NIST Special Publication 800-37
Revision 1

Guide for Security Authorization of Federal Information Systems

A Security Life Cycle Approach

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

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

INITIAL PUBLIC DRAFT

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

August 2008

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

National Institute of Standards and Technology
James M. Turner, 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 other than classified national security information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system 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) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law (P.L.) 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 in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by other (nongovernmental) organizations on a voluntary basis and is not subject to copyright. (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, Secretary of Defense, Director of National Intelligence, Director of the OMB, or any other federal official.

NIST Special Publication 800-37, Revision 1, 81 pages

(August 2008)

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 the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There are references in this publication to documents currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. The methodologies in this document may be used even before the completion of such companion documents. Thus, until such time as each document is completed, current requirements, guidelines, and procedures (where they exist) remain operative. For planning and transition purposes, agencies may wish to closely follow the development of these new documents by NIST. Individuals are also encouraged to review the public draft documents and offer their comments to NIST.

All NIST documents mentioned in this publication, other than the ones noted above, are available at http://csrc.nist.gov/publications.

The public comment period for this document is August 19 through September 30, 2008.

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: sec-cert@nist.gov

Compliance with NIST Standards and Guidelines

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.

- Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.
- Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB FISMA Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.[1]
- Other security-related publications, including NIST interagency and internal reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB.

Schedule for Compliance with NIST Standards and Guidelines

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.[2]
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

[1] While agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility within NIST's guidance in how agencies apply the guidance. Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. When assessing federal agency compliance with NIST guidance, auditors, evaluators, and assessors should consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

[2] The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions. With regard to legacy information systems and the implementation of the new security authorization process, the one-year compliance requirement does not mean that agencies must automatically reauthorize all information systems to be in compliance. Rather, the new guidelines should be applied in accordance with current OMB and CNSS policies, current federal agency authorization/reauthorization cycles, and the agency's transition strategy.

Acknowledgements

This publication was developed by the *Joint Task Force Transformation Initiative* Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities in an ongoing effort to produce unified guidance and a consistent process for authorizing federal information systems to operate. The Project Leader, Ron Ross, from the National Institute of Standards and Technology, wishes to acknowledge and thank the senior leadership team from the U.S. Departments of Commerce and Defense, the Office of the Director of National Intelligence, and the Committee on National Security Systems, and members of the working group whose dedicated efforts contributed significantly to the final publication. The authors also gratefully acknowledge Elizabeth Lennon and Peggy Himes for their superb administrative support. The senior leadership team, working group members, and their organizational affiliations include:

U.S Department of Defense

Honorable John G. Grimes
Assistant Secretary of Defense (NII))
DOD Chief Information Officer

Robert Lentz
Deputy Assistant Secretary of Defense (IIA)

Gus Guissanie
Principal Director, ODASD (IIA)

Eustace D. King
Chief, Acquisition and Technology Oversight, ODASD (IIA)

Don Jones
Senior Policy Advisor, ODASD (IIA)

Office of the Director of National Intelligence

Honorable Dale Meyerrose
Associate Director of National Intelligence and Chief Information Officer

Sherrill Nicely
Deputy Intelligence Community Chief Information Officer (Acting)

Sharon Ehlers
Assistant Deputy Associate Director of National Intelligence for Intelligence Community Technology Governance (Acting)

Roger Caslow
Lead, C&A Transformation

Frank Sinkular
Lead, C&A Transformation

National Institute of Standards and Technology

Cita M. Furlani
Director, Information Technology Laboratory

William C. Barker
Chief, Computer Security Division

Committee on National Security Systems

Honorable John G. Grimes
Chairman, Committee on National Security Systems

Eustace D. King
CNSS Subcommittee Co-Chairman

Joint Task Force Transformation Initiative ≈ Interagency Working Group

Dr. Ron Ross, *Project Leader*
NIST

Marianne Swanson
NIST

Arnold Johnson
NIST

Dr. Stuart Katzke
NIST

Gary Stoneburner
Johns Hopkins University APL

Jennifer Fabius Greene
MITRE Corporation

Dominic Cussatt
IBM Corporation

Chris Sumstine
MITRE Corporation

Glenda Turner
MITRE Corporation

Peter Williams
Booz Allen Hamilton

Anthony Cornish
National Security Agency

George Rogers
BAE Systems, Inc.

Kelley Dempsey
NIST

Christian Enloe
NIST

Peter Gouldmann
U.S. Department of State

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by the Federal Information Security Management Act (FISMA), NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems. In addition to its comprehensive public review and vetting process, NIST is working with the Office of the Director of National Intelligence (DNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. The common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their support contractors, more uniform and consistent ways to manage the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation that results from the operation and use of information systems. In another collaboration initiative, NIST is working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001, Information Security Management System (ISMS).

Notes to Reviewers

This revision to NIST Special Publication 800-37 is historic in nature. For the past two years, NIST has been working in partnership with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and Committee on National Security Systems (CNSS) to develop a common information security framework for the federal government and its support contractors. The project, designated as the *Certification and Accreditation (C&A) Transformation Initiative*, is on target to produce a series of new CNSS policies and instructions that address risk management, security categorization, security control specification, security control assessment, and security authorization and that closely parallel the NIST security standards and guidelines developed during the past five years in response to Congressional legislation known as the Federal Information Security Management Act (FISMA). The CNSS policies and instructions, when approved by the CNSS Chairman and adopted by the national security community, will represent a significant and unprecedented move toward convergence of information security standards, guidelines, and best practices across the Civil, Defense, and Intelligence Communities. NIST plans to continue this rapid convergence by incorporating new material from the CNSS publications into future updates of its core FISMA publications. The ultimate objective of the convergence activities is to develop, whenever possible and practicable, a common foundation for information security for all federal agencies and contractors supporting those agencies and diverging only when necessary to satisfy community-specific requirements.

In the spirit of continuing the rapid convergence, NIST, ODNI, DOD, and CNSS initiated an interagency working group in March 2008 to develop a common security authorization process for federal information systems. The new security authorization process changes the traditional focus from the stove-pipe, organization-centric, static-based approaches to C&A and provides the capability to more effectively manage information system-related security risks in highly dynamic environments of complex and sophisticated cyber threats, ever increasing system vulnerabilities, and rapidly changing missions. The process, designed to be tightly integrated into enterprise architectures and ongoing system development life cycle processes, promotes the concept of *near real-time risk management*, capitalizes on current and previous investments in technology including automated support tools, and takes advantage of over three decades of lessons learned in previous C&A approaches. The ultimate objective is to be able to provide the right information to senior leaders so they can explicitly manage the security risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.

The purpose of revising NIST Special Publication 800-37 is four-fold:

- Develop a common *security authorization process* for federal information systems (currently known as the C&A process).
- Express the process of authorizing information systems to operate as an integral part of the *System Development Life* Cycle and the *Risk Management Framework*;
- Provide a well-defined and comprehensive security authorization process that helps ensure appropriate entities are assigned *responsibility* and are *accountable* for managing information system-related security risks; and
- Incorporate a *risk executive (function)* into the security authorization process to help ensure that managing security risks from individual information systems: (i) is consistent across the organization; (ii) reflects organizational risk tolerance; and (iii) is performed as part of an organization-wide process that considers other organizational risks affecting mission/business success.

This draft publication represents the results of the interagency working group chartered to develop a common process for authorizing federal information systems to operate. It includes the best aspects of current and previous security authorization processes while adhering to the goals and objectives of the C&A transformation.

Your feedback to us, as always, is important. We appreciate each and every contribution from our reviewers. The very insightful comments from both the public and private sectors continue to help shape our publications and ensure that they are meeting the needs of our customers.

-- RON ROSS
FISMA IMPLEMENTATION PROJECT LEADER

Table of Contents

Prologue

"*…Through the process of risk management, leaders must consider risk to US interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations… "*

"…For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations…"

"…Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain…"

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

Security authorization to operate (formerly called certification and accreditation) ensures that on a near real-time basis, the organization's senior leaders ***understand*** the security state of the information system and explicitly ***accept*** the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

≈

CHAPTER ONE

INTRODUCTION

THE NEED FOR MANAGING INFORMATION SYSTEM-RELATED SECURITY RISKS

Organizations[3] in the public and private sectors depend on information technology and the information systems[4] that are developed from that technology to successfully carry out their missions and business functions. Information systems can include a range of diverse computing platforms from high-end supercomputers to personal digital assistants. Information systems can also include very specialized systems and devices (e.g., industrial/process control systems, testing and calibration devices, telecommunications systems, weapons systems, command and control systems, and environmental control systems). Modern information systems are subject to serious *threats* that can have adverse impacts on organizational operations[5] and assets, individuals, other organizations, and the Nation by compromising the confidentiality, integrity, or availability of information being processed, stored, or transmitted by those systems. Threats to information systems include environmental disruptions, human or machine errors, and purposeful attacks. Attacks on information systems today are often aggressive, disciplined, well-organized, well-funded, and in a growing number of documented cases, very sophisticated. Successful attacks on public and private sector information systems can result in great harm to the national and economic security interests of the United States. Given the significant danger of these attacks, it is imperative that leaders at all levels understand their responsibilities in managing information system-related security risks.[6]

Information system-related security risk is just another component of organizational risk that senior leaders must address as a routine part of their ongoing management responsibilities. Organizational risk can include many types of risk (e.g., investment risk, budgetary risk, program management risk, legal liability risk, safety risk, inventory risk, and the risk from information systems). Effective risk management requires recognition that organizations operate in a highly complex and interconnected world using state-of-the-art and legacy information systems that organizations depend upon to accomplish critical missions and to conduct important business. Leaders must recognize that explicit, well-informed management decisions are necessary in order to balance the benefits gained from the use of these information systems with the risk of the same systems being the vehicle through which adversaries cause harm. Managing risk, either information system-related security risk or other types of risk, is not an exact science. It brings together the best collective judgments of the individuals responsible for the strategic planning and day-to-day operations of organizations to provide adequate risk mitigation, which for information system-related security risk, is termed *adequate security*.[7]

[3] The term *organization* is used in this publication to describe an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

[4] An information system is a discrete set of information resources (people, processes, and technology) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information in accordance with defined procedures, whether automated or manual. For manual or nonautomated systems, there are specific policies, directives, regulations, standards, and guidance covering physical protection requirements.

[5] Organizational operations include mission, functions, image, and reputation.

[6] Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of the likelihood of the circumstance or event occurring and of the resulting adverse impacts.

[7] The Office of Management and Budget (OMB) Circular A-130, Appendix III, describes *adequate security* as security commensurate with risk. This risk includes both the likelihood and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

1.1 BACKGROUND

The E-Government Act of 2002 (P.L. 107-347) recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, known as the Federal Information Security Management Act (FISMA), states that effective information security programs include:

- Periodic assessments of risk, including the likelihood and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations/assets of the organization;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and address information security throughout the life cycle of information systems;
- Plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures for continuity of operations for information systems that support the operations and assets of the organization.

FISMA, the Paperwork Reduction Act of 1995, and the Information Technology Management Reform Act of 1996, explicitly emphasize the employment of a risk-based policy for cost-effective security.[8] In support of this legislation, the Office of Management and Budget (OMB) through Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires executive agencies[9] within the federal government to:

- ***Plan*** for security;
- ***Ensure*** that appropriate officials are assigned security responsibility;
- ***Review*** the security controls in their information systems; and
- ***Authorize*** system processing prior to operations and periodically thereafter.

[8] A *risk-based* approach to information security at both the organizational and information-system levels is described in NIST Special Publication 800-39. Reviewing the fundamental risk management concepts in that publication is highly recommended prior to conducting security authorizations of federal information systems.

[9] An *executive agency* is: (i) an Executive Department specified in 5 U.S.C., Section 101; (ii) a Military Department specified in 5 U.S.C., Section 102; (iii) an independent establishment as defined in 5 U.S.C., Section 104(1); and (iv) a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. In this publication, the term executive agency is synonymous with the term *federal agency*.

Security authorization[10] is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation[11] based on the implementation of an agreed-upon set of security controls. The senior official, or *authorizing official*, should be in an appropriate management position with a level of authority commensurate with accepting the risk of operating an information system. Authorizing officials typically are responsible for the mission or business operations supported by an information system. Required by OMB Circular A-130, Appendix III, security authorization challenges managers at all levels to implement the most effective security controls possible in an information system, given mission and business requirements, technical constraints, operational constraints, cost/schedule constraints, and risk-related considerations. By authorizing an information system for operation, an organizational official accepts *responsibility* for the security of the system and is *accountable* for any adverse impacts that may occur if the system is breached thereby compromising the confidentiality, integrity, or availability of the information being processed, stored, or transmitted.

Security control assessment is a process employed by an organization to review the management, operational, and technical security controls in an information system. This assessment determines 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.[12] Security control assessments can include a variety of assessment methods (e.g., interviewing, examining, testing) and associated assessment procedures depending on the depth and breadth of the assessment. Security assessment results in the form of findings describe weaknesses or deficiencies in the security controls employed in an information system and are used to provide an authorizing official with critical information needed to support a credible, risk-based decision on whether to place the system into operation or continue its operation.

Security control assessments do not include a *determination of risk*. The determination of program-level or organizational-level risk generally requires a broader, more strategic view of the organization than can be obtained from the more technically focused, system-level view of the security control assessment. Authorizing officials or their designated representatives are better positioned to make such risk determinations. The ultimate decision on the *acceptability* of such risk is the responsibility of the authorizing official. By authorizing an information system to operate, an authorizing official accepts the risks associated with operating the system and the associated implications on organizational operations and assets, individuals, other organizations, and the Nation. Authorizing officials or their designated representatives may consult other individuals within the organization or external to the organization at any phase in the security authorization process to obtain expert advice on the security state of the information system and its environment of operation and factor that advice into their final risk decisions.

[10] The term *security authorization* is used throughout this publication to be synonymous with the term *security accreditation*. Since both terms are used in current federal policies, directives, instructions, standards, and guidance documents from the Civil, Defense, and Intelligence Communities, a single term was agreed upon for this publication for clarity, consistency, and a closer linkage to the System Development Life Cycle and Risk Management Framework (also known as the *security life cycle*).

[11] Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.

[12] Traditionally, the term *security certification* has been associated with the assessment of security controls in support of security authorization. However, *security control assessment* is a more general term that is now used to describe assessments of security controls at any time during the risk management process.

1.2 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for the security authorization of federal information systems.[13] The guidelines have been developed to help achieve more secure systems within the federal government by:

- Ensuring authorizing officials are appropriately engaged throughout the risk management process;
- Promoting a better understanding of organizational risks resulting from the operation and use of information systems; and
- Supporting consistent, informed security authorization decisions.

The guidelines provided in this special publication have been broadly developed from a technical perspective to be generally useful across a wide range of organizations employing information systems to implement mission and business processes. The guidelines are directly applicable to federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.[14] However, the guidelines may also be used for national security systems with the approval of the Director of National Intelligence (DNI), the Secretary of Defense (DOD), the Chairman of the Committee on National Security Systems (CNSS), or their designees.[15] State, local, and tribal governments, as well as private sector organizations that compose the critical infrastructure of the United States, are also encouraged to consider the use of these guidelines, as appropriate.

1.3 TARGET AUDIENCE

This publication is intended to serve a diverse group of information system and information security professionals including:

- Individuals with information system development and integration responsibilities (e.g., program managers, information technology product developers, information system developers, systems integrators);
- Individuals with information system and security management and oversight responsibilities (e.g., authorizing officials, chief information officers, senior agency[16] information security officers, information system managers, information security managers);
- Individuals with information system and security control assessment and monitoring responsibilities (e.g., system evaluators, assessors/assessment teams, independent verification and validation assessors, auditors, Inspectors General, or information system owners); and
- Individuals with information security implementation and operational responsibilities (e.g., information system owners, common control providers, information owners/stewards, mission/business owners, information system security engineers/officers).

[13] A *federal information system* is defined as an information system used or operated by a federal agency, or by a contractor of a federal agency or by another organization on behalf of a federal agency.

[14] NIST Special Publication 800-59 provides guidance for identifying an information system as a national security system.

[15] The Director of National Intelligence, the Secretary of Defense, and the Chairman of the Committee on National Security Systems have agreed to follow these guidelines with augmentation and tailoring as needed to meet their organizational requirements.

[16] The term *agency* is used in this publication in lieu of the more general term *organization* only in those circumstances where its usage is directly related to other source documents such as federal legislation or policy.

1.4 TRANSFORMING SECURITY AUTHORIZATIONS

Traditional security authorization approaches have been largely stove-piped, organization-centric activities that have viewed information security and risk management from a static (point-in-time) perspective. These approaches have not been conducive to achieving many of the important capabilities needed to create a *single information environment* for the federal government and its support contractors— capabilities such as timely information sharing, reuse of security-related information, reciprocity of security authorizations, ongoing authorizations with continuous monitoring, and managing risk in fast-paced, dynamic environments of operation with ongoing, sophisticated cyber threats. Moreover, traditional approaches to security authorization have not been tightly integrated into Enterprise Architectures or system development life cycle (SDLC) processes and have, in many cases, separated the process of managing information system-related security risks from managing other organizational risks that must be considered by senior leaders in carrying out their management responsibilities. The stove-piped, organization-centric approaches to security authorization also tend to discourage the rapid formation of partnership arrangements to support the very diverse missions and business processes carried out by the federal government. And finally, static approaches to security authorization do not facilitate the timely production of information needed by authorizing officials to make credible risk-based decisions regarding the continued operation and use of their information systems.

The new security authorization process described in this publication transforms the disparate approaches to Certification and Accreditation (C&A) from the various federal communities and creates a common process to authorize federal information systems for operation. As part of the C&A transformation, a unified information security framework has been developed for the federal government and its support contractors that provides a common foundation of information security building blocks including standardized approaches for: (i) categorizing information and information systems; (ii) specifying management, operational, and technical security controls for information systems; (iii) assessing the effectiveness of security controls; and (iv) managing risk.[17] The C&A transformation objectives are four-fold:

- Develop a common security authorization process for federal information systems that can effectively serve the needs of the Civil, Defense, and Intelligence Communities and provide the capability of near real-time risk management;
- Express the process of authorizing information systems to operate as an integral part of the SDLC and the Risk Management Framework (RMF);[18]
- Provide a well-defined and comprehensive process that helps to ensure appropriate entities are assigned *responsibility* and are *accountable* for managing information system-related security risks; and
- Incorporate a *risk executive (function)* into the security authorization process to ensure that managing information system-related security risks: (i) is consistent across the organization; (ii) reflects organizational risk tolerance; and (iii) is performed as part of an organization-wide process that considers other organizational risks affecting mission/business success.[19]

[17] The standardized building blocks that form the foundation for the *Unified Information Security Framework* can be found in a series of Federal Information Processing Standards (FIPS), NIST Special Publications, and CNSS policies and instructions. See http://csrc.nist.gov and http://www.cnss.gov.

