attack methods is essential to protecting the system against them. Providing application security training to the development and testing teams 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 developed and released to quality assurance (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 defects 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/Acquisition

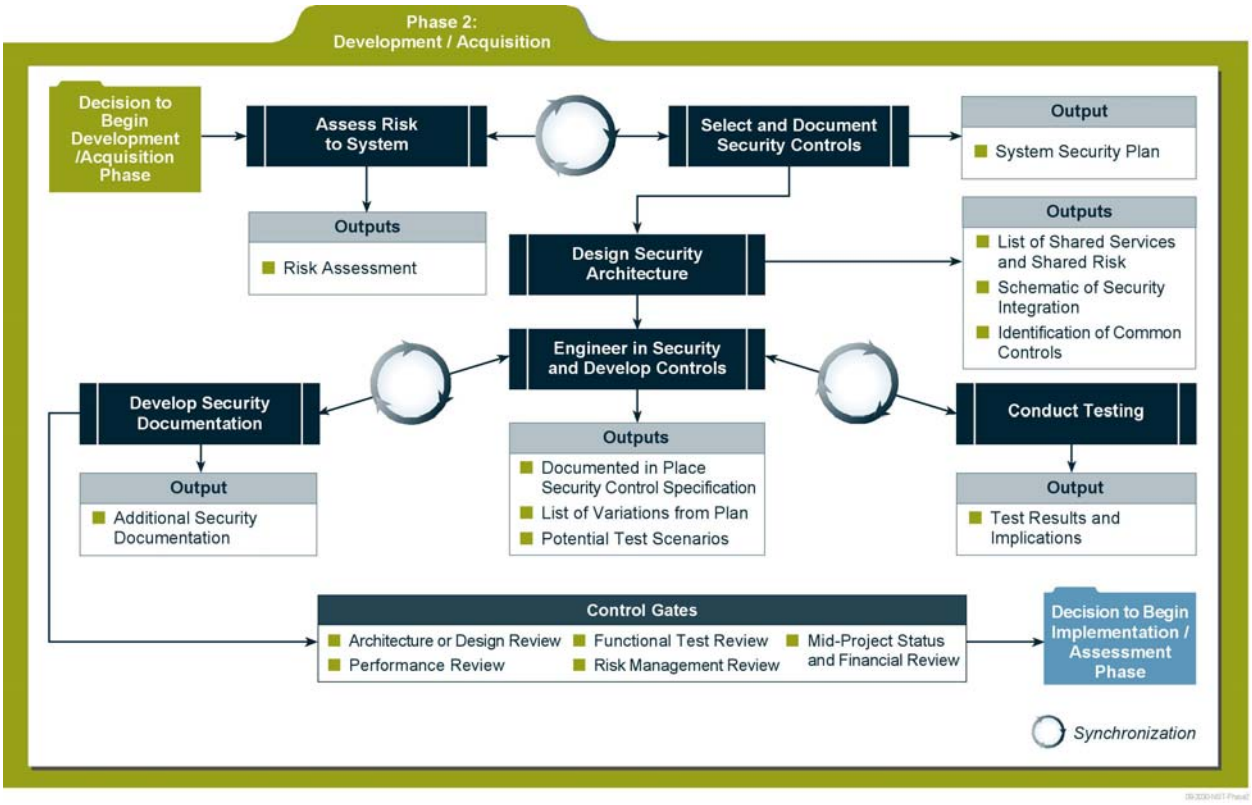


FIGURE 3-3. RELATING SECURITY CONSIDERATIONS IN THE DEVELOPMENT/ACQUISITION PHASE

3.2.1 Description

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

- Conduct the risk assessment and use the results to supplement the baseline security controls;
- Analyze security requirements;
- Perform functional and security testing;
- Prepare initial documents for system certification and accreditation; and
- Design security architecture.

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 that evaluates whether the system is delivering, or capable of delivering, to the documented expectation of the owner and whether the system behaves in a predictable manner if it is subjected to improper use. (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 Security 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 a 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 of threats and vulnerabilities.
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 required protection for information and information systems.

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. Continuously monitoring internal sources and using 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 and address 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, unlicensed or intentionally compromised material.

3.2.3.2 Select and Document Security Controls

Description:	The selection and documentation of security controls corresponds to step 2 in the NIST Risk Management Framework. The selection of security controls consists of three activities: the selection of baseline security controls (including common security controls); the application of security control tailoring guidance to adjust the initial security control baseline; and the supplementation of the tailored baseline with additional controls based on an assessment of risk and local conditions. An organization-wide view is essential in the security control selection process to ensure that adequate risk mitigation is achieved for all mission/business processes and the information systems and organizational infrastructure supporting those processes. . The security control selection 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 security controls selected. 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. The security controls allocated to individual information systems are documented in the system security plan as described in NIST Special Publication 800-18. Security plans provide an overview of the security requirements for the information systems within an organization and describe the security controls in place, or planned, for meeting those requirements. The plans also describe the rationale for security categorization, tailoring, and supplementation activities, how individual controls are implemented within specific operational environments, and any use restrictions to be enforced on information systems due to high-risk situations. Security plans are important because they document the decisions taken during the security control selection process and the rationale for those decisions. They are approved by appropriate authorizing officials within the organization and provide one of the key documents in security accreditation packages that are instrumental in authorization decisions.
Expected Outputs:	• System Security Plan - specification of security controls that identify which, where, and how security controls will be applied.
Synchronization:	• Security controls and associated specifications should reflect appropriate levels of protection to the system in line with the security control selection criteria. • 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 control requirements will be incorporated into the system security plan. • The risk assessment is a primary tool to identify if the tailored security controls are effective to address an organization's risk tolerance.
Implementer's Tips	
• Addressing security requirements in a matrix format allows the developers and security engineers to review implementation per major system component and can facilitate gap analysis, ensuring proper risk analysis and control implementation. • Information 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 for each added functional requirement. Then it is possible for undocumented risk to enter the system. • More detailed "attack prevention" requirements will also help to ensure that 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 assessments 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. • Agencies should initiate disposition planning during this phase and plan for disposal/transition throughout all phases of the life cycle. This activity is best done as part of the requirements phase so full resource requirements for disposal are understood and planned for. Disposition procedures can provide value throughout the life cycle, as hardware and software becomes obsolete or damaged in other phases.	

