The attached DISCUSSION DRAFT document (provided here for historical purposes), originally posted on September 28, 2017, **has been superseded by the following publication**:

Publication Number: **NIST Special Publication (SP) 800-37 Rev. 2 (Initial Public Draft)**

Title: ***Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy***

Publication Date: **May 9, 2018**

- For the most current version of SP 800-37 Rev. 2, see https://csrc.nist.gov/publications/sp800.
- Information about the attached Draft publication can be found at: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/archive/2017-09-28
- Information on other NIST Computer Security Division publications and programs can be found at: https://csrc.nist.gov/publications

Draft NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

PRE-RELEASE MATERIAL

This publication contains comprehensive updates to the NIST Risk Management Framework including the incorporation of key concepts from the *Cybersecurity Framework*, the privacy risk management framework introduced in NIST Interagency Report 8062, and the systems security engineering framework defined in NIST Special Publication 800-160. The frameworks can be used in a complementary manner to manage security and privacy risks to information systems, organizations, and individuals.

The 800-37, Revision 2 *discussion draft* is intended to solicit feedback on the initial changes and updates proposed for the Risk Management Framework 2.0 in preparation for the Initial Public Draft that is targeted for release in the Fall 2017. The feedback received from the public workshop and the reviewers from the public and private sectors will be carefully considered and inform subsequent versions of this document.

JOINT TASK FORCE

DISCUSSION DRAFT

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

Draft NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

September 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the 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, OMB Director, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-37, Revision 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-37, Rev. 2, **112 pages** (September 2017)
CODEN: NSPUE2

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

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts, practices, and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review draft publications during the designated public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at **http://csrc.nist.gov/publications**.

Public comments will be accepted during the Initial Public Draft projected for publication in November 2017.

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

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) 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 (IT). ITL's responsibilities include the development of management, administrative, technical, and physical standards/guidelines for the cost-effective security of other than national security-related information and protection of individuals' privacy in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information systems security and privacy and its collaborative activities with industry, government, and academic organizations.

Abstract

This publication provides guidelines for applying the Risk Management Framework (RMF) to information systems and organizations. The RMF includes a disciplined, structured, and flexible process for organizational asset valuation; security and privacy control selection, implementation, and assessment; system and control authorizations; and continuous monitoring. It also includes enterprise-level activities to help better prepare organizations to execute the RMF at the system level. The RMF promotes the concept of near real-time risk management and ongoing system authorization through the implementation of continuous monitoring processes; provides senior leaders and executives with the necessary information to make cost-effective, risk management decisions about the systems supporting their missions and business functions; and integrates security and privacy controls into the system development life cycle. Applying the RMF tasks enterprise-wide helps to link essential risk management processes at the system level to risk management processes at the organization level. In addition, it establishes responsibility and accountability for the security and privacy controls deployed within organizational systems and inherited by those systems. The RMF incorporates concepts from the Framework for Improving Critical Infrastructure Cybersecurity that complement the currently established risk management processes mandated by the Office of Management and Budget and the Federal Information Security Modernization Act.

Keywords

assess; authorization to operate; common control authorization; authorization to use; authorizing official; categorize; common control; common control provider; continuous monitoring; hybrid control; implement; information owner/steward; monitor; ongoing authorization; plan of action and milestones; privacy assessment report; privacy control; privacy plan; risk; risk assessment; risk executive function; risk management; risk management framework; threat intelligence; threat modelling; security assessment report; security control; security plan; senior agency information security officer; senior agency official for privacy; system development life cycle; system owner; system privacy officer; system security officer.

Acknowledgements

This publication was developed by the *Joint Task Force* Interagency Working Group. The group includes representatives from the Civil, Defense, and Intelligence Communities. The National Institute of Standards and Technology wishes to acknowledge and thank the senior leaders from the Departments of Commerce and Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency working group whose dedicated efforts contributed significantly to the publication.