[18] The Risk Management Framework is described in detail in NIST Special Publication 800-39. The SDLC process and its relationship to security authorization are described in Section 2.1.

[19] The *risk executive (function)* is introduced and fully described in NIST Special Publication 800-39.

Ultimately, security authorization is part of a dynamic, risk management process. An information system is authorized for operation at a specific point in time based on the risk associated with the current security state of the system. The inevitable changes to the information system or its environment of operation, and the resulting potential adverse impacts of those changes, require a structured and disciplined process capable of monitoring the effectiveness of security controls on a continuous basis in order to maintain an acceptable security state. Information system monitoring activities are most effective when integrated into the broader life cycle management processes carried out by the organization and not executed as stand-alone, security-centric activities.

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security authorizations including: (i) the integration of information security into the SDLC; (ii) the Risk Management Framework; (iii) the roles and responsibilities of individuals conducting or supporting authorization activities within an organization; (iv) the establishment of information system and authorization boundaries; (v) security control inheritance (i.e., the use of common controls) and its affect on authorization activities; (vi) the contents of security authorization packages and how the information is used to support and inform authorization decisions; (vii) the types of security authorization decisions; (viii) the types of operational scenarios in which security authorization decisions are carried out; (ix) maintenance of security authorizations through continuous monitoring of security controls and the effects on achieving near real-time risk management.
- **Chapter Three** describes the three phases of the security authorization process as an integral part of the Risk Management Framework including: (i) the *preparation* phase; (ii) the *execution* phase; and (iii) the *maintenance* phase. Each phase consists of authorization tasks that identify organizational roles with primary responsibility for carrying out the tasks, supporting roles, corresponding phases in the SDLC where the tasks are typically executed, implementation guidance to amplify and add greater clarity to the tasks, and national security and nonnational security publication references.
- **Supporting appendices** provide additional authorization-related information including: (i) references; (ii) glossary of common terms; (iii) acronyms; and (iv) summary list of phases and tasks.

CHAPTER TWO

THE FUNDAMENTALS

BASIC CONCEPTS ASSOCIATED WITH SECURITY AUTHORIZATION

This chapter describes the basic concepts associated with security authorization including: (i) the integration of information security into SDLC[20] processes; (ii) the relationship of the Risk Management Framework (RMF) to the SDLC; (iii) the roles and responsibilities of individuals conducting or supporting authorization activities; (iv) the establishment of authorization boundaries; (v) security control inheritance (i.e., the employment of common controls) and its effect on authorization activities; (vi) the content of authorization packages; (vii) the types of authorization decisions; (viii) operational scenarios in which authorization decisions are carried out; and (ix) authorization maintenance through continuous monitoring of security controls.

2.1 SYSTEM DEVELOPMENT LIFE CYCLE

All federal information systems, including operational systems, systems under development, and systems undergoing some form of modification or upgrade, are in some phase of the SDLC. Requirements definition is a critical part of the system development process and typically begins in the *system initiation* phase of the SDLC. Security requirements, including those requirements related to security authorization, are a subset of the overall requirements levied on an information system and therefore, should be incorporated into system development at the earliest phases of the SDLC, similar to functional requirements. The RMF described in the next section, provides a framework for dynamically managing risk throughout the SDLC and helps to ensure that appropriate security controls for the information system are developed, implemented, assessed for effectiveness, and maintained. The security authorization tasks listed in Chapter 3 are linked to specific phases in the SDLC where the tasks are typically carried out. Integrating security requirements into the SDLC is the most efficient and cost-effective method for an organization to ensure that its protection strategy is achieved and that authorization activities are not isolated or decoupled from the management processes employed by the organization to develop, implement, operate, and maintain information systems supporting ongoing missions or business functions.

Security authorization tasks should begin early in the SDLC typically during the system initiation (i.e., requirements definition) phase, and are important in shaping and influencing the security capabilities of the system. If security authorization tasks have not been adequately performed during the initiation, development, and acquisition phases of the SDLC, the authorization tasks will, of necessity, be undertaken later in the life cycle and be more costly to implement. In either situation, all of the tasks should be completed prior to placing the information system into operation or continuing its operation to ensure that: (i) information system-related security risks are being adequately addressed; and (ii) the authorizing official explicitly accepts the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

For operational or legacy systems currently in the *operations/maintenance* phase of the SDLC that have not received a prior authorization to operate, organizations should begin the security authorization process by completing all of the tasks in the *authorization preparation phase* (see

[20] There are typically five phases in the SDLC: (i) system *initiation*; (ii) system *development/acquisition*; (iii) system *implementation*; (iv) system *operations/maintenance*; and (v) system *disposition* (disposal).

Chapter 3) in a similar manner to a new development system. The artifacts produced during the authorization preparation phase (e.g., security categorization, security plan) should be compared to the existing artifacts already in place for the operational/legacy system to determine if any anomalies or gaps exist. This process helps to ensure that the desired security state of the information system is compared to the actual security state of the system and appropriate adjustments are made as needed. Once the preparatory work has been completed, the security control assessment and remaining authorization tasks proceed as required.

Many of the activities conducted during the SDLC can support or are complementary to the information security activities that are required to be carried out routinely by organizations. This emphasizes the importance of integrating the security life cycle (as described by the NIST RMF) into the SDLC. Organizations should maximize the use of security-relevant information (e.g., testing results, system documentation, and other artifacts) generated during the SDLC to satisfy requirements for similar information needed for information security-related purposes. Reuse of information helps to reduce or eliminate unnecessary documentation, duplication of effort, and cost that may result when security activities are conducted independently of SDLC processes. Reuse also promotes greater consistency of information used in the design, development, implementation, operation, maintenance, and disposition of an information system including any security-related considerations.

Organizations should ensure that there is close cooperation and collaboration among personnel responsible for the design, development, implementation, operation, maintenance, and disposition of information systems and the information security professionals advising the senior leadership on appropriate security controls needed to adequately mitigate risk and protect critical missions and business processes. Using the well-established concept of *integrated project teams*, security professionals should be an integral part of any information system-related development activities. Making information security requirements and activities an integral part of the SDLC as well as how risk is managed, helps to ensure that the organization's senior leaders, including authorizing officials, consider information system-related security risks to organizational operations and assets, individuals, other organizations, and the Nation and take appropriate actions to mitigate these risks.

Information security requirements should be integrated into program, planning, and budgeting activities within the organization to ensure that the resources to carry out security authorization activities are available when needed. As part of their ongoing management and oversight responsibilities, organizational officials should ensure that adequate resources are allocated to the security authorization process for information systems and for the review and approval of common controls inherited by those systems. Information system owners[21] should identify the resources necessary to complete the authorization tasks described in this publication and notify appropriate organizational officials. Resource allocation includes both funding to carry out the authorization tasks and assigning the personnel needed to accomplish the tasks.[22]

[21] Similar actions are required of *common control providers*. Resource allocations for all common control-related authorization activities are approved by the chief information officer, unless that responsibility is assigned to another organizational official by the head of the organization.

[22] Resource requirements should include funding for training security authorization team members to ensure that they can effectively carry out their assigned responsibilities. In some situations, additional personnel screening may be required on security authorization team members commensurate with the impact level of the information system undergoing authorization.

2.2 RISK MANAGEMENT FRAMEWORK

The Risk Management Framework represents a security life cycle that operates within the SDLC to manage information system-related security risks. The security authorization tasks in NIST Special Publication 800-37 are carried out by an organization during the execution of the RMF.[23] Figure 1 illustrates the six steps in the RMF including Step 5, the authorization step. While shown as a single step in the RMF, authorizing officials have responsibilities throughout the RMF as described in the task list in Chapter 3. Security authorization tasks are the activities in direct support of determining risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of information systems, and ultimately deciding if these risks are acceptable.

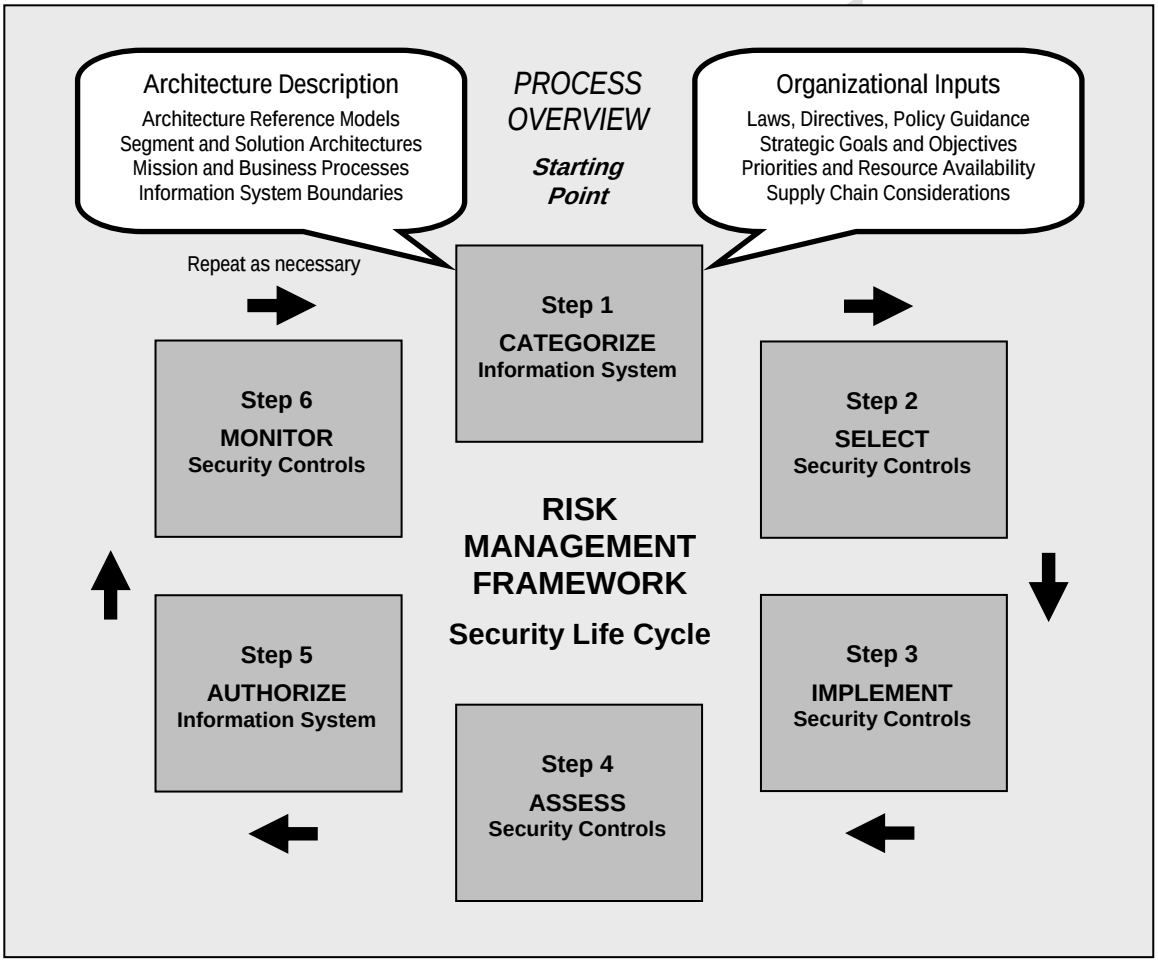

FIGURE 1: RISK MANAGEMENT FRAMEWORK

[23] Security authorization and security control assessment requirements are derived from and are traceable to: (i) the Federal Information Security Management Act (FISMA) and implementing standard FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*; and (ii) Office of Management and Budget (OMB), Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*. Requirements from FIPS 200 are further expressed in the associated security controls for security assessment and authorization in NIST Special Publication 800-53 (as amended), *Recommended Security Controls for Federal Information Systems*. Similar security controls for national security systems can be found in CNSS Instruction 1253.

2.3 ROLES AND RESPONSIBILITIES

The following sections describe the roles and responsibilities of key participants involved in an organization's security authorization process.[24] Recognizing that organizations have widely varying missions and organizational structures, there may be differences in naming conventions for security authorization-related roles and how specific responsibilities are allocated among organizational personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles).[25] However, the basic functions remain the same. The security authorization process described in this special publication is flexible, allowing organizations to effectively accomplish the intent of the specific tasks within their respective organizational structures to best manage information system-related security risks. Many security authorization roles defined in this publication have counterpart roles defined in the routine SDLC processes carried out by the organization. Whenever possible, organizations should align the security authorization roles with similar (or complementary) roles defined for the SDLC process in order to integrate the security life cycle tasks with the tasks from the SDLC.[26] Implemented correctly, the security authorization tasks will be executed concurrently with the organization's ongoing SDLC processes, thereby effectively integrating the process of managing information system-related security risks with ongoing system life cycle processes.

2.3.1 Authorizing Official

The *authorizing official* 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 organizational operations and assets, individuals, other organizations, and the Nation. Authorizing officials typically have budgetary oversight for an information system *or* are responsible for the mission or business operations supported by the system. Through the security authorization process, authorizing officials are *accountable* for the security risks associated with information system operations. Accordingly, authorizing officials should be in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Authorizing officials also approve security requirements, security plans, security assessment plans/reports, memorandums of agreement or understanding, and plans of action and milestones and determine whether or not significant changes in the information systems or environments of operation require reauthorization. Authorizing officials can deny authorization to operate an information system (or if the system is already operational, halt operations) if unacceptable security risks exist. With the increasing complexity of missions/business processes, partnership arrangements, and the use of external/shared services, it is possible that a particular information system may involve multiple authorizing officials. If so, agreements should be established among the authorizing officials and documented in the security plan. Authorizing officials are responsible for ensuring that all activities and functions associated with security authorization that are delegated to authorizing official designated representatives are carried out.[27] The role of authorizing official has inherent U.S. Government authority and should be assigned to government personnel only.

[24] Organizations may define other roles (e.g., facilities manager, human resources manager, systems administrator) to support the security authorization process.

[25] Caution should be exercised when one individual fills multiples roles in the security authorization process to ensure that the individual retains an appropriate level of independence and remains free from conflicts of interest.

[26] For example, the SDLC role of *system developer* or *program manager* can be aligned with *information system owner*; mission *owner/manager* can be aligned with *authorizing official*; and *system/software engineers* are complementary roles to *information system security engineers*.

[27] Authorizing official designated representative responsibilities are described in Section 2.3.2.

2.3.2 Authorizing Official Designated Representative

The *authorizing official designated representative* is an organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization. Authorizing official designated representatives coordinate their activities with the chief information officer, senior agency information security officer, risk executive (function), information system and common control providers, information system security officers, security control assessors, and other interested parties during the security authorization process. Designated representatives can be empowered by authorizing officials to make certain decisions with regard to the planning and resourcing of the security authorization process, acceptance of the security plan and security assessment plan, approval and monitoring the implementation of plans of action and milestones, and the assessment/determination of risk. The designated representative may also be called upon to prepare the final authorization package, obtain the authorizing official's signature on the authorization decision document, and transmit the authorization package to appropriate organizational officials. The only activity that cannot be delegated by the authorizing official to the designated representative is the authorization decision and the signing of the associated authorization decision document (i.e., the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation).

2.3.3 Chief Information Officer

The *chief information officer*[28] is an organizational official responsible for: (i) designating a senior agency information security officer; (ii) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements; (iii) overseeing personnel with significant responsibilities for information security and ensuring that the personnel are adequately trained; (iv) assisting senior organizational officials concerning their security responsibilities; and (v) in coordination with other senior officials, reporting annually to the head of the federal agency on the overall effectiveness of the organization's information security program, including progress of remedial actions. The chief information officer, with the support of the senior agency information security officer, works closely with authorizing officials and their designated representatives to help ensure that:

- An organization-wide information security program is effectively implemented;
- Information security considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, and acquisition/system development life cycles;
- Information systems are covered by an approved security plan and are authorized to operate;
- Security authorizations required across the organization are accomplished in an efficient, cost-effective, and timely manner; and
- There is centralized reporting of all security-related activities.

The chief information officer and authorizing officials also determine the appropriate allocation of resources dedicated to the protection of the organization's missions and business functions and the information systems supporting those missions/business functions based on organizational priorities. In certain instances, for selected information systems, the chief information officer may be designated as an authorizing official or a co-authorizing official with other senior officials. The role of chief information officer has inherent U.S. Government authority and should be assigned to government personnel only.

[28] When an organization has not designated a formal chief information officer position, FISMA requires the associated responsibilities to be handled by a comparable organizational official.

2.3.4 Senior Agency Information Security Officer

The *senior agency information security officer*[29] is an organizational official responsible for: (i) carrying out the chief information officer responsibilities under FISMA; (ii) serving as the chief information officer's primary liaison to the organization's authorizing officials, information system owners, and information system security officers. The senior agency information security officer possesses professional qualifications, including training and experience, required to administer the information security program functions, maintains information security duties as a primary responsibility, and heads an office with the mission and resources to assist in achieving FISMA compliance. The senior agency information security officer (or supporting security staff members) may also serve as authorizing official designated representatives or security control assessors. The role of senior agency information security officer has inherent U.S. Government authority and should be assigned to government personnel only.

2.3.5 Risk Executive (Function)

Organizations need a comprehensive and organization-wide approach for addressing risk—an approach that provides a greater understanding of the integrated operations/business flows of the organization. Authorizing officials may have narrow or localized perspectives in rendering authorization decisions, perhaps without fully understanding or explicitly accepting all of the risks being incurred from such decisions.[30] To address the issues related to managing risk and the associated capabilities that must be in place to achieve adequate security, organizations should include management of information system security-related risks as part of an overall *risk executive (function)*. The intent of the risk executive (function) is to provide a holistic view of risk beyond that risk associated with the operation and use of individual information systems. The risk executive (function) is an individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks in order to ensure mission or business success. The risk executive (function) facilitates the sharing of security risk-related information among authorizing officials and other senior leaders within an organization.

In general, the risk executive (function):

- Provides senior leadership input and oversight for all risk management-related activities across the organization (e.g., security categorizations) to help ensure consistent risk acceptance decisions;
- Ensures that authorization decisions consider all factors necessary for mission and business success organization-wide;
- Provides an organization-wide forum to consider all sources of risk (including aggregated risk from individual information systems) to organizational operations and assets, individuals, other organizations, and the Nation;

[29] Some organizations may use the term *chief information security officer* when describing the responsibilities of the senior agency information security officer.