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 be integrated into the system. An enterprise alignment of the system should ensure that the initiative fits the agency's 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 providing details on where, within the system, security is implemented and 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. • 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 normal development activities. 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/technology 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 security control variations resulting from development decisions and tradeoffs. • 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 referenced in the system security plan.

Implementer's Tips
Documenting security deviations from initial security requirements 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

Description:	While the most prominent document is the System Security Plan, documentation supporting it may include: • Configuration management plan • Contingency plan (including a Business Impact Assessment) • Continuous monitoring plan • Security awareness, training and education (SATE) plan • Incident response plan • Privacy impact assessment (PIA) Development of these documents should consider the maturity of the security services being documented. 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 DR 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 the system development progresses can provide cost savings and enhance decision-making capabilities through a comprehensive approach that allows early detection of gaps.
Expected Outputs:	• Additional security documentation supporting the system security plan.
Synchronization:	These documents will need to be updated toward the end of user acceptance testing to ensure that they are accurate.
Interdependencies:	• System security documentation should align with: o Security requirements analysis o Security architecture o Business impact assessment, and o Security categorization.

Implementer's Tips
• Security operations should not be driven by documentation of compliance but based on system need and described in compliance with security guidance. • For major systems that are large in size, complex in design, or politically sensitive, it is best to assign a point of contact POC) to each document and initiate development with a meeting on the document's scope, expectations, and level of granularity.

3.2.3.6 Conduct Testing (Developmental, Functional and Security)

Description:	Systems being developed or undergoing software, hardware, and/or communication modification(s) must be tested and evaluated prior to being implemented. The objective of the test and evaluation process is to validate that the developed system complies with the functional and security requirements. Testing of security controls is based on technical security specifications for

	those controls supplemented by 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 specificity, the testing must be scoped to test the relevant security requirement as it is intended for use in its environment. 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 that the test process is repeatable and iterative. The use of automated testing tools and integration of the NIST Security Content Automation Protocol (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 personally identifiable information (PII) should reside within any system or software during development.
Expected Outputs:	Documentation of test results, including any unexpected variations discovered during testing.
Synchronization:	All test results are returned to developers for configuration-managed updates. Unexpected 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. • The system risk assessment may need updating to accurately reflect current mitigations.

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 issues earlier in the development cycle (e.g., mandatory access controls, secure code development, and firewalls). Preliminary testing is considered development-level testing, not certification and accreditation (C&A) testing but if no changes occur, reuse test results to the 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 that each component or security zone is secure as an entity.
- Capture the process and results of all security testing that occurs throughout the life cycle 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.

3.3 SDLC Phase: Implementation / Assessment

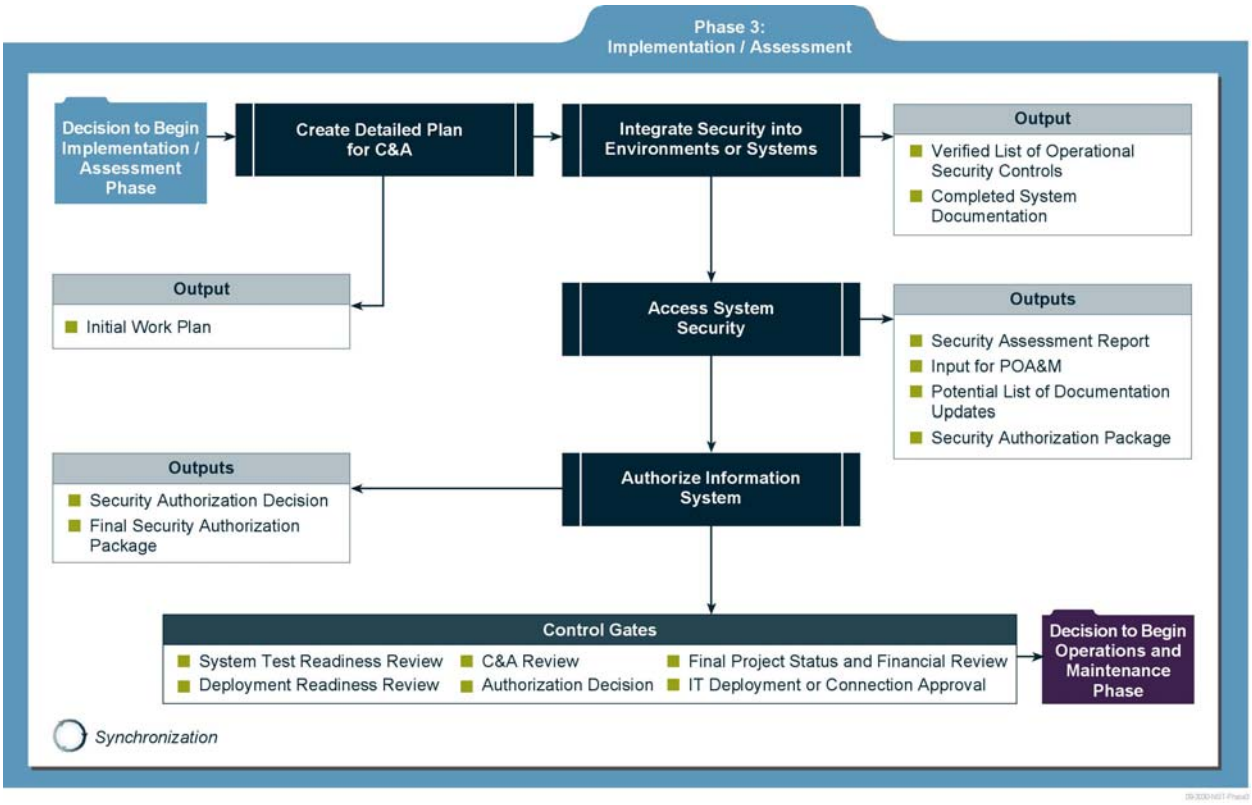


FIGURE 3-4. RELATING SECURITY CONSIDERATIONS IN THE IMPLEMENTATION/ASSESSMENT PHASE

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 activities for this phase include:

- Integrate the information system into its environment;
- Plan and conduct system certification activities in synchronization with testing of security controls; and
- 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
- Authorizing Official (AO) Decision
- IT Deployment or Connection Approval.

3.3.3 Major Security Activities

3.3.3.1 Create a Detailed Plan for C&A

Description:	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 AO 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 AO 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.
Expected Outputs:	• Initial Work Plan: 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.
Synchronization:	ISSO provides the system owner with completed documentation required to initiate and conduct C&A. The AO is notified.
Interdependencies:	Security Controls Assessment Plan will derive the foundational information from this planning document/session.
Implementer's Tips	
• 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 the C&A control gate.	