Department of Defense

John A. Zangardi
Acting DoD Chief Information Officer

Thomas P. Michelli
Acting Principal Deputy and DoD Chief Information Officer

Essye B. Miller
Deputy Chief Information Officer for Cybersecurity and DoD Senior Information Security Officer

John R. Mills
Director, Cybersecurity Policy, Strategy, and International

Office of the Director of National Intelligence

John Sherman
Assistant DNI and Chief Information Officer

Sally Holcomb
Deputy Chief Information Officer

Sue Dorr
Director, Information Assurance Division and Chief Information Security Officer

Wallace Coggins
Director, Security Coordination Center

National Institute of Standards and Technology

Charles H. Romine
Director, Information Technology Laboratory

Donna Dodson
Cybersecurity Advisor, Information Technology Laboratory

Matt Scholl
Chief, Computer Security Division

Kevin Stine
Chief, Applied Cybersecurity Division

Ron Ross
FISMA Implementation Project Leader

Committee on National Security Systems

Essye B. Miller
Chair

Cheryl Peace
Co-Chair

Kevin Dulany
Tri-Chair—Defense Community

Peter H. Duspiva
Tri-Chair—Intelligence Community

Daniel Dister
Tri-Chair—Civil Agencies

Joint Task Force Interagency Working Group

Ron Ross
NIST, JTF Leader

Kevin Dulany
Department of Defense

Peter Duspiva
Intelligence Community

Kelley Dempsey
NIST

Taylor Roberts
OMB

Ellen Nadeau
NIST

Victoria Pillitteri
NIST

Naomi Lefkovitz
NIST

Jordan Burris
OMB

Charles Cutshall
OMB

Jeff Marron
NIST

Chris Enloe
NIST

Jennifer Fabius
The MITRE Corporation

Carol Bales
OMB

A special note of thanks goes to Jim Foti and Elizabeth Lennon for their technical editing and administrative support. The authors also wish to recognize Kaitlin Boeckl, Jon Boyens, Kathleen Coupe, Jeff Eisensmith, Ned Goren, Matthew Halstead, Kevin Herms, Jody Jacobs, Ralph Jones, Martin Kihiko, Raquel Leone, Kirsten Moncada, Celia Paulsen, and the research staff from the NIST Computer Security and Applied Cybersecurity Divisions for their exceptional contributions in helping to improve the content of the publication.

Finally, the authors also gratefully acknowledge the significant contributions from individuals and organizations in both the public and private sectors, nationally and internationally, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

Historical Contributions to NIST Special Publication 800-37

The authors acknowledge the many individuals who contributed to previous versions of Special Publication 800-37 since its inception in 2005. They include Marshall Abrams, William Barker, Beckie Bolton, Roger Caslow, Dominic Cussatt, Priscilla Guthrie, Gus Guissanie, Sherrill Nicely, Mark Morrison, Cita Furlani, Eustace King, William Hunteman, Gary Stoneburner, Peggy Himes, Arnold Johnson, Cheryl Roby, Marianne Swanson, Elizabeth Lennon, Dorian Pappas, Christian Enloe, John Streufert, Stuart Katzke, Peter Williams, Peter Gouldmann, John Gilligan, Richard Graubart, Esten Porter, Karen Quigg, George Rogers, and Glenda Turner.

Notes to Reviewers

As we push computers to "the edge" building an increasingly complex world of interconnected systems and devices, security and privacy continue to dominate the national conversation. The Defense Science Board in its 2017 report, *Task Force on Cyber Defense*, provides a sobering assessment of the current vulnerabilities in the U.S. critical infrastructure and the systems that support the mission-essential operations and assets in the public and private sectors.

> *"…The Task Force notes that the cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries. It is clear that a more proactive and systematic approach to U.S. cyber deterrence is urgently needed…"*

There is an urgent need to further strengthen the underlying information systems, component products, and services that we depend on in every sector of the critical infrastructure—ensuring that those systems, products, and services are sufficiently trustworthy throughout the system development life cycle and provide the necessary resilience to support the economic and national security interests of the United States. System modernization, the aggressive use of automation, and the consolidation, standardization, and optimization of federal systems and networks to strengthen the protection for high-value assets, are key objectives for the federal government.

This update to NIST Special Publication 800-37 (Revision 2) responds to the call by the Defense Science Board, the President's Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, and the Office of Management and Budget Memorandum M-17-25 (implementation guidance for the Cybersecurity Executive Order) to develop the next-generation Risk Management Framework (RMF) for systems and organizations.