[30] The original responsibility of authorizing officials published in FIPS 200 and NIST Special Publication 800-37 (authorization with regard to risks to organizational operations, organizational assets, and to individuals) was extended in NIST Special Publication 800-53 and CNSS Instruction 1253 to address risks to other organizations and the Nation.

- Promotes cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility;
- Identifies the overall risk posture based on the aggregated risk from each of the information systems for which the organization is responsible; and
- Ensures that the shared responsibility for supporting organizational mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities.

Organizations have significant flexibility in how the risk executive (function) is implemented. The risk executive (function) presumes neither a specific organizational structure nor formal responsibility assigned to any one individual or group within the organization. The head of the organization may choose to retain the risk executive (function) or to delegate the function to another official (e.g., the chief information officer) or group (e.g., an executive leadership council). However implemented, risk management remains an organization-wide responsibility that starts with the head of the organization and goes through all levels of the organization.

2.3.6 Information System Owner

The *information system owner*[31] is an organizational official responsible for the procurement, development, integration, modification, operation, and maintenance of an information system. The information system owner is responsible for addressing the operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements) and for ensuring compliance with information security requirements. The information system owner is responsible for the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security requirements and security controls. In coordination with the information owner/steward, the information system owner is also responsible for deciding who has access to the system (and with what types of privileges or access rights)[32] and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior). The information system owner informs appropriate organizational officials of the need to conduct the security authorization, ensures that the necessary resources are available for the effort, and provides the required documentation to the security control assessor.[33] The information system owner receives the security assessment results from the security control assessor. After taking appropriate steps to reduce or eliminate vulnerabilities, the information system owner assembles the authorization package and submits the package to the authorizing official or the authorizing official designated representative for adjudication.[34]

[31] The *information system owner* serves as the focal point for the information system. In that capacity, the information system owner serves both as an owner and as the central point of contact between the authorization process and the owners of components of the system including, for example: (i) applications, networking, servers, or workstations; (ii) owners/stewards of information processed, stored, or transmitted by the system; and (iii) owners of the missions and business functions supported by the system). Information system ownership may change during various phases of the SDLC. Some organizations may refer to information system owners as program managers or business/asset owners.

[32] The responsibility for deciding who has access to specific information within an information system (and with what types of privileges or access rights) may reside with the information owner/steward.

[33] In some situations, the notification of the need to conduct a security authorization may come from the senior agency information security officer or authorization official to help ensure compliance with federal or organizational policy.

[34] Depending on how the organization has organized its security authorization activities, the authorization official may choose to designate an individual other than the information system owner to compile and assemble the information for the security authorization package. In this situation, the designated individual must coordinate the compilation and assembly activities with the information system owner.

2.3.7 Common Control Provider

The *common control provider* is an organizational official responsible for the planning, development, implementation, assessment, authorization, and maintenance of common controls (i.e., security controls inherited by information systems).[35] Common control providers are responsible for: (i) documenting common controls in a *security plan* (or equivalent document prescribed by the organization); (ii) ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the organization; (iii) documenting assessment findings in a *security assessment report*; and (iv) producing a *plan of action and milestones* for all controls having weaknesses or deficiencies. Security plans, security assessment reports, and plans of action and milestones for common controls (or a summary of such information) must be made available to information system owners *inheriting* those controls after the information is reviewed and approved by the senior official or executive with oversight responsibility for those controls.

2.3.8 Information Owner/Steward[36]

The *information owner/steward* is an organizational official with statutory or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. In an information-sharing environment, the information owner/steward is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with or provided to other organizations. The owner/steward of the information processed, stored, or transmitted by an information system may or may not be the same as the system owner. Also, a single information system may contain information from multiple information owners/stewards. Information owners/stewards should provide input to information system owners regarding the security requirements and security controls for the systems where the information is processed, stored, or transmitted.

2.3.9 Information System Security Officer

The *information system security officer* is the individual responsible for helping to ensure that the appropriate operational security posture is maintained for an information system.[37] The information system security officer also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. The information system security officer has the detailed knowledge and expertise required to manage the security aspects of an information system and, in many organizations, is assigned responsibility for the day-to-day

[35] Organizations can have multiple common control providers depending on how information security responsibilities are allocated organization-wide. Common controls and inheritance are described in Section 2.5.

[36] Particularly within the federal government, the concept of the *information owner* may not be the most appropriate since citizens ultimately own the information. Federal information is an asset of the Nation, not of a particular federal agency or its subordinate organizations. In that spirit, many federal agencies are developing policies, procedures, processes, and training needed to end the practice of *information ownership* and implement the practice of *information stewardship*. Information stewardship is the careful and responsible management of federal information belonging to the Nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security-related federal policies, directives, regulations, standards, and guidance.

[37] Organizations may also employ an *information system security manager* role that has oversight responsibilities for an information security program. In these situations, information system security officers may report directly to the information system security managers. See Section 2.3.4 on senior agency information security officer responsibilities.

security operations of a system. This responsibility may also include, but is not limited to, physical and environmental protection, personnel security, incident handling, and security training and awareness. The information system security officer may be called upon to assist in the development of the security policies and procedures and to ensure compliance with those policies and procedures. In close coordination with the information system owner, the information system security officer often plays an active role in the continuous monitoring of a system and its environment of operation to include developing and updating the security plan and managing and controlling changes to the system and assessing the security impact of those changes.

2.3.10 Information System Security Engineer

The *information system security engineer* is the individual responsible for conducting information system security engineering activities. Information system security engineering is a process that captures and refines information security requirements and ensures that the requirements are effectively integrated into information technology component products and information systems through purposeful security architecting, design, development, and configuration. Information system security engineers employ best practices when implementing security controls within an information system including software engineering methodologies, security engineering principles, and secure coding techniques. Information system security engineers coordinate their activities with authorizing official designated representatives, chief information officers, senior agency information security officers, information system and common control providers, and information system security officers.

2.3.11 Security Control Assessor

The *security control assessor*[38] is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls in an information system 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. Security control assessors should also provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and recommend corrective actions to address identified vulnerabilities in the system. In addition to the above responsibilities, security control assessors prepare the final security assessment report containing the results and findings from the assessment. Prior to initiating the security control assessment activities, an assessor should provide an assessment of the security plan to help ensure that the plan provides a set of security controls for the information system that is adequate to meet all applicable security requirements.

The required level of assessor independence is determined by the specific conditions of the security control assessment. For example, when the assessment is conducted in support of an authorization decision, the authorizing official makes an explicit determination of the degree of independence required in accordance with federal policies, directives, standards, and guidelines. Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in

[38] Security control assessors may be called *certification agents* in some organizations. At the discretion of the organization, security control assessors may be given additional duties/responsibilities for the post processing and analysis of security control assessment findings and results. This may include, for example, making specific determinations for or recommendations to authorizing officials (known in some communities of interest as *certification recommendations* or *certification determinations*).

order to make an informed, risk-based, authorization decision.[39] The information system owner relies on the security expertise and the technical judgment of the assessor to: (i) assess the security controls in the information system and common controls inherited by information systems using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and address identified vulnerabilities.

2.3.12 User Representatives

User representatives are individuals that represent the operational interests of the user community and serve as liaisons for that community throughout the SDLC. Users are responsible for the identification of mission, business, and/or operational requirements and for complying with the security requirements and security controls described in the security plan. User representatives also assist in the security authorization process, when needed, to ensure that all mission and business requirements are satisfied.

2.4 AUTHORIZATION BOUNDARIES

One of the most challenging problems for information system owners, authorizing officials, chief information officers, and senior agency information security officers is identifying and establishing appropriate authorization boundaries for information systems. Authorization boundaries define the scope of protection for information systems (i.e., what the organization agrees to protect under its direct control or within the scope of its responsibilities) and include the people, processes, and technologies that are part of the systems supporting the organization's missions and business processes. Authorization boundaries need to be established before security categorization and the development of security plans. Authorization boundaries that are unnecessarily expansive (i.e., including too many system components) make the authorization process extremely unwieldy and complex. Boundaries that are unnecessarily limited increase the number of security authorizations that must be conducted and thus unnecessarily inflate the total security costs for the organization. The guidelines in the following sections are provided to assist organizations in defining appropriate information system boundaries to achieve cost-effective solutions for carrying out security authorizations and managing risk from information systems.

2.4.1 Establishing Information System Boundaries

The process of uniquely assigning information resources[40] to an information system defines the security authorization boundary for that system. Organizations have significant flexibility in determining what constitutes an information system and the resulting authorization boundary associated with that system. If a set of information resources is identified as an information system, the resources should generally be under the same direct management control.[41] Direct management control does not necessarily imply that there is no intervening management. It is quite possible for multiple information systems to be validly considered *subsystems*[42] of a single larger system provided all of these subsystems fall under the same higher management authority. This situation may arise in many organizations when smaller information systems are coalesced

[39] Additional information on security control assessor independence is provided in Chapter 3.

[40] Information resources consist of information and related resources including personnel, equipment, funds, and information technology.

[41] For information systems, direct management control involves budgetary, programmatic, or operational authority and associated *responsibility* and *accountability.*

[42] A subsystem is a major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

for purposes of security authorization into a larger, more comprehensive system. In addition to the consideration of direct management control, it may also be helpful for organizations to consider if the information resources being identified as an information system:

- Have the same function or mission objective and essentially the same operating characteristics and information security needs; and
- Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments).

While the above considerations may be useful to organizations in determining information system boundaries for purposes of security authorization, they should not be viewed as limiting the organization's flexibility in establishing commonsense boundaries that promote effective information security within the available resources of the organization. Authorizing officials, chief information officers, and senior agency information security officers should consult with information system owners when establishing or changing information system boundaries. The process of defining boundaries for information systems and the associated authorization implications is an organization-level activity that should include careful negotiation among all key participants—taking into account mission and business requirements, technical considerations with respect to information security, and programmatic costs to the organization.

Supplementing the above considerations, FIPS 199 and CNSS Instruction 1199 define security categories for information and information systems based on potential (worst case) adverse *impact* on organizational operations and assets, individuals, other organizations, or the Nation should there be a breach of security—that is, a loss of confidentiality, integrity (including authenticity and non-repudiation), or availability.[43] Security categories can play an important part in defining appropriate authorization boundaries by partitioning information systems according to impact levels and the importance of those systems in carrying out the organization's missions and business processes. The partitioning process facilitates the cost-effective application of security controls to achieve *adequate security* commensurate with the potential adverse impacts that may arise through the respective information systems.

Software applications do not require a separate security authorization. The applications should be included in the authorization boundary of the information system hosting the applications. The information system employs a set of security controls to provide a foundational level of protection for the hosted applications. Additional application-level controls should be documented in the security plan for the host information system and assessed for effectiveness during the security authorization or subsequent to the authorization if the applications are added after the system has been authorized to operate. Information system owners should ensure that hosted applications do not affect the security state of the hosting system, and should be provided necessary information from application owners to conduct security impact analyses, if necessary.

2.4.2 Boundaries for Large and Complex Information Systems

The application of security controls within large and complex information systems, even when using FIPS 199 and CNSS Instruction 1199 to categorize those systems, may be cost-prohibitive and technically infeasible for the organization. Accordingly, any attempt to assess the security controls in such systems may also be cost-prohibitive and unrealistic. To make this problem

[43] The terms *general support system* and *major application* are no longer used in the context of security authorization. Since general support systems and major applications are both types of information systems, FIPS 199 and CNSS Instruction 1199 are used to categorize the systems, determine the requirements for security controls in order to achieve adequate security, and manage risk.

more manageable, authorizing officials should examine the nature of the information systems being considered for security authorization and the feasibility of decomposing the systems into more manageable components. The decomposition of large and complex systems into multiple components, or *subsystems*, facilitates a more targeted application of security controls to achieve adequate security and promotes a more cost-effective security authorization process.

For large and complex information systems, the authorizing official, chief information officer, and senior agency information security officer, in collaboration with the information system owner and information system security officer, may define subsystem components with established subsystem boundaries. The decomposition into subsystem components should be reflected in the security plan for that large and complex information system. Each subsystem component is fully described in the security plan, an appropriate security category assigned in accordance with FIPS 199 or CNSS Instruction 1199, and an appropriate set of security controls identified. The security category for the large and complex system is the high water mark of the individual subsystem security categories.[44] The extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system, can be determined by combining security control assessments at the subsystem level and adding system-level considerations. This facilitates a more cost-effective security authorization process by enabling scaling of the effort at the subsystem level in accordance with that subsystem's security category and allowing for reuse of assessment results at the system level. Figure 2 illustrates the concept of information system decomposition for a large and complex system.

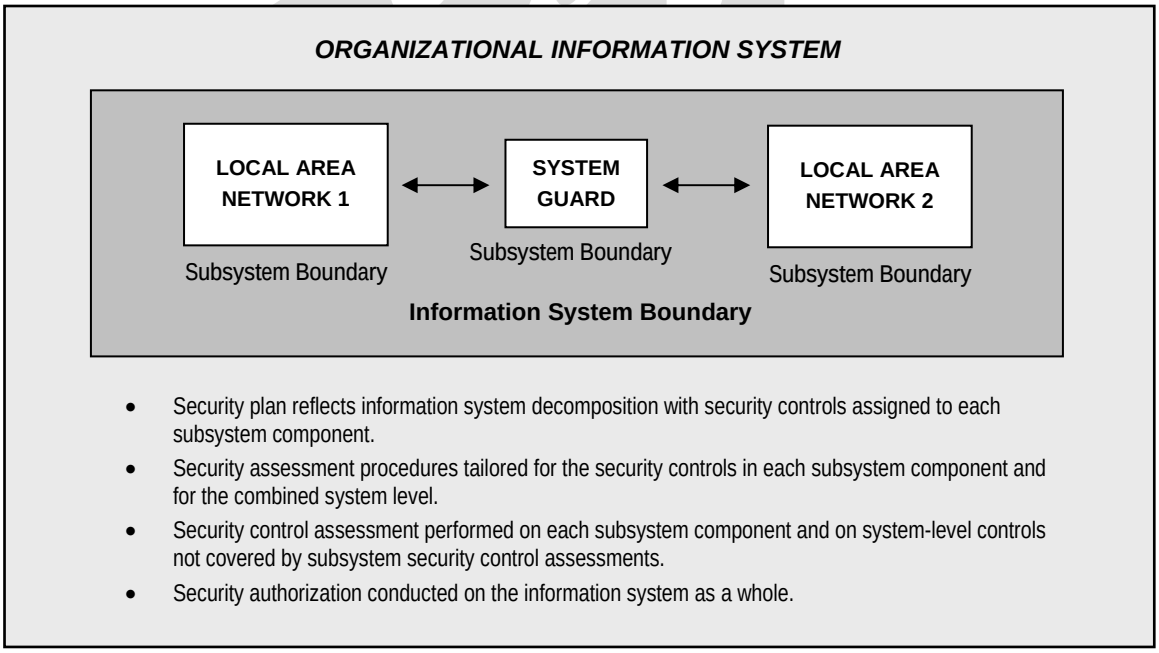

FIGURE 2: DECOMPOSITION OF LARGE AND COMPLEX SYSTEMS

[44] Tightly coupled subsystem components may introduce inadvertent weak links in a large and complex information system. For example, if a large organizational intranet is decomposed by enterprise services into smaller subsystems (e.g., severable components such as local area network (LAN) segments), then categorized individually, the specific protections at the subsystem level may allow a vector of attack against the intranet by requiring controls commensurate with a lower categorization level, than the rest of the system. To avoid this situation, organizations are encouraged to carefully examine the potential interfaces among subsystem components and to take appropriate actions to eliminate potential vulnerabilities in this area, thus, helping to ensure that the information system is adequately protected. .

In the above example, an information system contains a system guard that monitors the flow of information between two local area networks. The information system, in this case, can be partitioned into three subsystem components: (i) local area network one; (ii) local area network two; and (iii) the system guard separating the two networks. Each subsystem component within the information system can be assigned a security category in accordance with FIPS 199 or CNSS Instruction 1199. The overall categorization of the information system is determined by taking the high water mark of the security categorizations of the individual subsystem components. When all subsystems within the information system have completed the security control assessment, an additional assessment is performed on the system-level security controls not covered by the individual subsystem assessments, and the results are bundled together into the authorization package and presented as evidence to the authorizing official.

2.5 SECURITY CONTROL INHERITANCE

Authorizing officials and information system owners are becoming increasingly dependent on security controls provided by organizational entities that are outside of their authorization boundaries (e.g., organizational networks, facilities management office, human resources office, shared/external service providers). These security controls, often referred to as *common controls*, are typically not under the direct control of the information system owners and authorizing officials whose systems *inherit* those controls.[45] Common controls can be provided by an information system owner and documented in a security plan[46] or provided by organizational entities other than information system owners (e.g., physical security controls provided by the facilities management office, personnel security controls provided by the human resources office).[47] Common controls provided by entities other than information system owners can be documented in a security plan or equivalent document. Common controls can help facilitate more consistent and cost-effective security across the organization because the controls are deployed once and used by many information systems throughout the organization—thereby amortizing security control costs across a broad base of customers.

The identification of common controls should be an organization-wide activity including when the controls are provided by entities outside of the organization (e.g., external or shared service providers).[48] Common controls should be assigned to responsible entities (designated as common control providers) for planning, development, implementation, assessment, authorization, and maintenance. In addition, an appropriate official within the organization (or multiple officials in some cases) should be assigned authorization responsibility for the effective deployment of

[45] Security controls can be either *system-specific* (i.e., controls implemented within an information system), *common* (i.e., controls inherited by an information system), or *hybrid* (i.e., controls that have both system-specific and common control characteristics).

[46] Common controls that are employed in common information systems, subsystems, or applications are sometimes associated with the term *type authorization*.

[47] When common controls are provided by entities other than information system owners and those entities are under the jurisdiction of other controlling federal legislation, policies, directives, regulations, or standards (e.g., personnel security policies promulgated by the Office of Personnel Management), system owners, in coordination with appropriate organizational officials, should ensure that necessary evidence is obtained from common control providers to determine overall control effectiveness.