3.3.3.2 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 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 reoccurrence. • ISSO should review installed system to ensure that 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 that all test data is removed. • Extreme care should be exercised when integrating information systems into operational environments or systems so that critical operations are not disrupted.	

3.3.3.3 Assess System Security

Description:	Systems being developed or undergoing software, hardware, and/or communication modification(s) must be formally assessed prior to being granted formal accreditation. The objective of the security assessment 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*. 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 conducted to ensure continued effectiveness. In addition to verifying security control effectiveness, security certification 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:	• Security Accreditation Package, which includes the Security Assessment Report, the POA&M, and the updated System Security Plan.
Synchronization:	• Certifier provides written Certification Package results to system owner, ISSO, and system administrator. • Assessment results are shared with system owner, ISSO, system administrator, and developers.
Interdependencies:	All previous steps.
Implementer's Tips	
• All documents should be in final state for review to ensure a current picture of the system at review time. • Copying Certification Package to CD/DVD or other electronic media also helps to ensure configuration control and a current archive. • Assigning a core team of representatives from the major stakeholders to meet throughout testing will assist in communication and reduce surprises. • Clearly articulating the C&A process to all parties and agreeing on the level of rigor and scope of testing are very important	

in ensuring a smooth certification effort. • Prioritize continuous monitoring by risk and cost-effectiveness. • Reuse as many prior and relevant assessment results as possible.

3.3.3.4 Authorize the Information System

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 authorization 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 authorizing 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 authorization decision to permit operation of the information system and to accept explicitly the residual risk to agency assets or operations.
Expected Outputs:	• Security Authorization Decision, documented and transmitted from Authorizing Official to System Owner and ISSO • Final Security Authorization Package
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	
Authorizing officials need to make risk decisions not only for the information system, but for the risk extended to the organization as a whole by placing the system into operation.	

3.4 SDLC Phase: Operations and Maintenance

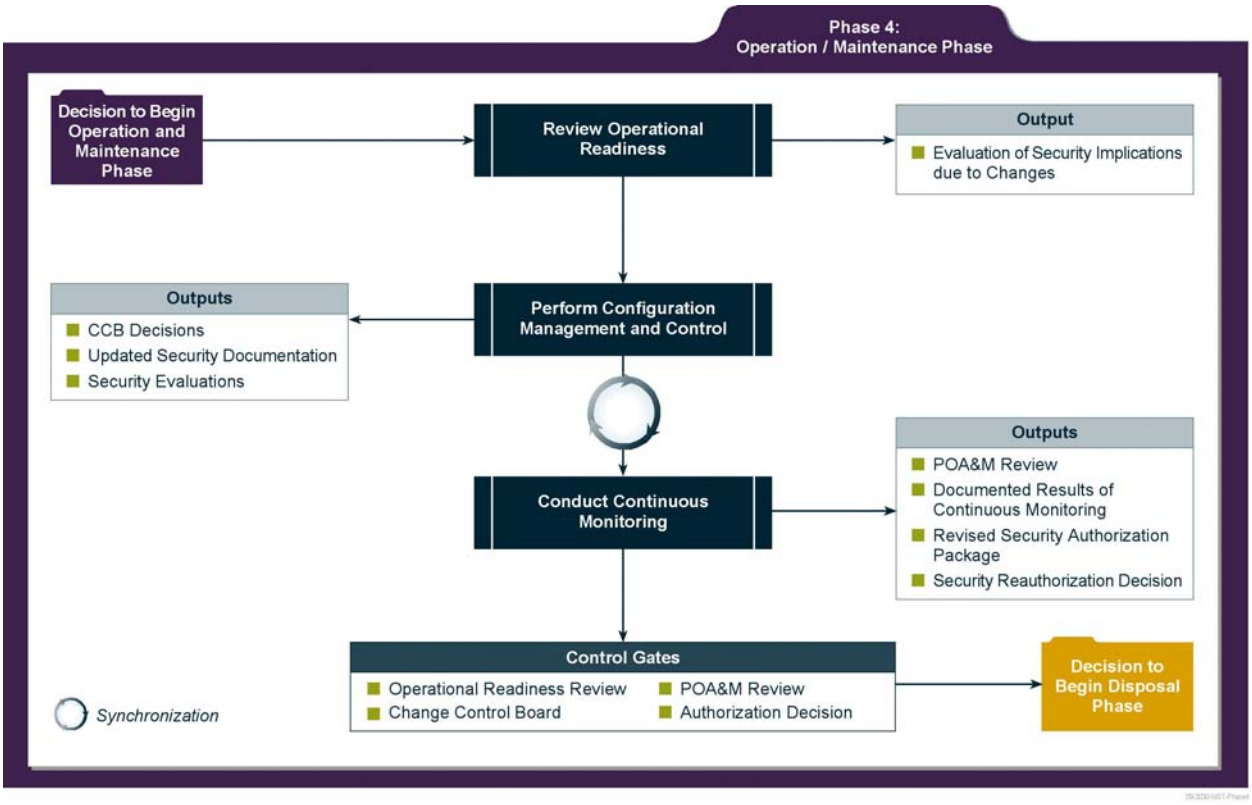


FIGURE 3-5. RELATING SECURITY CONSIDERATIONS IN THE OPERATIONS/MAINTENANCE PHASE

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 reenter a previous phase of the SDLC.

Key security activities 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 reauthorization 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 three years or after a major system change).

3.4.3 Major Security Activities

3.4.3.1 Review Operational Readiness

Description:	Many times when a system transitions to a production environment, unplanned modifications to the system occur. If changes are significant, a modified 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 security implications due to any system changes.
Synchronization:	• System Administrator and ISSO confirmation to System Owner that system is operating normally and compliant with security requirements. • Should a last minute change occur that fundamentally changes the level of risk to the system, the system owner should consider recertification - this is rare.
Interdependencies:	• An operational readiness review supplements the C&A process to ensure that changes are 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. • 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. • Ensure users are adequately trained on security awareness and practices for the new IT system prior to deploying the system in a production environment.	