There are four major objectives for this update—

- To provide closer linkage and communication between the risk management processes and activities at the C-suite level of the organization and the processes and activities at the system and operational level of the organization;
- To institutionalize critical enterprise-wide risk management preparatory activities to facilitate a more efficient and cost-effective execution of the Risk Management Framework at the system and operational level;
- To demonstrate how the Cybersecurity Framework can be implemented using the established NIST risk management processes (i.e., developing a Federal use case); and
- To provide an integration of privacy concepts into the Risk Management Framework and support the use of the consolidated security and privacy control catalog in NIST Special Publication 800-53, Revision 5.

The addition of the *organizational preparation* step is one of the key changes to the RMF—incorporated to achieve more effective, efficient, and cost-effective risk management processes. The primary objectives for institutionalizing organizational preparation are as follows:

- To facilitate better communication between senior leaders and executives at the enterprise and mission/business process levels and system owners—conveying acceptable limits regarding the implementation of security and privacy controls within the established organizational risk tolerance;

- To facilitate organization-wide identification of common controls and the development of organization-wide tailored security and privacy control baselines, to reduce the workload on individual system owners and the cost of system development and protection;
- To reduce the complexity of the IT infrastructure by consolidating, standardizing, and optimizing systems, applications, and services through the application of enterprise architecture concepts and models; and
- To identify, prioritize, and focus resources on high-value assets and high-impact systems that require increased levels of protection—taking steps commensurate with risk such as moving lower-impact systems to cloud or shared services, systems, and applications.

Recognizing that organizational preparation for RMF execution may vary from organization to organization, achieving the objectives outlined above can significantly reduce the information technology footprint and attack surface of organizations, promote IT modernization objectives, conserve security resources, prioritize security activities to focus protection strategies on the most critical assets and systems, and promote privacy protections for individuals.

This draft is intended to promote discussion on the new organizational preparation step and the other innovations introduced in RMF 2.0—including how these changes work to achieve the primary objectives stated above. After the discussion draft, NIST anticipates publishing an initial public draft in November 2017, a final draft in January 2018, and the final publication in March 2018.

- **RON ROSS**
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

COMMON SECURITY FOUNDATIONS

In developing standards and guidelines required by FISMA, NIST consults with federal agencies, state, local, and tribal governments, and private sector organizations to improve information security; avoid unnecessary and costly duplication of effort; and ensure that its publications are complementary with the standards and guidelines used for the protection of national security systems. In addition to a comprehensive and transparent public review and vetting process, NIST is engaged in a collaborative partnership with the Office of the Director of National Intelligence, Department of Defense, and Committee on National Security Systems, and has established a risk management framework for the federal government. This common foundation for security provides the Civil, Defense, and Intelligence Communities of the federal government and their contractors, more cost-effective, flexible, and consistent methods to manage security risks to organizational operations and assets, individuals, other organizations, and the Nation. The unified framework also provides a strong basis for reciprocal acceptance of authorization decisions and facilitates information sharing and collaboration. NIST continues to work with both public and private sector entities to establish mappings and relationships between its information security standards and guidelines and those developed by external organizations.

MANAGING INFORMATION SECURITY RISK

Using the Cybersecurity Framework

Executive Order (E.O.) 13800 requires federal agencies to modernize their IT infrastructure and systems, and recognizes the increasing interconnectedness of federal information systems and networks. The E.O. also requires agency heads to manage risk at the agency level and across the Executive Branch using the Framework for Improving Critical Infrastructure Cybersecurity (also known as the Cybersecurity Framework) developed by NIST. And finally, the E.O. reinforces the Federal Information Security Modernization Act (FISMA) of 2014 by holding agency heads accountable for managing the cybersecurity risk to their enterprises.

The Cybersecurity Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Therefore, consistent with OMB Memorandum M-17-25, the federal implementation of the Cybersecurity Framework will employ the risk management processes defined in NIST Special Publications 800-39 and 800-37. This will allow agencies to meet their concurrent obligations to comply with the requirements of FISMA and E.O. 13800.