[48] When common controls are provided by entities external to the organization (e.g., from shared/external service providers), the organization should take appropriate actions to manage, track, and maintain those controls. This includes, as a minimum, assigning responsibility to organizational officials to ensure that the common controls provided by external entities have been developed, implemented, and assessed for effectiveness and that any risks associated with the inheritance of those controls is adequately mitigated in accordance with the organization's overall protect strategy.

common controls inherited by information system owners. The objective of the organization is to have *accountability* for every security control supporting the information security program. Common controls should be managed at the organizational level to ensure that all common control-related information (e.g., security plan or equivalent document, security assessment report, and plan of action and milestones) is available to information system owners and authorizing officials whose systems depend on those inherited controls.[49] Figure 3 illustrates the concept of security control inheritance based on the employment of common controls. The security plan, security assessment report, and plan of action and milestones are key documents used by authorizing officials in making risk-based authorization decisions that are affected by the deployment and inheritance of common controls.[50]

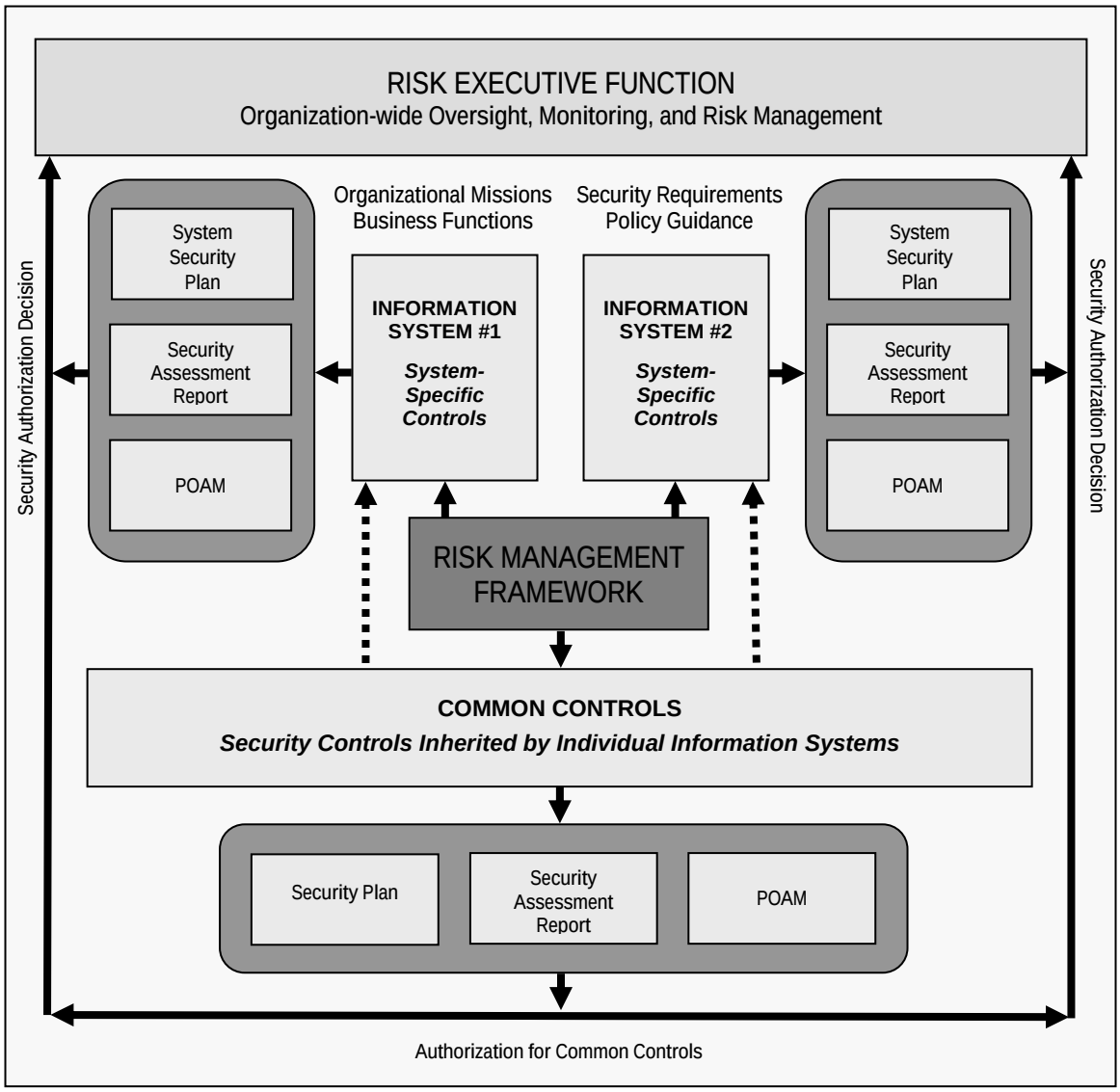

FIGURE 3: SECURITY CONTROL INHERITANCE

[49] Common controls should be listed or referenced in the security plans for information systems. Hybrid controls should also be listed in the security plans for information systems and in the applicable security plans (or equivalent documents) for common controls and managed in accordance with organizational policies and procedures.

[50] The security plan, security assessment report, and plan of action and milestones are described in Section 2.6.

2.6 AUTHORIZATION PACKAGE

The security *authorization package* documents the results of the security control assessment and provides the authorizing official with essential information needed to make a credible, risk-based decision on whether to authorize operation of an information system. Unless specifically designated otherwise by the chief information officer or authorizing official, the information system owner is responsible for the assembly, compilation, and submission of the authorization package. The information system owner receives inputs from the information system security officer, security control assessor, senior agency information security officer, and risk executive (function) during the preparation of the authorization package. The authorization package[51] contains the following documents:

- Security plan;
- Security assessment report; and
- Plan of action and milestones.

The *security plan*, prepared by the information system owner or common control provider, provides an overview of the security requirements and describes the security controls in place or planned for meeting those requirements. The plan provides sufficient information to understand the intended expression of each security control in the context of the information system, or for a common control, the organization.[52] The security plan also contains as supporting appendices or as references to appropriate sources, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. In accordance with the *near real-time* risk management objectives of the security authorization process, the security plan should be updated whenever events dictate changes to the agreed-upon security controls for the information system. This type of update to the security plan may be triggered by a variety of events, for example: (i) a vulnerability scan of the information system; (ii) new threat information; (iii) weaknesses or deficiencies discovered in currently deployed security controls after an information system breach; (iv) a redefinition of mission priorities or business objectives resulting in a change to the security category of the information system; and (v) a change in the information system (e.g., adding new hardware, software, or firmware; establishing new connections) or the system's environment of operation.

The *security assessment report*, prepared by the security control assessor, provides the results of assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements. The findings documented in the security assessment report represent the results of carrying out specified assessment procedures for the security controls described in the security plan and implemented in the information system. The security assessment report should also contain a list of recommended corrective actions for weaknesses or deficiencies identified in the security controls. Also supporting the near real-time risk management objectives of the security authorization process, security assessment reports are updated on an ongoing basis whenever changes are made to either the

[51] The authorizing official determines what additional supporting documentation or references may be required to be included in the security authorization package. Appropriate measures should be employed to protect the information contained in security authorization packages in accordance with federal and organizational policy.

[52] The *security plan* is a conceptual body of information which may be accounted for within one or more repositories and include documents (electronic or hard copy) that come from a variety of sources produced throughout the system development life cycle.

security controls in the information system or the common controls inherited by those systems. Updates to the security assessment reports, as needed, help to ensure that information system owners and authorizing officials maintain *situational awareness* with regard to security control effectiveness. It is this effectiveness that directly affects risk mitigation activities and the ultimate security state of the information system and explicit acceptance of risk.

The *plan of action and milestones*, prepared by the information system owner, describes the specific measures that are planned: (i) to correct weaknesses or deficiencies noted in the security controls during the security control assessment; and (ii) to address known vulnerabilities in the information system.[53] The most effective plans of action and milestones contain a robust set of actual and potential weaknesses or deficiencies identified in the security controls deployed in the information system or inherited by the system. Assuming most information systems have more vulnerabilities than available resources can address, organizations should define a strategy for developing plans of action and milestones that facilitates a prioritized approach to risk mitigation that is consistent across the organization. This strategy helps to ensure that plans of action and milestones are based on:

- The security category of the information system;[54]
- The specific weaknesses or deficiencies in the information system security controls;
- The importance of the identified security control weaknesses or deficiencies (i.e., the direct or indirect effect the weaknesses or deficiencies may have on the overall security state of the information system and hence on the risk exposure[55] of the organization);
- The organization's proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g., prioritization of risk mitigation actions, allocation of risk mitigation resources); and
- The organization's rationale for accepting certain weaknesses or deficiencies in the security controls.[56]

Organizational strategies for plans of action and milestones should be guided by the security categories of the respective information systems affected by the risk mitigation activities. Organizations may decide, for example, to allocate the vast majority of risk mitigation resources initially to the *highest impact* information systems because a failure to correct the weaknesses or deficiencies in those systems could potentially have the most significant adverse effects on the organization's missions or business operations. Organizations should also prioritize weaknesses or deficiencies within the categorized information systems. Thus, a high-impact system would have a prioritized list of weaknesses or deficiencies for that system, as would moderate-impact and low-impact systems. In general, the plan of action and milestones strategy should always address the highest priority weaknesses or deficiencies within those prioritized systems.

[53] Organizations may choose to document the specific measures *implemented* to correct weaknesses or deficiencies in security controls in the plan of action and milestones, thereby providing an historical record of actions completed.

[54] FIPS 199 and CNSS Instruction 1199 provide guidance for security categorization of information systems. NIST Special Publication 800-53 and CNSS Instruction 1253 provide guidance on determining information system impact levels derived from the information system categorization process.

[55] In general, risk exposure is the degree to which an organization is threatened by the potential adverse effects on organizational operations and assets, individuals, other organizations, or the Nation.

[56] Organizations should document their rationale for accepting security control weakness or deficiencies.

After completion of the security plan, security assessment report, and plan of action and milestones, the system owner submits the final authorization package to the authorizing official or designated representative. Figure 4 illustrates the key sections of the authorization package.

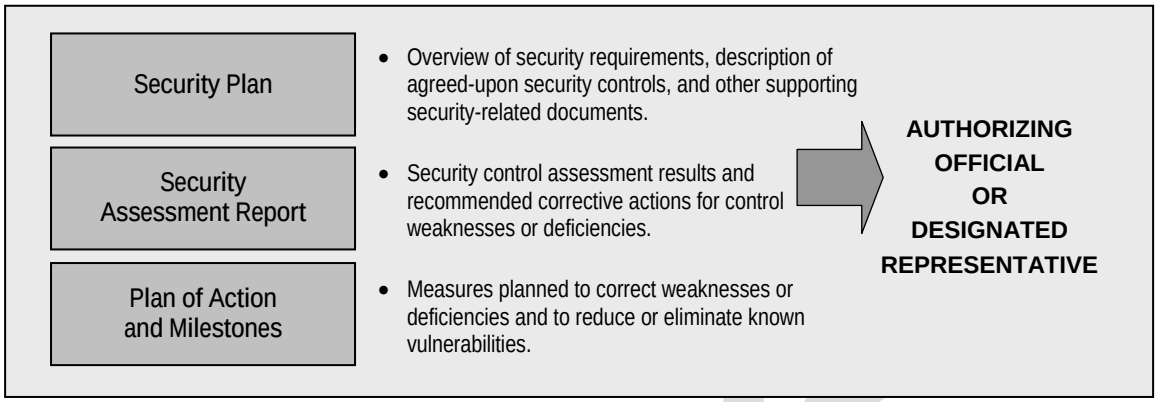

FIGURE 4: CONTENTS OF THE SECURITY AUTHORIZATION PACKAGE

2.7 AUTHORIZATION DECISIONS

Security authorization decisions should be based on the content of the authorization package submitted by the information system owner and any inputs received from the organization's risk executive (function). The security authorization package provides detailed and comprehensive information on the security state of the information system. Risk executive (function) inputs, including previously established overarching risk guidance to authorizing officials, provide additional organization-wide information to the authorizing official that may be relevant and affect the authorization decision (e.g., organizational risk tolerance, organization's overall risk mitigation strategy, specific organization-wide mission and business requirements, dependencies among information systems, and other types of risks not directly associated with the information system). Risk executive (function) inputs are documented and become part of the security authorization decision.

Security authorization decisions, including inputs from the organization's risk executive (function), should be conveyed to information system owners and made available to interested parties within the organization (e.g., information system owners and authorizing officials for interconnected systems, chief information officers, , information owners/stewards, senior managers). To ensure that the organization's mission, business, and operational needs are fully considered, the authorizing official should meet with the information system owner prior to issuing the authorization decision to discuss the assessment results, the terms and conditions of the authorization, and any other factors affecting the organization at large. There are two types of authorization decisions that can be rendered by authorizing officials:

- Authorization to operate; and
- Denial of authorization to operate.

2.7.1 Authorization to Operate

If the authorizing official, after reviewing the information provided in the authorization package, deems that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable, an *authorization to operate* is issued for the information system.[57] The information system is authorized to operate for a specified time period in accordance with the terms and conditions established by the authorizing official. An *authorization termination date* is also established by the authorizing official as a condition of authorization. The authorization termination date can be adjusted by the authorizing official to reflect an increased level of concern regarding the security state of the information system.[58] Authorization termination dates should not exceed the maximum allowable time periods for authorization established by federal or organizational policy.

The authorizing official should take specific actions to reduce or eliminate vulnerabilities in the information system unless the vulnerabilities have been explicitly accepted as part of the risk-based authorization decision. In addition, the information system owner should establish a disciplined, structured, and repeatable process to monitor the ongoing effectiveness of the deployed security controls and the progress of any actions taken to correct or eliminate weaknesses or deficiencies. The plan of action and milestones submitted by the information system owner is used by the authorizing official to monitor the progress in correcting deficiencies and weaknesses noted during the security control assessment.

2.7.2 Denial of Authorization to Operate

If the authorizing official, after reviewing the information provided in the authorization package, deems that the risk to organizational operations and assets, individuals, other organizations, and the Nation is unacceptable and immediate steps cannot be taken to reduce the risk to an acceptable level, a *denial of authorization to operate* is issued for the information system. The information system is not authorized to operate and should not be placed into operation. If the information system is currently in operation, all activity should be halted. Failure to receive an authorization to operate indicates that there are major deficiencies in the security controls required for the information system. The authorizing official or designated representative should work with the information system owner to revise the plan of action and milestones to ensure that proactive measures are taken to correct the identified deficiencies and weaknesses in the system.

A special case of a denial of authorization to operate is an *authorization rescission*. Authorizing officials can rescind a previous authorization decision at any time in situations where there is a specific violation of: (i) federal/organizational security policies, directives, regulations, standards, guidance, or practices; or (ii) the terms and conditions of the original authorization. For example, failure to maintain an effective continuous monitoring program may be grounds for rescinding an authorization decision. Authorization officials should consult with the senior agency information security officer and the risk executive (function) before rescinding security authorizations.

---

[57] An *interim authorization to test* is a special type of authorization decision allowing an information system to operate in an operational environment for the express purpose of testing the system or with live data for a specified time period. An interim authorization to test is granted by an authorizing official only when the actual operational environment or live data is required to complete specific test objectives. The information system is not to be used for operational purposes during the temporary authorization period. All security controls specified for employment in the information system should be assessed for effectiveness prior to testing the system in the operational environment or with live data except for those controls that can only be assessed in an operational environment.

[58] Some organizations may choose to use the term *interim authorization to operate* to focus attention on the increased risk being accepted by the authorizing official in situations where there are significant weaknesses or deficiencies in the information system, but an overarching mission necessity to place the system into operation or continue its operation.

2.7.3 Authorization Decision Document

The *authorization decision document* transmits the final security authorization decision from the authorizing official to the information system owner and other key organizational officials, as appropriate. The authorization decision document contains the following information:

- Authorization decision;
- Terms and conditions for the authorization; and
- Authorization termination date.

The security *authorization decision* indicates to the information system owner whether the system is: (i) authorized to operate; or (ii) not authorized to operate. The *terms and conditions* for the authorization provide a description of any limitations or restrictions placed on the operation of the information system that must be followed by the system owner. The *authorization termination date*, established by the authorizing official, indicates when the security authorization expires and reauthorization is required (see Section 2.7.4). An authorizing official designated representative can prepare the authorization decision document for the authorizing official with authorization recommendations, as appropriate. The authorization decision document is attached to the original security authorization package containing the supporting documentation and transmitted to the information system owner.

Upon receipt of the authorization decision document and authorization package, the information system owner accepts the terms and conditions of the authorization. The information system owner keeps the original authorization decision document and authorization package on file. The authorizing official and senior agency information security officer also retain copies of the authorization decision document and authorization package. The contents of the organization's authorization documentation, especially information regarding information system vulnerabilities, should be: (i) marked and appropriately protected in accordance with federal and organizational policy;[59] and (ii) retained in accordance with the organization's record retention policy.

2.7.4 Reauthorization Actions

A robust and comprehensive continuous monitoring[60] strategy integrated in the ongoing SDLC processes carried out by an organization can significantly reduce the resources required for reauthorizing information systems. Risk management can become near real-time with continuous security control monitoring using automated support tools. When continuous monitoring is conducted in accordance with the information needs of the authorizing official, that monitoring results in the information authorizing officials need to determine the current security state of the information system, the resulting risks, and whether to authorize continued operation of the system. This also amortizes the resource expenditures for reauthorization activities over the authorization period. The goal is *ongoing authorization* where the authorizing official maintains sufficient knowledge of the current security state of the information system to determine whether continued operation is acceptable, and if not, which step of the RMF needs to be executed in order to adequately mitigate the risk.

Reauthorization occurs at the discretion of the authorizing official in accordance with federal or organizational policy. Reauthorization actions are either *time-driven* or *event-driven*. Time-driven reauthorizations occur when the authorization termination date is reached. Authorization

[59] Authorization decision documents may be digitally signed to ensure authenticity.

[60] Continuous monitoring is described in Section 2.9.

termination dates are influenced by federal and/or organizational policies and by the requirements of authorizing officials which may establish maximum authorization periods. For example, if the maximum authorization period for an information system is three years, then an organization establishes a continuous monitoring strategy for assessing a subset of the security controls employed in the system (i.e., conducting partial assessments) during the authorization period such that all security controls designated in the security plan are assessed at least one time by the end of the three-year period. If the security control assessments are conducted by assessors with the required degree of *independence* based on federal and/or organizational policies, federal information security standards and guidelines, and the needs of the authorizing official, the assessment results can be cumulatively applied to the information system reauthorization.[61] Thus, the reauthorization action can be as simple as updating key documents in the security authorization package (i.e., the *security plan*, *security assessment report*, and *plan of action and milestones*). The authorizing official subsequently signs an updated authorization decision document based on the current determination and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation.[62]

Event-driven reauthorizations occur when there is a significant change[63] to an information system or its environment of operation. Most, if not all routine changes to an information system or its environment of operation (unless the system is undergoing a major upgrade) can be handled by the organization's continuous monitoring program. An effective continuous monitoring program, therefore, can significantly reduce reauthorization actions due to changes in information systems or environments of operation. In the event that there is a change in authorizing officials for the information system, the new authorizing official should review the current authorization decision document and associated authorization package (i.e., *security plan*, *security assessment report*, and *plan of actions and milestones*) and any updated documents created as a result of the continuous monitoring process. If the new authorizing official is willing to accept the currently documented information system-related security risk, then the official signs a new authorization decision document, thus formally transferring responsibility and accountability for the security of the information system and explicitly accepting the risk to organizational operations and assets, individuals, other organizations, and the Nation.[64] If the new authorizing official is not willing to accept the previous security authorization, a *reauthorization* action may need to be initiated or the new authorizing official may establish new terms and conditions for continuing operation of the information system, but not extend the original authorization termination date. In all situations where there is a decision to reauthorize an information system, the maximum reuse of security authorization information is strongly encouraged to minimize the time and expense associated with the reauthorization effort.