3.4.3.2 Perform Configuration Management and Control

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:	• Change Control Board (CCB) decisions • Updated security documentation (System Security Plan, POA&M) • Security evaluations of documented system changes
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:	• 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 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. • Abbreviated CM processes that allow for unique emergency 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 Conduct Continuous Monitoring

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. Automation should be leveraged where possible to reduce level of effort and ensure repeatability. Included as a part of continuous monitoring is reaccreditation which 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.
Expected Outputs:	• Documented results of continuous monitoring • POA&M review • Security reviews, metrics, measures, and trend analysis • Updated security documentation and security reaccreditation decision, as necessary

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 reuse upon recertification.
- Continuous monitoring activities can provide useful data to support security performance plans and measures of security return on investment (ROI).
- Defining agency-specific criteria for triggering a reaccreditation 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

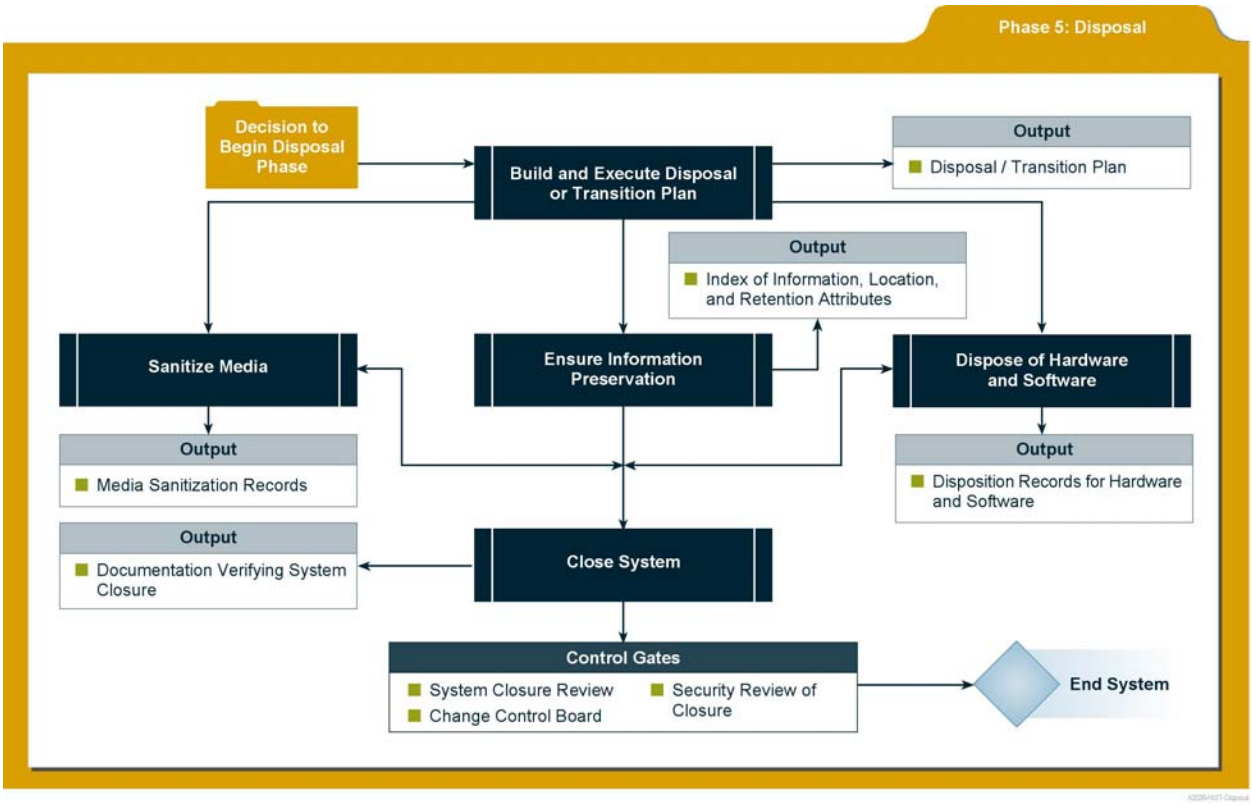


FIGURE 3-6. RELATING SECURITY CONSIDERATIONS IN THE DISPOSAL PHASE

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 a system. 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 activities for this phase include:

- Build and Execute a Disposal/Transition Plan;
- Archive of critical information;
- Sanitization of media; and
- 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 Security 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 disposal/transition plan 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 and security 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. • Do not wait for the disposal phase to make a disposal/transition plan. Plan for disposal/transition throughout all phases of the life cycle. This is best done as part of the requirements phase so full resource requirements for disposal/transition are understood and planned for. Throughout the life cycle, this can be done as hardware and software become 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:	Index of preserved information, and its 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 SP 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:	Media sanitization records
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 so that proper sanitization techniques are applied.

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 may be consulted for additional disposal options or verification of risk.
Expected Outputs:	• Disposition records for hardware and software. These records may include lists of hardware and software released (sold, discarded, or donated), and lists of hardware and software redeployed to other projects or tasks within the organization.
Synchronization:	Updating of system and component inventories.
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 nonprofit 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 and disassembled at this point.
Expected Outputs:	• Documentation verifying system closure, including final closure notification to the authorizing 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 highlights common examples and provides 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[4] 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 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 multidisciplinary 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.

[4] 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 Architecture

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 reaccreditation is cost-effective and manageable.

As many traditional analytic tools (scanners, intrusion detection systems [IDSs], 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), Extensible Access Control Markup Language (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; and
- 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; and 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 that all parties are adequately protected. Further, it is necessary to agree upon test and 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 and Major Migrations

With the fast pace of innovation and correspondingly selective obsolescence in the information technology arena, 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 new challenges in enterprise security as well as risks 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, organizations are likely to experience the following organizational behaviors 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.
- During the eventual C&A of a legacy information system, the adequacy of existing information system security controls will be evaluated. 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.

However, technology advancement, coupled with these anticipated organizational behaviors, provides opportunities for an organization to capitalize on the need for the advanced technology by planning for a secure migration from legacy technologies in a secure manner.

Further, this pattern of behavior is not limited to technology that is truly advanced or new. It is not uncommon for technology developed ten or more years ago to be thrust into the limelight. This technology, however, may have lacked the scrutiny over time to be assured that the discovery of vulnerabilities and active patching of vulnerabilities discovered in similar/equivalent technologies has been conducted.

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 that 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 interrelated in order to supply high availability, 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 LANs (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 interception 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 commonly 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
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) monitoring.

Due to its distributed network and complexity, mobilizing virtualization can further exacerbate 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.
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.

Term	Definition
Contracting Officer (CO)	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.
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 Resources	Information and related resources, such as personnel, equipment, funds, and information technology. *SOURCE: 44 U.S.C., Sec. 3502*
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: 44 U.S.C., Sec. 3542*

Term	Definition
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposal of information. *SOURCE: 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 that the appropriate operational security posture is maintained for an information system or program. *SOURCE: SP 800-53; CNSSI-4009 Adapted*
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. The purpose of this POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. *SOURCE: OMB Memorandum 02-01*
Privacy Impact Assessment (PIA)	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: 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 - ACRONYMS

AO	Authorizing Official
AV	Anti-Virus
BIA	Business Impact Assessment
C&A	Certification and Accreditation
CCB	Change Control Board
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
COI	Community of Interest
CONOPS	Concept of Operations
COOP	Continuity of Operations
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-The-Shelf
CP	Contingency Plan
CPIC	Capital Planning and Investment Control
DR	Disaster Recovery
EA	Enterprise Architecture
FAR	Federal Acquisition Register
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GAO	Government Accountability Office
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IR	Incident Response
ISSO	Information System Security Officer
IT	Information Technology
ITL	Information Technology Laboratory
JAD	Joint Application Development
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
QA	Quality Assurance
RAD	Rapid Application Development
RFP	Request for Proposal
SAISO	Senior Agency Information Security Officer
SAML	Security Assertion Markup Language
SATE	Security Awareness, Training, and Education
SCAP	Security Content Automation Protocol
SDLC	System Development Life Cycle
SLA	Service-Level Agreement
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SP	Special Publication

SSP	System Security Plan
ST&E	Security Test and Evaluation
UDDI	Universal Description, Discovery, and Integration
USC	United States Code
VLAN	Virtual Local Area Network
WSDL	Web Services Description Language
XACML	Extensible Access Control Markup Language

APPENDIX C - 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.

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

Privacy Act of 1974, 5 U.S.C. 552a.

E-Government Act, P.L. 107-347, December 2002.

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

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

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

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, June 2001.

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Information Technology Systems*, February 2006.

NIST SP 800-30,[5] *Risk Management Guide for Information Technology Systems*, January 2002.

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

NIST SP 800-37 Revision 1, Draft *Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach*, August 2008.

NIST SP 800-39, Draft *Managing Risk from Information Systems: An Organizational Perspective*, April 2008

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, December 2007.

[5] NIST SP 800-30 is being revised to focus exclusively on risk assessments with application to the various steps in the Risk Management Framework described in SP 800-39.

NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, June 2008.

NIST SP 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categorization Levels*, August 2008.

NIST SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

NIST Interagency Report (NISTIR) 7298, *Glossary of Key Information Security Terms*, April 2006.

APPENDIX D - NIST REFERENCE MATRIX AND WEBSITES

To assist in further research, the matrix below provides a mapping of relevant NIST publications to the corresponding SDLC security activity. Additional information is available at the following NIST websites: http://csrc.nist.gov and http://nvd.nist.gov/scap.

Security Activity	Supporting NIST Pub(s)
Phase 1 – Initiation	
1. Initiate Security Planning	SP 800-64, -100, -37, -53
2. Categorize the Information System	SP 800-60, FIPS 199
3. Assess Business Impact	SP 800-34
4. Assess Privacy Impact	SP 800-37
5. Ensure Secure Information System Development	SP 800-64, -16
Phase 2 – Development / Acquisition	
1. Assess Risk to System	SP 800-30
2. Select and Document Security Controls	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 above)
Phase 3 – Implementation / Assessment	
1. Create Detailed Plan for C&A	SP 800-37
2. Integrate Security into Established Environments or Systems	SP 800-64
3. Assess System Security	SP 800-37, -53A
4. Authorize the Information System	SP 800-37
Phase 4 – Operation / 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
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

APPENDIX E - OTHER SDLC METHODOLOGIES

There are many SDLC methodologies, in addition to the waterfall methodology discussed in this publication, which can be used by an organization to effectively develop an information system. The expected size and complexity of the system, the development schedule, and the anticipated length of a system's life may affect the choice of which SDLC model to use. In many cases, the choice of SDLC model will be defined by an organization's acquisition policy. Regardless of the methodology employed, or the formality or duration of the development process, it is critical that security requirements and considerations, including key security documentation, are planned for and adequately addressed throughout the entire life cycle.

Joint Application Development

In a traditional waterfall methodology, the development team gathers requirements, many times through a series of interviews with the customer, and then proceeds to develop the application. Using a Joint Application Development (JAD) methodology, however, the client or end user collaborates with the developers through JAD sessions to design and develop an application. Because the development process involves greater involvement of the client, this methodology may lead to faster development and greater client satisfaction.

Prototype Model

The Prototype Model is a development methodology similar to the waterfall model, in that once the requirements analysis is performed and the prototype is designed, the prototype development begins. Once created, the prototype is evaluated by the customer, who then provides feedback to the developer. The developer, in turn, refines the product according to the customer's expectation. After a number of iterations of this process, the final product is provided to the customer.

Rapid Application Development

Rapid Application Development (RAD) is a development methodology that creates an application more quickly by employing techniques aimed at speeding application development, such as the use of fewer formal methodologies and reuse of software components. In exchange for faster development, some compromises in functionality and performance may be realized. It is important to ensure, however, that this exchange for a faster product delivery does not result in compromises being made in the selection and specification of the security controls necessary to provide adequate security for the information and the information system, and the mission function they support.

Spiral Model

The Spiral Model is a development methodology that combines the features of the prototype and waterfall models, and is often favored for large, expensive, and complicated projects. The spiral model process generally involves defining requirements and creating an initial design, and constructing and evaluating the first prototype. This same process is then repeated for subsequent prototypes until the refined prototype represents the product desired. The final system is constructed based on the final prototype, and is evaluated and maintained in a production environment.

APPENDIX F - ADDITIONAL ACQUISITION PLANNING CONSIDERATIONS

This publication has been developed to assist agencies in integrating essential information security steps into an established IT system development life cycle (SDLC). This appendix discusses additional acquisition planning considerations that contribute to information security during the Development / Acquisition phase of the SDLC.

- **Type of Contract**

  The type of contract (e.g., firm fixed price, time and materials, cost plus fixed fee) can have significant security implications. The information security technical representative developing the specifications and the contracting officer should work together to select the contract type that will be most advantageous to the organization.