[61] The specific conditions under which security-related information can be effectively reused in security authorization and reauthorization activities is described in NIST Special Publication 800-53A and CNSS Instruction 1253A.

[62] Reauthorization decisions include inputs from the risk executive (function) and senior agency information security officer.

[63] Examples of significant changes to an information system that should be reviewed for possible reauthorization include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reauthorization action. Reauthorization should be avoided in situations where the continuous monitoring process provides the necessary and sufficient information to authorizing officials to manage the potential risk arising from the information system changes.

[64] Reauthorization decisions can be based on a variety of factors, for example, the acceptability of the previous authorization information provided in the authorization package, the length of time since the previous authorization decision, the new authorizing official's risk tolerance, and current organizational requirements and priorities.

2.8 OPERATIONAL SCENARIOS

Conducting security authorizations in modern computing environments with a diverse set of potential business relationships can be challenging for organizations. Relationships are established and maintained in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency and intra-agency agreements, lines of business arrangements), licensing agreements, and supply chain exchanges (i.e., supply chain collaborations or partnerships). Security authorization requirements apply only to federal information systems.[65] There are two distinct types of operational scenarios that affect how organizations address security authorizations:

- Information systems used/operated by federal agencies and their subordinate organizations; and
- Information systems used/operated by other organizations on behalf of federal agencies and their subordinate organizations.

For an information system that is used or operated by a *federal agency or one of its subordinate organizations*, the security authorization boundary is defined by the agency or the appropriate subordinate organization of the agency. The appropriate organization conducts all steps in the RMF to include issuing the authorization decision. The agency or its appropriate subordinate organization maintains complete control over the security controls employed within the information system to protect organizational missions and business functions. For an information system that is used or operated by *another organization*[66] on behalf of a federal agency or one of its subordinate organizations, the security authorization boundary is defined by the agency or its appropriate subordinate organization in consultation with the organization.

- If the organization is contracted to a federal agency or one of its subordinate organizations, the contractor can conduct all security authorization tasks except those tasks which must be carried out by the federal agency or its appropriate subordinate organization as part of the agency's inherent governmental responsibilities.[67] The contractor provides appropriate evidence in the security authorization package for the authorization decision by the federal agency or its appropriate subordinate organization. The agency or its appropriate subordinate organization provides authorization-related inputs to the contractor, as needed, and maintains oversight on all contractor-executed steps in the RMF.
- If the organization is a federal agency or one of its subordinate organizations, the organization can conduct all steps in the RMF to include the information system authorization step and authorization decision. The security authorization decision can also be a joint authorization decision if both parties agree to share the authorization responsibilities. Accordingly, each organization participating in the joint authorization is responsible for implementing and assessing the security controls that are directly under their purview. In situations where a federal agency or one of its subordinate organizations uses or operates an information system on behalf of multiple federal agencies or their subordinate organizations, the joint authorization can include all participating agencies and organizations.

[65] A *federal information system* is defined as an information system used or operated by a federal agency, by a contractor of a federal agency, or by another organization on behalf of a federal agency.

[66] Organizations that use or operate an information system on behalf of a federal agency or one of its subordinate organizations can include, for example, other federal agencies or their subordinate organizations, state and local government agencies, and academic institutions.

[67] Organizations should ensure that requirements for conducting the specific steps in the RMF are included in appropriate contractual vehicles, including requirements for independent assessments, when appropriate.

2.9 CONTINUOUS MONITORING

A critical aspect of the security authorization process is the post-authorization period involving the continuous monitoring of an information system's security controls (including common controls). Conducting a thorough point-in-time assessment of the security controls in an organizational information system is a necessary but not sufficient condition to demonstrate security due diligence. Effective information security programs should also include a continuous monitoring program integrated with SDLC processes to check the status of subsets of the security controls in an information system on an ongoing basis. The ultimate objective of the continuous monitoring program 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. Continuous monitoring is a proven technique to address the security impacts on information systems resulting from changes to the hardware, software, firmware, or operational environment. A well-designed and well-managed continuous monitoring program 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-related information to appropriate organizational officials in order to take appropriate risk mitigation actions and make credible, risk-based decisions regarding the operation of the information system. Continuous monitoring programs provide organizations with an effective mechanism to update *security plans*, *security assessment reports*, and *plans of action and milestones*.

2.9.1 Monitoring Strategy

Organizations should develop a strategy and implement a program for the continuous monitoring of security control effectiveness taking into account any proposed/actual changes to the information system or its environment of operation. The monitoring program should be integrated into the organization's SDLC processes. A robust continuous monitoring program requires the active involvement of information system owners and common control providers, chief information officers, senior agency information security officers, and authorizing officials. The monitoring program allows an organization to: (i) track the security state of an information system on a continuous basis; and (ii) maintain the security authorization for the system over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and represents a significant paradigm shift in the way security authorization activities have been employed in the past.[68] An effective continuous monitoring program includes:

- Configuration management and control processes for information systems;
- Security impact analyses on actual or proposed changes to information systems and environments of operation;
- Assessment of selected security controls based on continuous monitoring strategy;

[68] Near real-time risk management of information systems can be facilitated by employing automated support tools to execute various steps in the RMF including authorization-related activities. In addition to vulnerability scanning tools, system and network monitoring tools, and other automated support tools that can help to determine the security state of an information system, organizations can employ automated security management and reporting tools to update critical documents in the authorization package including the security plan, security assessment report, and plan of action and milestones. The documents in the authorization package should be considered "living documents" and updated accordingly based on actual events that may affect the security of the information system. Transitioning to a near real-time risk management environment will require the increased use of automated support tools over time as organizations integrate these technologies into their information security programs in accordance with available resources.

- Security status reporting to appropriate organizational officials;[69] and
- Active involvement by authorizing officials in the ongoing management of information system-related security risks.

With regard to configuration management and control, it is important to document the proposed or actual changes to the information system or its environment of operation and to subsequently determine the impact of those proposed or actual changes on the overall security state of the system. Information systems will typically be in a constant state of change with upgrades to hardware, software, or firmware and possible modifications to the surrounding environments where the systems reside. Documenting information system changes as part of routine SDLC processes and assessing the potential impact those changes may have on the security state of the system is an essential aspect of continuous monitoring, achieving situational awareness, maintaining the authorization, and supporting a decision for reauthorization when appropriate.

2.9.2 Selection of Security Controls for Monitoring

The criteria for selecting which security controls to monitor and for determining the frequency of such monitoring should be established by the information system owner or common control provider in collaboration with the authorizing official or designated representative, chief information officer, senior agency information security officer, and risk executive (function). The criteria should reflect the organization's priorities and importance of the information system (or in the case of common controls, the information systems inheriting the controls) to organizational operations and assets, individuals, other organizations, and the Nation in accordance with FIPS 199 or CNSS Instruction 1199. Organizations should use recent risk assessments, results of previous security assessments, and operational requirements in guiding the selection of security controls to be monitored and the frequency of the monitoring process.

Priority for control monitoring should be given to the security controls that have the greatest volatility (i.e., greatest potential for change) after implementation and the controls that have been identified in the organization's plan of action and milestones for the information system. Security control volatility is a measure of how frequently a control is likely to change over time after implementation. For example, security policies and implementing procedures in a particular organization may not be likely to change from one year to the next and thus would likely be security controls with lower volatility. Access control mechanisms or other technical controls that are subject to the direct effects or side effects of frequent changes in hardware, software, and/or firmware components of an information system would, therefore, likely be security controls with higher volatility.

Organizations usually apply greater resources to security controls deemed to be of higher volatility as there is typically a higher return on investment for assessing security controls of this type. Security controls identified in the plan of action and milestones should also be a priority in the continuous monitoring process, due to the fact that these controls have been deemed to be ineffective to some degree (or nonexistent, in the worst case). Those security controls that are the most volatile, critical to certain aspects of the organization's protection strategy, or identified in current plans of action and milestones documents are assessed at least annually. All other

[69] Organizations have significant latitude and flexibility in the breadth, depth, and formality of security status reports. At a minimum, security status reports should describe or summarize key changes to security plans, security assessment reports, and plans of action and milestones. At the discretion of the organization, security status reports on information systems can be used to help satisfy the FISMA reporting requirement for documenting remedial actions on any security-related weaknesses or deficiencies.

controls are assessed at least once during the information system's routine authorization cycle in accordance with federal or organizational policies. The authorizing official and the senior agency information security officer should approve the set of security controls that are to be monitored on a continuous basis as well as the frequency of the monitoring activities.

2.9.3 Critical Updates and Status Reporting

Continuous monitoring results should be considered with respect to any necessary updates to the security plan, security assessment report, and plan of action and milestones, since these documents are used to guide future security authorization activities. Updated security plans should reflect any modifications to security controls based on risk mitigation activities carried out by information system owners or common control providers. Updated security assessment reports should reflect additional assessment activities carried out to determine security control effectiveness based on modifications to the security plan and deployed controls. Updated plans of action and milestones should: (i) report progress made on the current outstanding items listed in the plan; (ii) address vulnerabilities in the information system discovered during the security impact analysis or security control monitoring; and (iii) describe how the information system owner or common control provider intends to address those vulnerabilities.

The results of continuous monitoring should be reported to the authorizing officials and senior agency information security officers on a regular basis. With the use of automated support tools and effective organization-wide security program management practices, authorizing officials should be able to access the most recent documentation in the authorization package at any time to determine the current security state of the information system, to help manage risk, and to provide essential information for reauthorization decisions. The monitoring of security controls continues throughout the SDLC.

In summary, organizations must make informed judgments regarding the application of limited assessment resources when conducting continuous monitoring activities to ensure that the expenditures are consistent with the organization's mission requirements, security categorization in accordance with FIPS 199 or CNSS Instruction 1199, and assessment requirements articulated in federal legislation, policy, directives, and regulations. As the security authorization process becomes more dynamic in nature, relying to a greater degree on the continuous monitoring aspects of the process as an integrated and tightly coupled part of the SDLC, the ability to update the security assessment report frequently based on the assessment results obtained from the continuous monitoring process becomes a critical aspect of an organization's information security program. It is important to emphasize the relationship among the three key documents in the authorization package (i.e., the security plan including the organizational assessment of risk, the security assessment report, and the plan of action and milestones). It is these documents that provide the best indication of the overall security state of the information system and the ability of the system to protect, to the degree necessary, the organization's operations and assets, individuals, other organizations, and the Nation.

CHAPTER THREE

THE PROCESS

PHASES AND TASKS ASSOCIATED WITH SECURITY AUTHORIZATION

This chapter describes the security authorization process as an integral part of the Risk Management Framework (RMF). The security authorization process consists of three phases: (i) the preparation phase; (ii) the execution phase; and (iii) the maintenance phase. The authorization *preparation phase* consists of the first four steps in the RMF (i.e., categorize information system, select security controls, implement security controls, and assess security controls). The authorization *execution phase* consists of the fifth step in the RMF (i.e., authorize information system). The authorization *maintenance phase* consists of the sixth step in the RMF (i.e., monitor security controls). Each phase in the authorization process employs a set of well-defined tasks that are to be carried out by selected individuals within the organization or external to the organization (e.g., authorizing official, authorizing official designated representative, chief information officer, risk executive (function), senior agency information security officer, information owner/steward, information system owner or common control provider, information system security officer, and security control assessor). Each task description includes the individual, group, or function with primary responsibility for carrying out the task, supporting roles, SDLC phase, implementing guidance, and appropriate references for national security and nonnational security systems. Figure 5 provides a high-level overview of the security authorization process including the RMF steps associated with each phase in the process.[70]

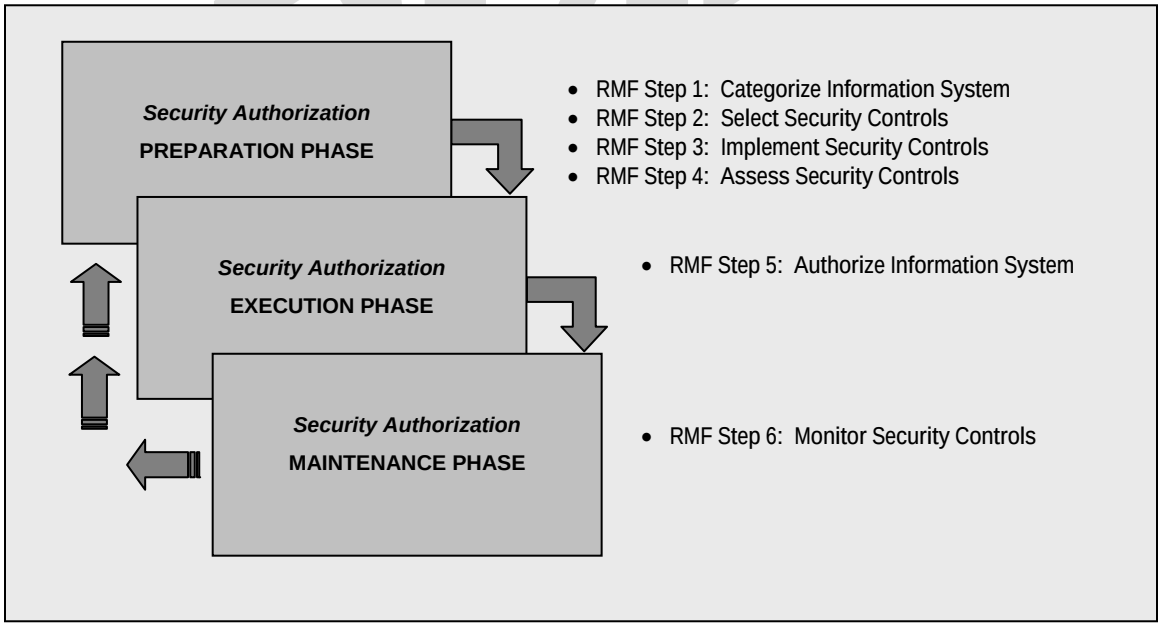

FIGURE 5: SECURITY AUTHORIZATION PROCESS

[70] The security authorization process expressed in this publication can be tailored to meet the needs of many diverse communities of interest (e.g., Civil, Defense, or Intelligence Communities). Tailoring provides flexibility in applying a level of effort and rigor that is most suitable for the information system undergoing authorization.

The following security authorization tasks can be applied at appropriate phases in the SDLC. While the tasks appear in sequential order, there can be many points in the authorization process that are cyclic in nature. For example, the results from security control assessments (i.e., findings and recommendations from security control assessors) can trigger remediation actions on the part of an information system owner, which in turn can require the reassessment of selected controls. Monitoring the security controls in an information system can also generate a potential cycle of tracking changes to the system and its environment of operation, conducting security impact analyses, taking remediation actions, reassessing security controls, and reporting the security status of the system. Process and execution (i.e., the order and manner in which the tasks occur, the names of security authorization roles, the names and format of artifacts) may vary depending on the community of interest or organization. The level of effort and resources expended for security authorization activities or actions should be commensurate with the *security category* of the information system.[71] A summary table of all security authorization tasks and the individuals with the primary responsibility for accomplishing those tasks is provided in Appendix D. The legend below provides a brief explanation of the various elements of the authorization tasks included in Chapter 3.

LEGEND

Task: This section describes the specific security authorization task within the appropriate security authorization phase and step in the Risk Management Framework.

Primary Responsibility: This section lists the individual or group within the organization having primary responsibility for executing the security authorization task.

Supporting Roles: This section lists the supporting roles within the organization that may be necessary to help the individual or group with primary responsibility for executing the security authorization task.

SDLC Phase: This section lists the particular phase of the SDLC when the security authorization task is typically executed.

Guidance: This section provides supplemental guidance for executing the security authorization task including additional information from relevant supporting security policies, instructions, standards, and guidelines.

References: This section provides general references to NIST security standards and guidelines that should be consulted for additional information with regard to executing the security authorization task.

NSS References: This section provides specific national security system references to CNSS policies and instructions that should be consulted for additional information with regard to executing the security authorization task when the general references are either insufficient or inappropriate for national security application.

[71] FIPS 199 and CNSS Instruction 1199 provide guidance for security categorization of information systems. NIST Special Publication 800-53 and CNSS Instruction 1253 provide guidance on determining information system impact levels derived from the information system categorization process.

3.1 PREPARING FOR THE AUTHORIZATION *(PREPARATION PHASE)*

The organization prepares for security authorization by completing the following RMF steps and associated tasks in the security authorization *preparation phase*.

Step 1 Categorize Information System

SYSTEM DESCRIPTION

Task 1: Describe the information system (including system boundary) and document the description in the security plan.

Primary Responsibility: Information System Owner.

Supporting Roles: Authorizing Official or Designated Representative; Senior Agency Information Security Officer; Information Owner/Steward; Information System Security Officer.

SDLC Phase: System Initiation (requirements definition).