- **Review by Other Functional Groups**

  Depending on the size and scope of the system, a review of the system by participants from various functional groups (e.g., legal, human resources, physical security, records management) may be useful. These functional groups should have insight into the confidentiality, integrity, and availability requirements. Involving these groups early in the planning process is important because it may result in reduced life-cycle costs, and it is easier to change requirements in the early stages.

- **Review by Certification Agent and Authorizing Official**

  OMB Circular A-130, Appendix III, requires that systems be approved, or authorized, to process data in specific environments. Management, operational, and technical controls must be employed to adequately protect the information system. Management and operational security controls can sometimes be outside the scope of the contract, as the developer, in most cases, cannot be responsible for the organization's implementation of these security controls. The technical security control functional and assurance specifications must be contained in the contract with the developer. These security controls should be factored into the development of the technical specifications. The authorizing official (AO) can take these assumptions into account when deciding on the adequacy of the total set of security controls for reducing the residual risks to an acceptable level.

  C&A testing also includes management and operational security controls implemented by the organization. Determination of the efficacy of these organization-implemented security controls is part of the security controls assessment. Assessment processes should confirm that the assumptions in the system security plan have been implemented, and that the total set of security controls are adequate to reduce the residual risks to an acceptable level. Acceptance testing of the security properties of the contractor-developed system is a prerequisite to security testing as part of the C&A process.

  Because the AO is responsible for accepting the risk of operating the system, they can advise the development team if the risks associated with the 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 AO 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.

- **Cyclical Nature of the Process**

  The security steps in the Development / Acquisition phase may need to be addressed cyclically. These security steps interrelate and build on each other. Depending on the size and complexity of the system, these steps may be performed often as ideas are refined.

- **Evaluation and Acceptance**

  The system evaluation plan and appropriate acceptance criteria are developed in the Development / Acquisition phase. The solicitation should be designed for evaluation, which should include testing and analysis. Specifications should be written in a way to make it easy to clearly determine if the implemented system complies with the specification. In general, two separate activities require security testing – contract acceptance and C&A.

  Contract acceptance usually addresses only the functional and assurance security specifications contained in the contract with the developer. C&A testing also includes management and operational security controls implemented by the organization. The existence and correct operation of controls, which may be assumed by the developer, may have been included as assumptions in the system security requirements. An adequate determination of the organization's security controls as implemented is part of C&A testing. Acceptance testing of the security properties of the developed system is a prerequisite to security testing under the C&A process.

- **Request for Proposal (RFP) Development**

  An RFP enables an organization to make a best-value decision based on an offeror's proposal. One strength of the RFP process is the flexibility it provides the government and the offeror to negotiate a contract that best meets the government's needs.

  The organization can identify needed information security features, procedures, and assurances in many ways. An RFP can be a flexible document. Guidance on acquisition alternatives should be obtained from the organization's acquisition office or the contracting officer.

- **Security Specifications and Statement of Work Development**

  Security specifications and the statement of work (SOW) are based on the requirements analysis. The specifications provide details of what the system is supposed to do. Specifications should also be written independently of the implementation mechanisms, strategy, and design. In other words, the specifications should state what the system is to do, not how. The developer's implementation of the system in conformance with the specifications can and should be tested. This implies that well-written specifications are those that can be tested.

  The SOW details what the developer must do in the performance of the contract. Documentation developed under the contract, for example, is specified in the SOW. Security assurance requirements, which detail many aspects of the processes the developer follows

and what evidence must be provided to assure the organization that the processes have been conducted correctly and completely, may also be specified in the SOW.

There is an exception to the general rule that security functional requirements map into security specifications. Selection of mechanisms to implement security functions may occur during the system operation life cycle rather than during proposal preparation. Such decisions may be deferred to the system operational life cycle to respond to changes in technology or the security environment. For example, the authentication mechanism may change from memorized reusable password to token to biometric technique during the life cycle. The acquiring organization may deal with selection of mechanisms to implement security functions during the system operation life cycle by tasking the developer in the SOW to perform a study and to recommend a mechanism or combination of mechanisms. The selection of the mechanism or combination of mechanisms remains the procuring organizations function.

Experience has shown that if the specifications and the SOW do not delineate the security properties of the system completely and unambiguously, then the system may not achieve the desired level of security.

The following sections describe two sources for information security specifications: general specifications and federally mandated specifications. The acquisition initiator should focus on what is required and work with the contracting officer to determine the best way to ask for it.

- General Specifications

  Many sources of general information security specifications are available and may include NIST guidelines, commercial sources, and industry organizations.

  General information security specifications should be reviewed for applicability to the system being acquired. These specifications may provide information about overlooked areas. They can also save time because they provide language that can be used directly. However, care should be taken when selecting features, procedures, and assurances from these sources. The items may be grouped in these documents based on interdependencies among the items. It is necessary to understand the features, procedures, assurances, and groupings before specifying them separately.

  Each specification must be justified from the requirements analysis, specifically from the risk assessment. Safeguards recommended by a general source should be considered, but they should not be included in an RFP if the risk assessment does not support them.

- Federally Mandated Specifications

  Agencies must also include additional specifications in the RFP, as required by law. These are often referred to as directed specifications. All federal agencies must ensure that systems comply with applicable federal policies and FIPS publications. Agencies may require directed specifications, which are official policies issued with the concurrence of organization’s legal and acquisition officials.

  Directed specifications must be incorporated in an RFP or other applicable acquisition document if the system being acquired matches the criteria in the directed specification. It is very important to be aware of directed specifications.

It is the acquiring agency's responsibility to incorporate applicable law, regulations, and policy in the RFP. In addition to mandates affecting the entire Executive Branch, each department and independent agency has its own set of directives, orders, and standards.

Merely citing the requirements separately from technical specifications has proven to be inadequate. Leaving it up to the development contractor to interpret policy does not work. Rather, relevant policy and guidance should be interpreted or at least referenced in the technical security specifications.

Federal Information Processing Standard (FIPS) publications may be found at the NIST Computer Security Resource Center (http://csrc.nist.gov). Applicable OMB circulars, memorandums, and policy documents may be found at http://www.whitehouse.gov/omb.

The National Technology Transfer and Advancement Act of 1995 (Public Law [P.L.] 104-113) directs federal government departments and agencies to use, when practical, technical industry standards that are developed in voluntary, consensus-based standards bodies.

It is incumbent on the acquisition initiator to know what federally mandated specifications apply to the system(s) being procured. Many people erroneously believe that the contracting officer is responsible for this effort. Because these are technical issues, the responsibility is that of the acquisition initiator.

- **Proposal Evaluation**

  The proposal evaluation process determines if an offer meets the minimum requirements described in the RFP and assesses the offeror's ability to successfully accomplish the prospective contract. This effort involves a technical analysis of the merits of a proposal. As part of the Development / Acquisition phase, the acquisition initiator, working with the contracting officer, develops an evaluation plan to determine the basis for the evaluation and how it will be conducted. The evaluation itself is performed during the source selection phase of the acquisition. Information security should be addressed in the evaluation criteria to call attention to the importance of security to the government. Offerors study the RFP to understand what the government considers most important.

- **Developing an Evaluation Plan**

  When evaluating information security features, it can be difficult to assess if the offer meets the minimum requirements or can successfully accomplish the prospective contract. Therefore, offerors should provide assurance to the government that hardware and software claims regarding information security features are true, and that the offeror can provide the proposed services. Because information security, like other aspects of computer systems, is a complex and important subject, the offeror's assertions may not provide sufficient assurance.

  How assurances are provided may determine the government's ability to adequately assess them. The SOW specifies the government's requirements on the development of the system, including the assurance requirements. Assurance specifications typically include documentation that will be examined by the government. After award, if the government determines that more assurance is required, additional funding may be required to fully develop the system.

The determination of how the offerors will be required to provide assurance should be considered when developing the evaluation plan. This plan will be used to help develop RFP sections that provide instructions to the offerors and information about how the proposals will be evaluated and how source selection will be performed.

As part of this process, a determination of security acceptance testing should be made. It may be important to coordinate security test and evaluation (ST&E) activities as part of acceptance as well as C&A to effectively manage the government's efforts.

A certain amount of test and evaluation may occur as part of proposal evaluation. Benchmarking and functional demonstrations can be employed. Benchmarking has included stress testing (e.g., response time, throughput), which is similar to some security testing. Selecting the breadth and depth of such benchmarking is a business decision. Both the government, as purchaser, and the offeror incur costs. Either party may decide that the costs are prohibitive. It may be possible to structure proposal evaluation to limit the number of proposals that receive intensive ST&E. For example, security functional demonstrations could be required of all offerors, whereas assurance and penetration testing could be applied to only the apparent selectee.

There are significant differences among ST&E of existing products, systems to be developed, and services. Organizations will have some uncertainty about services and the systems to be developed. One approach is to consider the failure to deliver the proposed security functions, assurances, and services as a breach of contract for which various legal remedies exist. The government can structure the pre-award functional demonstrations so that they provide meaningful and consistent results for evaluation purposes.

It is important that the threats to security and organizational security policy commitments be clearly articulated and that the proposed security measures be demonstrably sufficient for their intended purpose. Assurance should be based on an evaluation (active investigation) of the product or information system that is to be trusted. The validity of the documentation and of the resulting IT product or system should be measured by expert evaluators with increasing emphases on scope, depth, and rigor.

Architecture and design have a significant impact on vulnerabilities and testing. Good design includes testability as criteria. The cost of ST&E can be minimized by an architecture and design that reduces the security impact of employing systems and services with unknown security properties. Security architecture and design should employ techniques (e.g., encapsulation and isolation), and mechanisms (e.g., demilitarized zones and firewalls) to mitigate vulnerabilities and risks and the cost of ST&E.

Security architecture that integrates countermeasures should be considered. These countermeasures include point solutions for individual networks (e.g., firewalls and intrusion detection systems [IDSs]), security information management (SIM) systems, and SIM integration with a secure network management system.

- **Items to Consider in the Evaluation Plan**

  The remainder of this section presents ideas to help develop the information security portions of the evaluation plan.

  When the evaluation plan is developed, the functional and security alternatives may conflict with each other. For example, features that provide information security can conflict with those that provide ease of use. The government should clarify how offerors propose different

configurations and present conflicting options and trade-offs. However, care should be taken to keep the size of the proposal manageable to facilitate review and to minimize proposal preparation costs.

Testing is one method of determining if the proposed system or product can meet the information security requirements. Depending on the nature of the system, testing can be part of the proposal evaluation, in the form of live test demonstrations or benchmarks, or it can be part of post-award acceptance testing. During the evaluation process, testing can be used at different times, depending on cost, technical, and acquisition integrity considerations. Expensive tests should be kept to a minimum to help control offeror proposal preparation costs. Not only do expensive proposals limit competition, but also the costs are ultimately passed to the government in higher contract costs.