Guidance: Descriptive information about the information system is typically documented in the *system identification* section of the security plan, included in attachments to the plan or referenced in other standard sources for the information generated as part of the SDLC. System identification information can also be provided by reference. The level of detail provided in the security plan is determined by the organization and is typically commensurate with the security category of the information system in accordance with FIPS 199 or CNSS Instruction 1199 (i.e., the level of detail in the plan increases as the potential impact on organizational operations and assets, individuals, other organizations, and the Nation increases). Information may be added to the information system description as it becomes available during the security authorization process. A typical system description may include, for example:

- unique system identifier (typically a number or code);
- system owner including contact information;
- parent or governing organization that manages, owns, and/or controls the system;
- full descriptive name of the system including associated acronym;
- location of the system and physical environment in which the system operates;
- system version or release number;
- system description including the purpose, functions, and capabilities;
- status of the system with respect to acquisition and/or system development life cycle;
- security category of the system;
- types of information processed, stored, and transmitted;
- boundary of the system for security authorization purposes;
- applicable laws, directives, policies, regulations, or standards affecting the security of the system;
- architectural description of the system including network topology;
- hardware and firmware devices (including wireless);
- system and applications software (including mobile code);
- hardware, software, and system interfaces (internal and external);
- information flows (i.e., inputs and outputs);
- network connection rules for communicating with external information systems;
- interconnected information systems and identifiers for those systems;
- encryption techniques used for information processing, transmission, and storage;
- public key infrastructures, certificate authorities, and certificate practice statements;
- system users (including organizational affiliations, access rights, privileges, citizenship, if applicable);
- system operation (e.g., government owned, government operated; government owned, contractor operated; contractor owned, contractor operated; nonfederal (state and local governments, grantees);
- security authorization date and authorization termination date (provided upon authorization completion);
- security authorization process roles (see Section 2.3); and
- other information as required by the organization.

References: NIST Special Publication 800-18.

NSS References: None.

SYSTEM REGISTRATION

Task 2: Register the information system with appropriate organizational program/management offices.

Primary Responsibility: Information System Owner.

Supporting Roles: Information System Security Officer.

SDLC Phase: System Initiation (requirements definition).

Guidance: The *registration* process begins by identifying the information system in the system inventory and establishes a relationship between the information system undergoing security authorization and the parent or governing organization that owns, manages, and/or controls the system. Registration, either formal or informal in accordance with organizational policy, uses information in the system identification section of the security plan to inform the parent or governing organization of: (i) the existence of the information system; (ii) the key characteristics of the system; and (iii) any security implications for the organization due to the ongoing operation of the system. Information system registration provides organizations with an effective management and tracking tool that is necessary for security status reporting in accordance with the requirements of FISMA and OMB policy.

References: NIST Special Publication 800-18.

NSS References: None.

SECURITY CATEGORIZATION

Task 3: Determine the security category for the information system and document the category in the security plan.

Primary Responsibility: Information System Owner.

Supporting Roles: Authorizing Official ***or*** Designated Representative; Chief Information Officer; Senior Agency Information Security Officer; Risk Executive (Function); Information Owner/Steward.

SDLC Phase: System Initiation (requirements definition).

Guidance: The security category of an information system should be determined in consultation with appropriate organizational officials (typically at the senior leadership level) with mission/business-related and risk management responsibilities. If possible, the security categorization process should be undertaken as an organization-wide activity and integrated into the Enterprise Architecture. This helps to ensure that individual information systems are categorized at the appropriate impact level in accordance with the mission and business objectives of the organization. The risk executive (function) provides guidance and relevant information for authorizing officials concerning organizational risk tolerance, known existing aggregated risks from current information systems, and other sources of risk. Security categorization determinations consider potential adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation.

It is recognized that an information system may contain more than one type of information, each of which is subject to security categorization. The security category of an information system that processes, stores, or transmits multiple types of information should be at least the highest impact level that has been determined for each type of information for each security objective of confidentiality, integrity, and availability. The security category for the information system guides the selection of security controls for the system. Security categorization information is typically documented in the system identification section of the security plan or included as an attachment to the plan.

References: FIPS 199; NIST Special Publication 800-60.

NSS References: CNSS Instruction 1199.

Step 2 Select Security Controls

COMMON CONTROL SELECTION

Task 1a: Identify the common controls inherited by information systems within the organization and document the controls in a security plan (or equivalent document).

Primary Responsibility: Chief Information Officer ***or*** Senior Agency Information Security Officer.

Supporting Roles: Common Control Provider(s); Information System Security Engineer; Authorizing Official or Designated Representative.

SDLC Phase: System Initiation (requirements definition).[72]

Guidance: Common controls should be identified by the organization and assigned to specific organizational entities (designated as common control providers) for planning, development, implementation, assessment, and maintenance. In addition to common control providers, a senior official or executive within the organization (or multiple officials/executives in some cases) should be assigned responsibility and be accountable for accepting the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the deployment of common controls that are less than effective. Common control providers are responsible for: (i) documenting common controls in a *security plan* (or equivalent document prescribed by the organization); (ii) ensuring that required assessments of common controls are carried out by qualified assessors with a level of independence required by the organization and documenting findings in a *security assessment report*; and (iii) producing a *plan of action and milestones* for all controls having weaknesses or deficiencies. Security plans, security assessment reports, and plans of action and milestones for common controls (or a summary of such information) must be made available to information system owners *inheriting* those controls after the information is reviewed and approved by the senior official or executive responsible and accountable for those controls. This information should be used by authorizing officials within the organization in helping to make risk-based decisions in the security authorization process for their information systems. If common controls are provided to the organization (and its information systems) by entities *external* to the organization (e.g., shared service providers, external service providers), arrangements should be made with the external/shared service providers by the organization to obtain information on the effectiveness of the controls. Information obtained from external organizations regarding the effectiveness of common controls should be factored into risk-based authorization decisions.

Organizations should also determine the appropriate *impact level* of the common controls supporting information systems within the organization. Since these information systems depend on the security capabilities provided by common controls, impact-level decisions can affect the types of protections provided to supported information systems. Organizations should consider the impact levels of the information systems inheriting the security capabilities from the common controls in making the final impact determination. If the agreed-upon impact level of the common controls is lower than the highest impact level of the information systems inheriting the controls, the organization and information system owners agree to a course of action to ensure that the appropriate impact level is maintained for those information systems with a higher impact level than that of the common controls. Information system owners inheriting common controls can either list the common controls in their respective security plans or reference the controls contained in the security plan of the common control provider.

References: FIPS 199; NIST Special Publications 800-18, 800-53.

NSS References: CNSS Instructions 1199, 1253.

[72] Organizations may choose to defer common control selection until the *System Development/Acquisition* phase of the SDLC.

SECURITY CONTROL SELECTION

Task 1b: Select the security controls for the information system and document the controls in the security plan.

Primary Responsibility: Information System Owner.

Supporting Roles: Information System Security Officer; Information System Security Engineer; Information Owner/Steward.

SDLC Phase: System Initiation (requirements definition).[73]

Guidance: The initial set of baseline security controls is selected in accordance with the security category of the information system. The selection process should also include, as appropriate: (i) tailoring the baseline security controls by applying scoping, parameterization, and compensating control guidance; and (ii) supplementing the tailored baseline security controls with additional controls or control enhancements to address unique organizational needs based on an assessment of risk and local conditions (including for example, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances). The security plan contains an overview of the security requirements for the information system in sufficient detail to enable confirmation that the security controls selected would meet these requirements. The security plan also, in addition to the list of controls from NIST Special Publication 800-53 or CNSS Instruction 1253 to be implemented, describes the intended application of each control in the context of the information system with sufficient detail to enable a compliant implementation of the intent of the security plan. Information system owners *inheriting* common controls can either list the controls in their respective security plans or reference the controls contained in the security plan of the common control provider.

References: FIPS 199, 200; NIST Special Publications 800-18, 800-30, 800-53.

NSS References: CNSS Instructions 1199, 1230, 1253.

[73] Organizations may choose to defer security control selection until the *System Development/Acquisition* phase of the SDLC. Organizations may also choose to centralize the security control selection process for their subordinate units at a designated organizational level (e.g., agency, department, component, bureau), including any risk management decisions associated with that selection process.

SECURITY PLAN APPROVAL

Task 2: Review and approve the security plan.

Primary Responsibility: Authorizing Official ***or*** Designated Representative.

Supporting Roles: Senior Agency Information Security Officer; Chief Information Officer; Security Control Assessor; Risk Executive (Function).

SDLC Phase: System Development/Acquisition.

Guidance: The independent review of the security plan by the authorizing official or designated representative with support from the senior agency information security officer, chief information officer, risk executive (function), and security control assessor, helps determine if the plan is complete and consistent with the security requirements for the information system. The security plan review also helps to determine, to the greatest extent possible with available planning or operational documents, if the security plan correctly identifies the potential risk to organizational operations and assets, individuals, other organizations, and the Nation, that would be incurred if the controls identified in the plan were implemented as intended. Based on the results of this independent review and analysis, the authorizing official or designated representative, chief information officer, risk executive (function), senior agency information security officer, or security control assessor may recommend changes to the security plan.

If the security plan is deemed unacceptable, the authorizing official or designated representative sends the plan back to the information system owner (or common control provider) for appropriate action. If the security plan is deemed acceptable, the authorizing official or designated representative accepts the plan. The acceptance of the security plan represents an important milestone in the security authorization process for the information system. The authorizing official or designated representative by accepting the security plan, agrees to the set of security controls proposed to meet the security requirements for the information system. This organization-level agreement allows the security authorization process to advance to the next phase (i.e., the implementation and assessment of the security controls). The acceptance of the security plan also approves the level of effort and resources required to successfully complete the associated security authorization activities.

References: NIST Special Publications 800-18, 800-53.

NSS References: CNSS Instruction 1253.

Step 3 Implement Security Controls

SECURITY CONTROL IMPLEMENTATION

Task 1: Implement the security controls specified in the security plan.

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Information System Security Engineer; Information System Security Officer; Information Owner/Steward.

SDLC Phase: System Implementation.

Guidance: Organizations should use best practices when implementing security controls within an information system including system/software engineering methodologies, security engineering principles, and secure coding techniques. In most cases, security controls contained in NIST Special Publication 800-53 and CNSS Instruction 1253 are defined at a higher level of abstraction. When required, information system security engineers with support from information system security officers should employ a sound security engineering process that captures and refines information security requirements from the security controls and ensures their integration into information technology products and systems through purposeful security design or configuration. When available, organizations should consider the use of information technology products that have been tested, evaluated, or validated by approved, independent, third-party assessment facilities. As a starting point, organizations should follow the minimum assurance requirements described in NIST Special Publication 800-53 and CNSS Instruction 1253 when implementing security controls. For higher-impact systems (i.e., potential high-value targets) in situations where specific and credible threat information indicates the likelihood of advanced cyber attacks, additional assurance measures should be considered in accordance with the guidance in NIST Special Publication 800-53 and CNSS Instruction 1253.

References: FIPS 200; NIST Special Publication 800-53.

NSS References: CNSS Instructions 1199, 1253.

SECURITY CONTROL DOCUMENTATION

Task 2: Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Information Owner/Steward; Information System Security Officer.

SDLC Phase: System Implementation.

Guidance: Security control implementation documentation should follow best practices for software development and system, software, and security engineering disciplines and be consistent with established organizational policies and procedures for documenting activities associated with the system development life cycle. Whenever possible and practicable for technical security controls that are mechanism-based, organizations should take advantage of functional specifications and documentation provided by or obtainable from hardware/software vendors and systems integrators. Similarly, for management and operational controls, organizations should obtain security control implementation information from appropriate organizational entities (e.g., facilities offices, physical security offices, human resources offices).

References: NIST Special Publication 800-18.

NSS References: None.

Step 4 Assess Security Controls

ASSESSOR SELECTION AND INDEPENDENCE

Task 1: Identify and select the security control assessor(s) and determine if the selected assessor(s) possess the required degree of independence for the assessment.

Primary Responsibility: Authorizing Official ***or*** Designated Representative.

Supporting Roles: Information System Owner ***or*** Common Control Provider; Senior Agency Information Security Officer; Chief Information Officer; Risk Executive (Function).

SDLC Phase: System Implementation.

Guidance: An independent security control assessor is any individual or group capable of conducting an impartial assessment of an information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or the determination of security control effectiveness. Independent security control assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted security assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the assessor or assessors conducting the assessment of the security controls in the information system. The authorizing official determines the required level of assessor independence based on the impact level of the information system and the ultimate risk to organizational operations and assets, individuals, other organizations, and the Nation. The authorizing official determines if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision on whether to place the information system into operation or continue its operation.

In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the security control assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner or authorizing official, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results. The authorizing official should consult with the Office of the Inspector General, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on assessor independence in the types of special circumstances described above.

References: NIST Special Publications 800-53, 800-53A.

NSS References: CNSS Instructions 1253, 1253A.

SECURITY ASSESSMENT PLAN

Task 2: Develop a plan to assess the security controls.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Information System Owner ***or*** Common Control Provider; Information Owner/Steward; Information System Security Officer.

SDLC Phase: System Implementation.

Guidance: The *security assessment plan* provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. In lieu of developing unique or specialized methods and procedures to assess the security controls in the information system, assessors should consult NIST Special Publication 800-53A or CNSS Instruction 1253A, which provide standardized methods and procedures for assessing the security controls listed in NIST Special Publication 800-53 and CNSS Instruction 1253, respectively. The following items should be considered by assessors in developing plans to assess the security controls in information systems:

- Determine which security controls/control enhancements are to be included in the assessment based upon the contents of the security plan and the purpose/scope of the assessment;
- Select the appropriate assessment procedures to be used during the assessment based on the security controls and control enhancements that are to be included in the assessment;
- Tailor the selected assessment procedures, as needed;
- Develop additional assessment procedures, if necessary, to address security controls and control enhancements that are not contained in NIST Special Publication 800-53 or CNSS Instruction 1253 or to address additional assurance needs beyond what is provided in NIST Special Publication 800-53A or CNSS Instruction 1253A;
- Optimize the assessment procedures to reduce duplication of effort and provide cost-effective assessment solutions; and
- Finalize the assessment plan and obtain the necessary approvals to execute the plan.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

SECURITY ASSESSMENT PLAN APPROVAL

Task 3: Review and approve the plan to assess the security controls.

Primary Responsibility: Authorizing Official ***or*** Designated Representative

Supporting Roles: Senior Agency Information Security Officer; Chief Information Officer; Information System Owner ***or*** Common Control Provider; Information Owner/Steward; Security Control Assessor.

SDLC Phase: System Implementation.

Guidance: The purpose of the security assessment plan approval is two-fold: (i) to establish the appropriate expectations for the security control assessment; and (ii) to bound the level of effort for the security control assessment. An approved security assessment plan helps to ensure that a necessary and sufficient level of resources is applied toward determining security control effectiveness. Once the security assessment plan is completed, the plan is reviewed and approved by appropriate organizational officials to ensure that the plan is complete, consistent with the security objectives of the organization and organizational assessment of risk, and cost-effective with regard to the resources allocated for the assessment. Organizations should establish an approval process with the organizational officials (e.g., information system owners or common control providers, chief information officers, senior agency information security officers, authorizing official designated representatives, authorizing officials) designated as approving authorities for the security assessment plan.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

SUPPORTING MATERIALS

Task 4: Obtain appropriate documentation, records, artifacts, test results, and other materials needed to assess the security controls.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Information System Security Officer; Information System Owner ***or*** Common Control Provider; Information Owner/Steward.

SDLC Phase: System Implementation.

Guidance: The information system owner (or common control provider, as appropriate) should assist the assessor in gathering all relevant documents and supporting materials from the organization that will be required during the assessment of the security controls. Descriptive information about the information system is typically documented in the system identification section of the security plan or, in some cases, included by reference or as attachments to the plan. Supporting materials such as procedures, reports, logs, and records showing evidence of security control implementation should be identified as well. Assessing the security controls in an information system can be a very costly and time-consuming process. In order to make the security authorization process as timely and cost-effective as possible, the reuse of previous assessment results, when reasonable and appropriate, is strongly recommended. For example, a recent audit of an information system may have produced important information about the effectiveness of selected security controls. Another opportunity, as appropriate, to reuse previous assessment results comes from programs that test and evaluate the security features of commercial information technology products. And finally, if prior assessment results from the system developer are available, the security control assessor, under appropriate circumstances may incorporate those results into the assessment. Assessors should maximize the use of previous assessment results in determining the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

SECURITY CONTROL ASSESSMENT

Task 5: Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Information System Owner ***or*** Common Control Provider; Information Owner/Steward; Information System Security Officer.

SDLC Phase: System Implementation.

Guidance: Security control assessments 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 information system. The information system owner relies on the security expertise and the technical judgment of the assessor to: (i) assess the security controls in the information system and common controls inherited by information systems using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and reduce or eliminate identified vulnerabilities. The assessor findings should be an unbiased, factual reporting of what was found concerning the security controls assessed.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

PRELIMINARY SECURITY ASSESSMENT REPORT

Task 6: Prepare the preliminary security assessment report documenting the issues, findings, and recommendations from the security control assessment.

Primary Responsibility: Security Control Assessor.

Supporting Roles: None.

SDLC Phase: System Implementation.

Guidance: The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the *security assessment report*. The security assessment report is one of three key documents in the security authorization package developed by information system owners for authorizing officials. The security assessment report includes information from the assessor (in the form of assessment findings) necessary to determine the effectiveness of the security controls employed in the information system based upon the assessor's findings. The security assessment report is an important factor in an authorizing official's determination of risk to organizational operations and assets, individuals, other organizations, and the Nation. Security assessment reports are also produced for common control assessments and should be made available to all authorizing officials for information systems inheriting the controls. Security control assessment results should be documented at the level of detail appropriate for the assessment in accordance with the reporting format prescribed by organizational policy, NIST/CNSS guidelines, and OMB policy. The reporting format should also be appropriate for the type of security control assessment conducted (e.g., self-assessments, independent verification and validation, independent assessments supporting the security authorization process, or independent audits and evaluations of security controls by auditors or Inspectors General).

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

SECURITY ASSESSMENT REPORT REVIEW

Task 7: Review the preliminary security assessment report.

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Information System Security Officer; Information Owner/Steward; Authorizing Official or Designated Representative; Chief Information Officer; Senior Agency Information Security Officer.

SDLC Phase: System Implementation.

Guidance: Assessment findings in preliminary security assessment reports provide visibility into specific weaknesses and deficiencies in information systems and facilitate a disciplined and structured approach to mitigating risks in accordance with organizational priorities. Information system owners, in consultation with designated officials (e.g., authorizing official designated representative, chief information officer, senior agency information security officer, information owner/steward), may decide that certain assessment findings are inconsequential and present no significant risk to the organization. Alternatively, system owners and organizational officials may decide that certain findings are, in fact, significant, requiring immediate remediation actions. In all cases, organizations review assessor findings where weaknesses or deficiencies have been noted and apply judgment in determining the severity or seriousness of the findings (i.e., the potential adverse impact on organizational operations and assets, individuals, other organizations, or the Nation), and whether the findings are significant enough to be worthy of further investigation or remediation.