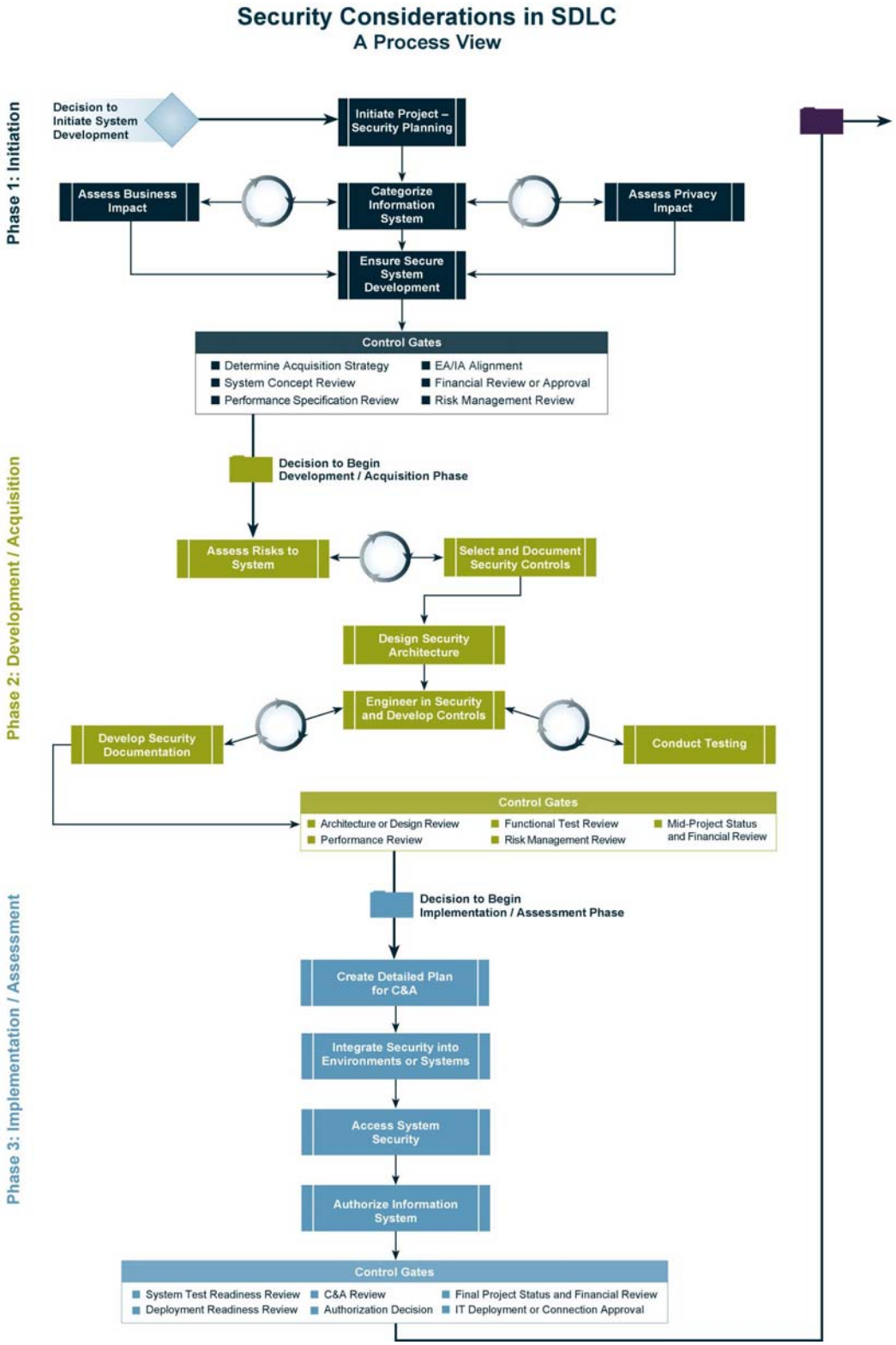
Information system testing, especially performance testing, should be performed with the information security features enabled.

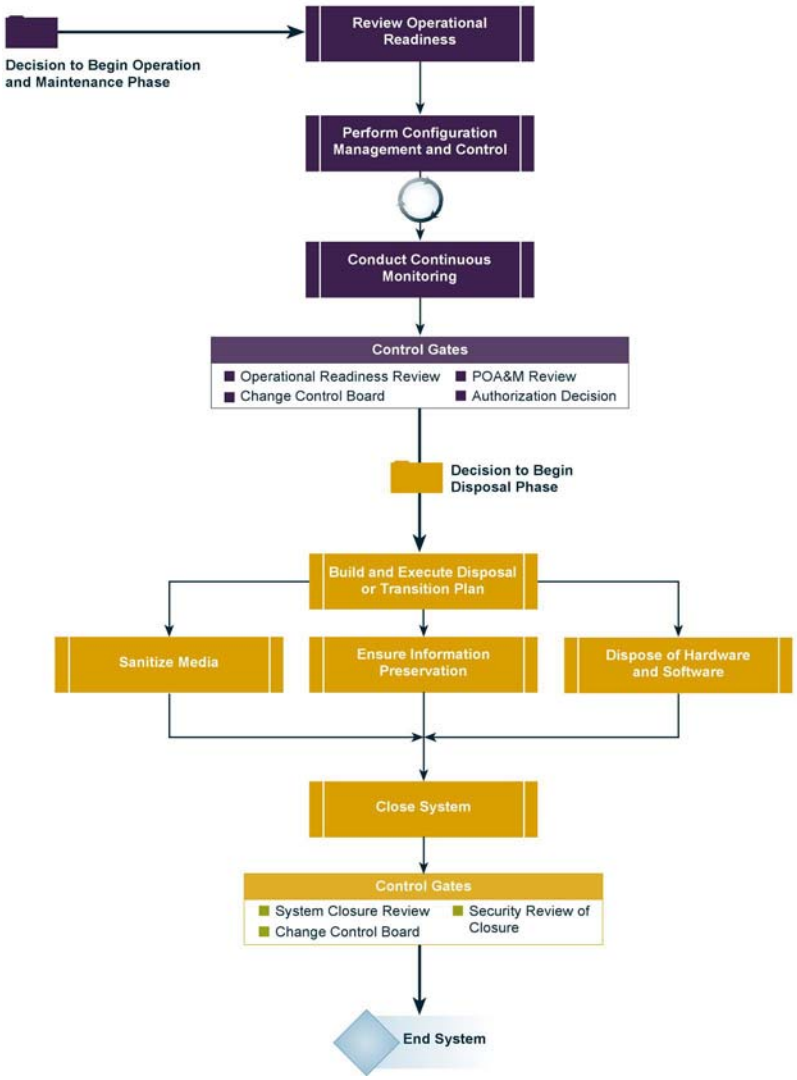
The more the acquisition initiator knows about the marketplace, the easier it is to develop an evaluation plan. However, proposals cannot be used for market research. The evaluation plan cannot be changed after the receipt of proposals. Additional information from other proposals cannot be used to modify the evaluation plan. It is worthwhile to investigate alternatives that could be offered to ensure the development of an evaluation scheme that reflects the true priorities of the government.

- **Special Contract Requirements**

  Some elements in an RFP are information security-related but are not contained in the SOW or the evaluation criteria. These elements usually address rights, responsibilities, and remedies assigned to the parties of the contract. Often, such obligations survive the actual period of performance of the contract. Therefore, such elements are best addressed through specific contract clauses or requirements. The requirement for nondisclosure of information obtained during the course of the contract is one example.

APPENDIX G - ADDITIONAL GRAPHICAL VIEWS OF SECURITY WITHIN SDLC




Phase 4: Operation / Maintenance
Phase 5: Disposal
Decision to Begin Operation and Maintenance Phase
Review Operational Readiness
Perform Configuration Management and Control
Conduct Continuous Monitoring
Control Gates
Operational Readiness Review
POA&M Review
Change Control Board
Authorization Decision
Decision to Begin Disposal Phase
Build and Execute Disposal or Transition Plan
Sanitize Media
Ensure Information Preservation
Dispose of Hardware and Software
Close System
Control Gates
System Closure Review
Security Review of Closure
Change Control Board
End System