Since the results of security control assessments ultimately influence the content of security plans and plans of action and milestones, information system owners review the findings of assessors and with the concurrence of designated organizational officials, determine the appropriate steps required to correct weaknesses and deficiencies identified during the assessment. Senior leadership involvement in the mitigation process may be necessary in order to ensure that the organization's resources are effectively allocated in accordance with organizational priorities, providing resources first to the information systems that are supporting the most critical and sensitive missions for the organization or correcting the deficiencies that pose the greatest degree of risk.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

REMEDIATION ACTIONS

Task 8: If necessary, conduct remediation actions based on the preliminary security assessment report.[74]

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Information System Security Officer; Information Owner/Steward.

SDLC Phase: System Implementation.

Guidance: The assessment information produced by the assessor is provided to the information system owner or common control provider in the *preliminary security assessment report*. The system owner or common control provider may choose to act on selected recommendations of the assessor before the security assessment report is finalized if there are specific opportunities to correct weaknesses or deficiencies in the security controls or to correct/clarify misunderstandings or interpretations of assessment results. Security controls that are modified, enhanced, or added during this process may be reassessed by the assessor prior to the production of the final security assessment report or included within the plan of actions and milestones that accompanies the final security assessment report. The correction of deficiencies in security controls or carrying out of selected assessor recommendations during the information system owner's review of the preliminary security assessment report is not intended to replace the risk mitigation activities which occur after the delivery and acceptance of the final report. Rather, it provides the information system owner with an opportunity to address problems or deficiencies that may be quickly corrected.

References: NIST Special Publications 800-30, 800-53, 800-53A.

NSS References: CNSS Instructions 1230, 1253, 1253A.

REMEDIATION ASSESSMENT

Task 9: Assess the remediated security controls.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Information System Owner ***or*** Common Control Provider; Information System Security Officer; Information Owner/Steward.

SDLC Phase: System Implementation.

Guidance: If weaknesses or deficiencies in security controls are corrected, the remediated controls must be reassessed for effectiveness. Security control assessments determine the extent to which the *remediated* controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The information system owner relies on the security expertise and the technical judgment of the assessor to: (i) assess the remediated security controls in the information system (including remediated common controls inherited by information systems) using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the remediated controls and reduce or eliminate identified vulnerabilities. See RMF Step 4, Task 5.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

[74] Tasks 8, 9, and 10 may proceed in a cyclic manner as information system owners perform selected risk mitigation activities that are subsequently checked by the security control assessors, resulting in updates to security assessment reports.

FINAL SECURITY ASSESSMENT REPORT

Task 10: Update the security assessment report and prepare the executive summary.[75]

Primary Responsibility: Security Control Assessor.

Supporting Roles: None.

SDLC Phase: System Implementation.

Guidance: The preliminary security assessment report is updated with the latest assessment results and findings from any reassessments of remediated security controls. The delivery of the final assessment report to the information system owner or common control provider marks the official end of the security control assessment. Organizations may choose to develop an assessment *summary* from the detailed findings that are generated during a security control assessment. An assessment summary can provide an authorizing official with an abbreviated version a of security assessment report focusing on the highlights of the assessment, synopsis of key findings, and/or recommendations for addressing weaknesses and deficiencies in the security controls.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

SECURITY ASSESSMENT REPORT ADDENDUM

Task 11: If necessary, prepare an addendum to the security assessment report that reflects the initial results of the remediation actions taken and provides the information system owner or common control provider perspective on the assessment findings and recommendations.

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Information System Security Officer; Information Owner/Steward.

SDLC Phase: System Implementation.

Guidance: The optional addendum to the *security assessment report* provides information system owners and common control providers with an opportunity to respond to the initial findings of assessors. The addendum may include, for example, information regarding initial remediation actions taken by information system owners or common control providers in response to assessor findings, or provide an owner's perspective on the findings (e.g., including additional explanatory material, rebutting certain findings, and correcting the record). The addendum to the security assessment report should not change or influence in any manner, the initial assessor findings provided in the original report. Information provided by information system owners in the addendum should be considered by authorizing officials in their risk-based security authorization decisions. Similar consideration should be given to the addendums produced by common control providers during the review and risk-related decisions of organizational officials responsible for the effective deployment of common controls inherited by information systems within the organization.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

[75] At the discretion of the organization, security control assessors may be given additional duties or responsibilities for the post-processing and analysis of security control assessment findings and results. This may include, for example, making specific recommendations and determinations to authorizing officials (known in some communities of interest as *certification recommendations* or *certification determinations*).

SECURITY PLAN UPDATE

Task 12: Update the security plan based on the findings and recommendations of the security assessment report and any remediation actions taken.

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Information System Security Officer; Information Owner/Steward.

SDLC Phase: System Implementation.

Guidance: The security plan should reflect the actual state of the security controls after the initial security control assessment and any modifications by the information system owner or common control provider in addressing the recommendations for corrective actions from the assessor. At the completion of the security control assessment, the security plan should contain an accurate list and description of the security controls implemented (including compensating controls) and a list of identified vulnerabilities (i.e., security controls not implemented).

References: NIST Special Publications 800-18, 800-53A.

NSS References: CNSS Instruction 1253A.

PLAN OF ACTION AND MILESTONES

Task 13: Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report.

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Information System Security Officer; Information Owner/Steward.

SDLC Phase: System Implementation.

Guidance: The *plan of action and milestones*, prepared by the information system owner for the authorizing official, is one of three key documents in the security authorization package and describes the specific measures that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the security control assessment; and (ii) to address the remaining known vulnerabilities in the information system. The plan of action and milestones document identifies: (i) the tasks needing to be accomplished; (ii) the resources required to accomplish the elements of the plan; (iii) any milestones in meeting the tasks; and (iv) the scheduled completion dates for the milestones. Thus, the plan of action and milestones is used by the authorizing official to monitor the progress in correcting weaknesses or deficiencies noted during the security control assessment.

Organizations should define a strategy for developing plans of action and milestones that facilitates a prioritized approach to risk mitigation that is consistent across the organization. The strategy helps to ensure that plans of action and milestones are based on:

- The security category of the information system;
- The specific weaknesses or deficiencies in the information system security controls;
- The importance of the identified security control weaknesses or deficiencies (i.e., the direct or indirect effect the weaknesses or deficiencies may have on the overall security state of the information system, and hence on the risk exposure of the organization, or ability of the organization to perform its mission or business functions);
- The organization's proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g., prioritization of risk mitigation actions, allocation of risk mitigation resources); and
- The organization's rationale for accepting certain weaknesses or deficiencies in the security controls.

Organizational strategies for plans of action and milestones should be guided by the security categories of the respective information systems where the risk mitigation activities will occur in accordance with FIPS 199 and CNSS Instruction 1199. Organizations may decide, for example, to allocate the majority of risk mitigation resources initially to the *highest impact* information systems because a failure to correct the weaknesses or deficiencies in those systems could potentially have the most significant adverse impacts on the organization's missions or business operations. Organizations should also prioritize weaknesses or deficiencies within the categorized information systems. In general, the plan of action and milestones strategy should always address the highest-impact information systems first and subsequently, the highest-priority weaknesses or deficiencies within those prioritized systems.

References: OMB Memorandum 02-01; NIST Special Publication 800-53A.

NSS References: OMB Memorandum 02-01; CNSS Instruction 1253A.

3.2 CONDUCTING THE AUTHORIZATION *(EXECUTION PHASE)*

Subsequent to completing the preparation phase, the organization begins the security authorization *execution phase*. The following RMF step and associated tasks are completed during the execution phase.

Step 5 Authorize Information System

SECURITY AUTHORIZATION PACKAGE

Task 1: Assemble the authorization package and submit to authorizing official for approval.[76]

Primary Responsibility: Information System Owner.

Supporting Roles: Information System Security Officer; Security Control Assessor.

SDLC Phase: System Implementation.

Guidance: The *security authorization package* contains the security plan, security assessment report, and plan of action and milestones. The information in these key documents is used by authorizing officials to make credible, risk-based decisions on authorizing an information system for operation or continuing its operation under current conditions. Additional information can be included in the basic security authorization package at the request of the organization carrying out the authorization of the information system. The contents of the security authorization package should be protected appropriately in accordance with organizational and federal policies. Organizations are strongly encouraged to use automated support tools in preparing and managing the content of the security authorization package to help provide an effective vehicle for maintaining and updating critical information for authorizing officials regarding the ongoing security status of information systems within the organization. Providing orderly and disciplined updates to the security plan, security assessment report, and plan of action and milestones on an ongoing basis, supports the principle of near real-time risk management and facilitates more cost-effective and meaningful reauthorization actions. Ultimately, with the use of automated tools and associated supporting databases, authorizing officials and other senior leaders within the organization should be able to obtain important information to maintain situational awareness with regard to the security state of the information systems supporting the organization's missions and business processes.

References: None.

NSS References: None.

[76] Common control providers are required to prepare security authorization packages. The security plans (or equivalent documents), security assessment reports, and plans of action and milestones for common controls are submitted to appropriate organizational officials for approval (i.e., senior officials or executives within the organization with oversight *responsibility* and *accountability* for the effective implementation of common controls).

RISK DETERMINATION

Task 2: Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

Primary Responsibility: Authorizing Official ***or*** Designated Representative.

Supporting Roles: Senior Agency Information Security Officer; Risk Executive (Function).

SDLC Phase: System Implementation.

Guidance: Given information from the information system owner provided in the security authorization package (i.e., security plan, security assessment report, and plan of action and milestones),[77] the risk executive (function) provides organization-level guidance and relevant information for authorizing officials concerning organizational risk tolerance, known existing aggregated risks from current information systems, and other sources of risk potentially impacting organizational operations and assets, individuals, other organizations, and the Nation. Security authorization decisions are based on an *understanding* and explicit *acceptance* of the organizational risk brought about by the operation and use of information systems. Risk determinations (conveyed in any format deemed appropriate by the organization) provide essential information for authorizing officials and promote a greater understanding of the actual risk to the organization and its critical missions and business functions. Risk determinations should incorporate risk-related information provided by common control providers and organizational entities responsible for overseeing the planning, development, implementation, and assessment of such inherited controls.

References: NIST Special Publications 800-30, 800-39.

NSS References: CNSS Instruction 1230.

RISK ACCEPTABILITY

Task 3: Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.

Primary Responsibility: Authorizing Official.

Supporting Roles: Authorizing Official Designated Representative; Senior Agency Information Security Officer; Risk Executive (Function).

SDLC Phase: System Implementation.

Guidance: The explicit acceptance of *risk* is the responsibility of the authorizing official and cannot be delegated to other officials within the organization. The authorizing official should consider many factors when deciding if the risk to organizational operations (including mission, function, image, or reputation), organizational assets, individuals, other organizations, and the Nation, is acceptable. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision. The authorizing official issues an official authorization decision for the information system after reviewing all of the relevant information and, where appropriate, consulting with key organizational officials, including the organization's risk executive (function).

References: None.

NSS References: None.

[77] Information system-related security risk information derived from the current authorization process, should be available to the risk executive (function) for use in formulating organization-wide, global risk recommendations and providing advice to authorizing officials.

SECURITY AUTHORIZATION DECISION

Task 4: Prepare the security authorization decision document and transmit authorization decision and authorization package to the information system owner.

Primary Responsibility: Authorizing Official.

Supporting Roles: Authorizing Official Designated Representative.

SDLC Phase: System Implementation.

Guidance: Security authorization decisions should be based on the content of the security authorization package submitted by the information system owner and any inputs received from the organization's risk executive (function). The authorization package provides comprehensive information on the security state of the information system. Risk executive (function) inputs, including previously established overarching risk guidance to authorizing officials, provide additional organization-wide information to the authorizing official that may be relevant and affect the authorization decision (e.g., organizational risk tolerance, specific mission and business requirements, dependencies among information systems, and other types of risks not directly associated with the information system). Risk executive (function) inputs are documented and become part of the security authorization decision. Security authorization decisions, including inputs from the risk executive (function), should be conveyed to information system owners and made available to interested parties within the organization (e.g., information system owners and authorizing officials for interconnected systems, chief information officers, , information owners/stewards, senior managers). To ensure that the organization's mission, business, and operational needs are fully considered, the authorizing official should meet with the information system owner prior to issuing the authorization decision to discuss the assessment results, the terms and conditions of the authorization, and any other factors affecting the organization.

The *authorization decision document* transmits the final security authorization decision from the authorizing official to the information system owner and other key organizational officials, as appropriate. The authorization decision document contains the following information:

- Authorization decision;
- Terms and conditions for the authorization; and
- Authorization termination date.

The security *authorization decision* indicates to the information system owner whether the system is: (i) authorized to operate; or (ii) not authorized to operate. The *terms and conditions* for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system that must be followed by the system owner. The *authorization termination date*, established by the authorizing official, indicates when the security authorization expires. Authorization termination dates should be consistent with federal and organizational policies. The authorization decision document is attached to the original security authorization package containing the supporting documentation and transmitted to the information system owner. Upon receipt of the authorization decision document and original authorization package, the information system owner accepts the terms and conditions of the authorization. Authorization documents, especially information dealing with information system vulnerabilities, should be: (i) marked and appropriately protected in accordance with federal and organizational policy; and (ii) retained in accordance with the organization's record retention policy.

References: None.

NSS References: None.

3.3 MAINTAINING THE AUTHORIZATION *(MAINTENANCE PHASE)*

Subsequent to completing the execution phase, the organization begins the authorization *maintenance phase*.[78] The following RMF step and associated tasks are completed during the maintenance phase.

Step 6 Monitor Security Controls

SECURITY CONTROL MONITORING STRATEGY

Task 1: Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes in the information system or its environment of operation.

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Authorizing Official or Designated Representative; Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer; Information System Security Officer; Information Owner/Steward.

SDLC Phase: System Operations/Maintenance.

Guidance: A critical aspect of the security authorization process is the post-authorization period involving the continuous monitoring of security controls in the information system (or controls inherited by the system). A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management for information systems. An effective continuous monitoring program includes:

- Configuration management and control processes;
- Security impact analyses on actual or proposed changes to information systems and environments of operation;
- Assessment of selected security controls in information systems and controls inherited by those systems (i.e., common controls); and
- Security status reporting to appropriate organizational officials.

The criteria for selecting which security controls will be monitored and for determining the frequency of such monitoring should be established by the information system owner or common control provider in collaboration with authorizing official or designated representative, chief information officer, senior agency information security officer, and risk executive (function). The criteria should reflect the organization's priorities and importance of the information system (or in the case of common controls, the information systems inheriting the controls) to organizational operations and assets, individuals, other organizations, and the Nation in accordance with FIPS 199 or CNSS Instruction 1199. Those security controls that are the most volatile (i.e., subject to change over time), critical to certain aspects of the organization's protection strategy, or identified in current plans of action and milestones documents are assessed at least annually. All other controls are assessed at least once during the information system's routine authorization cycle in accordance with federal or organizational policies. The authorizing official and the senior agency information security officer should approve the set of security controls that are to be monitored on a continuous basis as well as the frequency of the monitoring activities. The monitoring of security controls continues throughout the SDLC.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

[78] Owners of *common controls* that are not provided as part of an information system (e.g., personnel security controls, physical and environmental protection controls), are required to participate in the ongoing security control monitoring process established by the organization. This includes completing all of the tasks required by the security authorization maintenance process.

SYSTEM AND ENVIRONMENT CHANGES

Task 2: Document the proposed or actual changes to the information system or the environment of operation.

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Information System Security Officer; Information Owner/Steward.

SDLC Phase: System Operations/Maintenance.

Guidance: Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. An orderly and disciplined approach to managing, controlling, and documenting proposed or actual changes to information systems or their environments of operation is an essential element of an effective security control monitoring program. Therefore, strict configuration management and control processes should be established by organizations to support such monitoring activities. It is important to record any relevant information about the specific changes to the hardware, software, or firmware such as version or release numbers, descriptions of new or modified features/capabilities, and security implementation guidance. It is also important to record any changes to the information system's environment of operation such as modifications to hosting facilities. The information system owner should use this information in assessing the potential security impact of the changes. Documenting proposed or actual changes to an information system or its environment of operation and subsequently assessing the potential impact those changes may have on the overall security state of the system or the organization is an important aspect of security control monitoring, achieving situational awareness, and maintaining the security authorization. Information system changes should generally not be undertaken prior to assessing the security impact of such changes.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

SECURITY IMPACT ANALYSIS

Task 3: Determine the security impact of the proposed or actual changes to the information system or the environment of operation in accordance with the security control monitoring strategy.

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Information System Security Officer; Information Owner/Steward; Senior Agency Information Security Officer; Authorizing Official or Designated Representative; Risk Executive (Function).

SDLC Phase: System Operations/Maintenance.

Guidance: Security impact analysis conducted by the organization on an as needed basis determines the extent to which changes to the information system or its environment of operation have affected the security state of the system. Changes to the information system or its environment of operation may affect the security controls currently in place, produce new vulnerabilities in the system, or generate requirements for new security controls that were not needed previously. If the results of the impact analysis indicate that the proposed or actual changes to the information system will affect or have affected the security state of the system, corrective actions are initiated and appropriate documents revised/updated (e.g., the security plan, security assessment report, and plan of action and milestones). The information system owner should consult with appropriate organizational personnel (e.g., configuration management or control board, senior agency information security officer) prior to implementing any security-related changes to the information system. The authorizing official or designated representative should use the revised/updated security assessment report in consultation with the senior agency information security officer and risk executive (function) to determine if a reauthorization action is necessary. Conducting security impact analyses is part of an ongoing assessment of risk. The effort applied to the analyses is commensurate with the security category of the information system in accordance with FIPS 199 or CNSS Instruction 1199. The authorizing official or designated representative in consultation with the risk executive (function) confirms, as needed, determinations of resulting risk and, if performed by the designated representative, notifies the authorizing official of any significant changes in the risk being incurred.

References: NIST Special Publications 800-30, 800-53A.

NSS References: CNSS Instructions 1230, 1253A.

ONGOING SECURITY CONTROL ASSESSMENTS

Task 4: Assess a selected subset of the security controls in the information system or the environment of operation (including those controls affected by changes to the system/environment) in accordance with the continuous monitoring strategy.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Information System Owner ***or*** Common Control Provider; Information System Security Officer; Information Owner/Steward; Authorizing Official ***or*** Designated Representative.

SDLC Phase: System Operations/Maintenance.

Guidance: Organizations assess all security controls in an information system during the initial security authorization. Subsequent to the initial authorization and in accordance with OMB policy, the organization assesses a subset of the security controls annually during continuous monitoring. The selection of an appropriate subset of security controls to monitor and the frequency of monitoring is based on the monitoring strategy developed by the information system owner or common control provider (see RMF Step 6, Task 1).

Organizations can use the current year's assessment results to meet the annual FISMA security control assessment requirement. To satisfy this requirement, organizations can draw upon the assessment results from any of the following sources, including but not limited to: (i) security control assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring activities; or (iii) testing and evaluation of the information system as part of the system development life cycle process or audit (provided that the testing, evaluation, or audit results are current, relevant to the determination of security control effectiveness, and obtained by assessors with the required degree of independence required by the authorizing official). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

ONGOING REMEDIATION ACTIONS

Task 5: Conduct remediation actions based on the results of the selected security control assessments and outstanding items in the plan of action and milestones.

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Information System Security Officer; Information System Security Engineer; Security Control Assessor; Information Owner/Steward.

SDLC Phase: System Operations/Maintenance.

Guidance: The assessment information produced by an assessor during continuous monitoring is provided to the information system owner in an updated *security assessment report*. Information system owners initiate remediation actions on outstanding items listed in the plan of actions and milestones and findings produced during the continuous monitoring of security controls. The security control assessor may provide recommendations as to appropriate remediation actions. Security controls modified, enhanced, or added during this process should be reassessed by the assessor to ensure that appropriate corrective actions have been taken to eliminate weaknesses or deficiencies or mitigate the identified risk. See RMF Step 4, Task 8.

References: NIST Special Publications 80-30, 800-53, 800-53A.

NSS References: CNSS Instructions 1230, 1253, 1253A.

CRITICAL DOCUMENT UPDATES

Task 6: Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.

Primary Responsibility: Information System Owner ***or*** Common Control Provider.

Supporting Roles: Information System Security Officer; Information Owner/Steward.

SDLC Phase: System Operations/Maintenance.

Guidance: To facilitate the near real-time management of risk associated with the operation and use of information systems, organizations should update security plans, security assessment reports, and plans of action and milestones on a regular basis. Updated security plans should reflect any modifications to security controls based on risk mitigation activities carried out by information system owners. Updated security assessment reports should reflect additional assessment activities carried out to determine security control effectiveness based on modifications to the security plan and deployed controls. Updated plans of action and milestones should: (i) report progress made on the current outstanding items listed in the plan; (ii) address vulnerabilities in the information system discovered during the security impact analysis or security control monitoring; and (iii) describe how the information system owner intends to address those vulnerabilities.

The frequency of updates to critical authorization-related documents is at the discretion of information system owners and authorizing officials in accordance with federal and organizational policies. Updates should be accurate and timely since the information provided influences ongoing security-related actions and decisions by authorizing officials and other senior leaders within the organization with either direct or indirect responsibility for the ongoing management of information system-related security risks. With the use of automated support tools and effective organization-wide security program management practices, authorizing officials should be able to readily access the current security state of the information system, facilitating near real-time management of risk to organizational operations and assets, individuals, other organizations, and the Nation, and to provide essential information for reauthorization decisions.

When updating critical information in documents such as security plans, security assessment reports, and plans of action and milestones, organizations should ensure that the original information needed for oversight, management, and auditing purposes is not modified or destroyed. Providing an effective method of tracking changes to information over time through strict configuration management and control procedures (including version control) is necessary to: (i) achieve transparency in the information security activities of the organization; (ii) obtain individual accountability for security-related actions; and (iii) better understand emerging trends in the organization's information security program.

References: NIST Special Publications 800-18, 800-53A.

NSS References: CNSS Instruction 1253A.

SECURITY STATUS REPORTING

Task 7: Report the security status of the information system to the authorizing official and other appropriate organizational officials on a periodic basis.

Primary Responsibility: Information System Owner.

Supporting Roles: Information System Security Officer.

SDLC Phase: System Operations/Maintenance.

Guidance: The results of continuous monitoring activities should be recorded and reported to the authorizing official on a regular basis. Security status reports provide the authorizing official and other senior leaders within the organization, essential information with regard to the security state of the information system. Security status reports should describe the continuous monitoring activities employed by the information system owner. Security status reports should also address vulnerabilities in the information system discovered during the security control assessment, security impact analysis, and security control monitoring and how the information system owner intends to address those vulnerabilities. Organizations have significant latitude and flexibility in the breadth, depth, and formality of security status reports.[79] At a minimum, security status reports should summarize key changes to security plans, security assessment reports, and plans of action and milestones.

The frequency of security status reports is at the discretion of the organization and in accordance with federal policies. Status reports should occur at appropriate intervals to transmit significant security-related information about the information system, but not so frequently as to generate unnecessary work. The authorizing official should use the security status reports in consultation with the senior agency information security officer and risk executive (function) to determine if a reauthorization action is necessary. The authorizing official should notify the information system owner if there is a decision to reauthorize the system. Security status reports should be appropriately marked, protected, and handled in accordance with organizational and federal policies.

At the discretion of the organization, security status reports on information systems can be used to help satisfy FISMA reporting requirement for documenting remedial actions for any security-related deficiencies. Note that this status reporting is intended to be ongoing, not to be interpreted as requiring the time, expense, and formality associated with the information provided for initial approval to operate. Rather, the reporting is conducted in the most cost-effective manner consistent with achieving the reporting objectives.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

[79] Security status reports can take whatever form the organization deems most appropriate. The goal is efficient and effective ongoing communication of the current security state of the information system.

ONGOING RISK DETERMINATION AND ACCEPTANCE

Task 8: Periodically review the reported security status of the information system and determine whether the risk to organizational operations and assets, individuals, other organizations, or the Nation remains acceptable.

Primary Responsibility: Authorizing Official.

Supporting Roles: Authorizing Official Designated Representative; Senior Agency Information Security Officer; Risk Executive (Function).

SDLC Phase: System Operations/Maintenance.

Guidance: The authorizing official or designated representative reviews the reported security status of the information system periodically, to determine the current risk to organizational operations and assets, individuals, other organizations, or the Nation. The authorizing official determines, with inputs as appropriate from the authorizing official designated representative, senior agency information security officer, and the risk executive (function), whether the current risk is acceptable and forwards appropriate direction to the information system owner. The use of automated support tools to capture, organize, and maintain security status information promotes the concept of *near real-time risk management* through ongoing situational awareness regarding the overall risk posture of the organization. The risks being incurred may change over time based on the information provided in the security status reports. Determining how the changing conditions affect the mission/business risks associated with information systems within the organization is essential for maintaining *adequate security*. By carrying out ongoing *risk determination* and *risk acceptance*, authorizing officials can maintain the security authorization over time. Formal reauthorization of the information system (or common controls), whether *time-driven* or *event-driven*, occurs only in accordance with federal or organizational policies.

References: None.

NSS References: None.

SYSTEM REMOVAL AND DECOMMISSIONING

Task 9: Implement an organizationally approved information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.

Primary Responsibility: Information System Owner.

Supporting Roles: Information System Security Officer; Information Owner/Steward; Senior Agency Information Security Officer; Risk Executive (Function); Authorizing Official Designated Representative.

SDLC Phase: System Disposition.

Guidance: When a federal information system is removed from operation, a number of authorization-related actions are required. Organizations should ensure that all security controls addressing information system decommissioning (e.g., media sanitization, configuration management and control) are implemented. Organizational tracking and management systems should be updated to indicate the specific information system components that are being removed from the inventory. Security status reports should reflect the new status of the information system. Users and application owners hosted on the decommissioned information system should be notified as appropriate and any security control inheritance relationships should be reviewed and assessed for impact.

References: NIST Special Publication 800-53A.

NSS References: CNSS Instruction 1253A.

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, INSTRUCTIONS, STANDARDS, AND GUIDELINES

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act (P.L. 104-13), May 1995.
4. USA PATRIOT Act (P.L. 107-56), October 2001.

POLICIES, DIRECTIVES, INSTRUCTIONS

5. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
6. Office of Management and Budget, Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.
7. Committee on National Security Systems Instruction (CNSSI) 1199, *Security Categorization for National Security Systems and Information*, pending final publication.
8. Committee on National Security Systems Instruction (CNSSI) 1230, *Risk Assessment Guideline for National Security Systems*, pending final publication.
9. Committee on National Security Systems Instruction (CNSSI) 1253, *Security Control Catalog for National Security Systems*, pending final publication.
10. Committee on National Security Systems Instruction (CNSSI) 1253A, *Guide for Assessing Security Controls in National Security Systems*, pending final publication.
11. Committee on National Security Systems Instruction (CNSSI) 4009, *National Information Assurance Glossary*, June 2006.

STANDARDS

12. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
13. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

GUIDELINES

14. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
15. National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments* (Draft), October, 2008.
16. National Institute of Standards and Technology Special Publication 800-39 (Draft), *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

17. National Institute of Standards and Technology Special Publication 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007.
18. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008.
19. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
20. National Institute of Standards and Technology Special Publication 800-60, Revision 1 (Draft), *Guide for Mapping Types of Information and Information Systems to Security Categories*, November 2007.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

This appendix provides definitions for security terminology used within Special Publication 800-37. The terms in the glossary are consistent with the terms used in the suite of FISMA-related security standards and guidelines developed by NIST. Unless otherwise stated, all terms used in this publication are also consistent with the definitions contained in the CNSS Instruction 4009, *National Information Assurance Glossary*.

Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Assurance	The grounds for confidence that the set of intended security controls in an information system are effective in their application.
Authorizing Official [FIPS 200 adapted]	A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Authorizing Official Designated Representative	An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Chief Information Officer [PL 104-106, Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Common Control Provider	An organizational official responsible for the planning, development, implementation, assessment, authorization, and maintenance of common controls (i.e., security controls inherited by information systems).
Common Control	A security control that is inherited by an information system.
Compensating Security Control	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53 or in CNSS Instruction 1253, that provide equivalent or comparable protection for an information system.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. Synonymous with *Federal Agency*.
External Information System (or component)	An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service	An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system).

External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
Federal Agency	See Executive Agency.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by a federal agency, or by a contractor of a federal agency or by another organization on behalf of a federal agency.
Hybrid Security Control	A security control that is part common control and part system-specific control.
Information Owner [CNSS Inst. 4009 adapted]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy [CNSS Inst. 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information Steward	Individual or group that helps to ensure the careful and responsible management of federal information belonging to the Nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security-related federal policies, directives, regulations, standards, and guidance.

Information System [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
[OMB Circular A-130, Appendix III]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information in accordance with defined procedures, whether automated or manual.
Information System Owner (or Program Manager) [CNSS Inst. 4009, Adapted]	Official responsible for the overall procurement, development, integration, modification, operation, and maintenance of an information system.
Information System Security Engineer	Individual assigned responsibility for conducting information system security engineering activities.
Information System Security Engineering	Process that captures and refines information security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration.
Information System-related Security Risks	Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See *Risk*.
Information System Security Officer [CNSS Inst. 4009, Adapted]	Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Organization [FIPS 200]	A federal agency or, as appropriate, any of its operational elements.
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished, resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Risk [NIST SP 800-30, Revision 1]	A measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of the likelihood of the circumstance or event occurring and of the resulting adverse impacts.

Risk Assessment [NIST SP 800-30, Revision 1]	The process of determining risks; that is, determining the extent to which an entity is threatened by potential, adverse circumstances or events. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF). Risk assessment for information system-related security risks includes assessment of the susceptibility to adverse impacts through information (e.g., consideration of dependence on information, vulnerabilities in mission and business processes, and effectiveness of risk mitigations) and assessment of the threat environment with regard to causing such impacts. Synonymous with *risk analysis*.
Risk Executive (Function)	An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.
Risk Management [NIST SP 800-39]	A management process employed by an organization to achieve and maintain an acceptable level of risk. The Risk Management Framework describes the recommended process for managing information system-related security risks.
Security Authorization (to operate)	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Security Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Security Category [FIPS 199 as amended by NIST SP 800-53]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operation, organizational assets, individuals, other organizations, and the Nation.
Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system 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.
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment.
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed for effectiveness by other entities either internal or external to the organization where the system or application resides.
Security Impact Analysis	The analysis conducted by an organizational official, often during the maintenance phase of the security authorization process, to determine the extent to which changes to an information system or its environment of operation have impacted the security state of the system.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Plan [NIST SP 800-18, Rev 1]	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Security Requirements [FIPS 200]	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. Synonymous with *Chief Information Security Officer*.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
System	See Information System.
System-specific Security Control	Security control for an information system that has not been designated as a common control.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with *threat agent*.
Vulnerability [CNSS Inst. 4009, Adapted]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CNSS	Committee on National Security Systems
COTS	Commercial Off-The-Shelf
DNI	Director of National Intelligence
DOD	Department of Defense
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
NSS	National Security System
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
P.L.	Public Law
POAM	Plan of Action and Milestones
RMF	Risk Management Framework
SP	Special Publication
U.S.C.	United States Code

APPENDIX D

SUMMARY OF PHASES AND TASKS

LISTING OF PRIMARY RESPONSIBILITIES AND SUPPORTING ROLES

SUMMARY TABLE		
TASK	**PRIMARY RESPONSIBILITY**	**SUPPORTING ROLES**
Preparation Phase, RMF Step 1: Categorize Information System		
TASK 1 System Description	Information System Owner	Authorizing Official *or* Designated Representative Information System Security Officer Senior Agency Information Security Officer Information Owner/Steward
TASK 2 System Registration	Information System Owner	Information System Security Officer
TASK 3 Security Categorization	Information System Owner	Authorizing Official *or* Designated Representative Chief Information Officer Senior Agency Information Security Officer Risk Executive (Function) Information Owner/Steward
Preparation Phase, RMF Step 2: Select Security Controls		
TASK 1a Common Control Selection	Chief Information Officer Senior Agency Information Security Officer	Common Control Provider(s) Authorizing Official *or* Designated Representative Chief Information Officer Information System Security Engineer
TASK 1b Security Control Selection	Information System Owner	Information System Security Officer Information System Security Engineer Information Owner/Steward
TASK 2 Security Plan Approval	Authorizing Official *or* Designated Representative	Senior Agency Information Security Officer Chief Information Officer Risk Executive (Function) Security Control Assessor
Preparation Phase, RMF Step 3: Implement Security Controls		
TASK 1 Security Control Implementation	Information System Owner *or* Common Control Provider	Information System Security Officer Information System Security Engineer Information Owner/Steward
TASK 2 Security Control Documentation	Information System Owner *or* Common Control Provider	Information System Security Officer Information Owner/Steward

SUMMARY TABLE		
TASK	**PRIMARY RESPONSIBILITY**	**SUPPORTING ROLES**
Preparation Phase, RMF Step 4: Assess Security Controls		
TASK 1 Assessor Selection and Independence	Authorizing Official *or* Designated Representative	Information System Owner *or* Common Control Provider Senior Agency Information Security Officer Chief Information Officer Risk Executive (Function)
TASK 2 Security Assessment Plan	Security Control Assessor	Information System Security Officer Information System Owner *or* Common Control Provider Information Owner/Steward
TASK 3 Security Assessment Plan Approval	Authorizing Official *or* Designated Representative	Senior Agency Information Security Officer Chief Information Officer Information System Owner *or* Common Control Provider Security Control Assessor Information Owner/Steward
TASK 4 Supporting Materials	Security Control Assessor	Information System Security Officer Information System Owner *or* Common Control Provider Information Owner/Steward
TASK 5 Security Control Assessment	Security Control Assessor	Information System Owner *or* Common Control Provider Information System Security Officer Information Owner/Steward
TASK 6 Preliminary Security Assessment Report	Security Control Assessor	None
TASK 7 Security Assessment Report Review	Information System Owner *or* Common Control Provider	Authorizing Official or Designated Representative Chief Information Officer Senior Agency Information Security Officer Information System Security Officer Information Owner/Steward
TASK 8 Remediation Actions	Information System Owner *or* Common Control Provider	Information System Security Officer Information Owner/Steward
TASK 9 Remediation Assessment	Security Control Assessor	Information System Owner *or* Common Control Provider Information System Security Officer Information Owner/Steward
TASK 10 Final Security Assessment Report	Security Control Assessor	None

SUMMARY TABLE		
TASK	**PRIMARY RESPONSIBILITY**	**SUPPORTING ROLES**
Preparation Phase, RMF Step 4: Assess Security Controls		
TASK 11 Security Assessment Report Addendum	Information System Owner *or* Common Control Provider	Information System Security Officer Information Owner/Steward
TASK 12 Security Plan Update	Information System Owner *or* Common Control Provider	Information System Security Officer Information Owner/Steward
TASK 13 Plan of Action and Milestones	Information System Owner *or* Common Control Provider	Information System Security Officer Information Owner/Steward
Execution Phase, RMF Step 5: Authorize Information System		
TASK 1 Security Authorization Package	Information System Owner	Information System Security Officer
TASK 2 Risk Determination	Authorizing Official *or* Designated Representative	Senior Agency Information Security Officer Risk Executive (Function)
TASK 3 Risk Acceptability	Authorizing Official	Authorizing Official Designated Representative Senior Agency Information Security Officer Risk Executive (Function)
TASK 4 Security Authorization Decision	Authorizing Official	Authorizing Official Designated Representative
Maintenance Phase, RMF Step 6: Monitor Security Controls		
TASK 1 Security Control Monitoring Strategy	Information System Owner *or* Common Control Provider	Information System Security Officer Authorizing Official or Designated Representative Chief Information Officer Senior Agency Information Security Officer Risk Executive (Function) Information Owner/Steward
TASK 2 System and Environment Changes	Information System Owner *or* Common Control Provider	Information System Security Officer Information Owner/Steward
TASK 3 Security Impact Analysis	Information System Owner *or* Common Control Provider	Information System Security Officer Senior Agency Information Security Officer Authorizing Official or Designated Representative Information Owner/Steward

SUMMARY TABLE		
TASK	**PRIMARY RESPONSIBILITY**	**SUPPORTING ROLES**
TASK 4 Ongoing Security Control Assessments	Security Control Assessor	Information System Owner *or* Common Control Provider Information System Security Officer Authorizing Official *or* Designated Representative Information Owner/Steward
TASK 5 Ongoing Remediation Actions	Information System Owner *or* Common Control Provider	Information System Security Officer Information System Security Engineer Security Control Assessor Information Owner/Steward
Maintenance Phase, RMF Step 6: Monitor Security Controls		
TASK 6 Critical Document Updates	Information System Owner *or* Common Control Provider	Information System Security Officer Information Owner/Steward
TASK 7 Security Status Reporting	Information System Owner	Information System Security Officer
TASK 8 Ongoing Risk Determination and Acceptance	Authorizing Official	Authorizing Official Designated Representative Senior Agency Information Security Officer Risk Executive (Function)
TASK 9 System Removal and Decommissioning	Information System Owner	Information System Security Officer Authorizing Official Designated Representative Senior Agency Information Security Officer Risk Executive (Function) Information Owner/Steward