To ensure an effective and efficient transition to Cybersecurity Framework implementation, the Risk Management Framework (RMF) has been modified in this update in several key areas. The federal implementation of the Cybersecurity Framework will focus on—

- the ***preconditions*** and essential activities necessary to prepare for the enterprise-wide execution of the RMF and the conduct of the associated risk management actions at the information system level; and
- the ***postconditions*** and essential activities necessary to report the findings and risk-based decisions of authorizing officials for information systems and common controls to agency heads and the senior leaders in the Executive Branch.

Each task in the RMF includes references to applicable sections of the Cybersecurity Framework. For example, Organizational Preparation, Task 2, *Risk Management Strategy*, provides a direct linkage to the Cybersecurity Framework Core [Identify Function]; Organizational Preparation, Task 10, *Organization-Wide Tailored Control Baselines and Profiles*, aligns with the construct of Cybersecurity Framework Profiles; and Authorization, Task 6, *Authorization Reporting*, and Task 5, *Security Status Reporting*, support OMB risk management and status reporting requirements using the Cybersecurity Framework functions, categories, and subcategories. A mapping of Cybersecurity Framework Subcategories to the NIST Special Publication 800-53 security controls is available at: https://www.nist.gov/file/372651.

In summary, the federal implementation of the Cybersecurity Framework will provide agencies with a holistic and seamless method to *prepare* for cybersecurity risk management; the ability to use the RMF to select, implement, assess, and continuously monitor security controls to protect federal information systems and organizations; and an effective method to *report* and *communicate* risk-based information and risk-related decisions to officials at all levels of the federal government. Such preparation, execution, and communication can help agencies take maximum advantage of the Cybersecurity Framework and the underlying risk management processes provided by the RMF at the execution level to help achieve more consistent and cost-effective security solutions.

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED FOR INFORMATION SECURITY, PRIVACY, AND MANAGING RISK

Organizations depend on information systems[1] to successfully carry out their missions and business functions. Information and systems are subject to serious threats that can have adverse impacts on organizational operations[2] and assets, individuals, other organizations, and the Nation.[3] Such adverse impacts occur by compromising the confidentiality, integrity, or availability of information being processed, stored, or transmitted by those systems. Threats to organizational information and information systems include environmental disruptions, human or machine errors, and purposeful attacks. Attacks on systems are often disciplined, well-organized, well-funded, and in a growing number of cases, very sophisticated. Successful attacks on public and private sector information systems can result in serious or catastrophic damage to the national and economic security interests of the United States.

In addition to security concerns, privacy concerns also pose significant risk to individuals that reflect upon organizations and that can impact the national and economic interests of the United States. While security and privacy have complementary objectives with respect to managing the confidentiality, integrity, and availability of personally identifiable information, individual privacy cannot be achieved solely by securing personally identifiable information.[4] Thus, it is important that organizations comprehend the full scope of privacy concerns in the operation of their information systems.[5] Given the significant and ever-increasing danger of these threats and concerns, it is imperative that the leaders and managers at all organizational levels understand their responsibilities and are accountable for protecting organizational assets and for managing security and privacy risks.[6]

1.1 BACKGROUND

NIST in its partnership with the Department of Defense, the Office of the Director of National Intelligence, and the Committee on National Security Systems, developed a *Risk Management*

[1] An *information system* is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [See 44 U.S.C., Sec. 3502]. The term information system includes, for example, general- purpose computing systems; industrial and process controls systems; cyber-physical systems; weapons systems; super computers; command, control, and communications systems; environmental control systems; small form factor devices such as smart phones and tablets; and embedded devices and sensors.

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

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

[4] OMB Circular A-130 defines personally identifiable information (PII) as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Privacy concerns in systems arise from the authorized processing of PII as well as unauthorized access to PII. For example, existing information security guidance does not address the consequences of a poor consent mechanism for use of PII or the lack of transparency of PII processing such as what PII is being collected, or which changes in use of PII are permitted so long as authorized personnel are conducting the activity.

[5] NIST Interagency Report 8062 introduces the concepts of privacy engineering and privacy risk management and provides a privacy risk model that can be used to assess privacy risk arising from the authorized processing of PII in information systems.

[6] Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event. Risk is also a function of the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence. Types of risk include program risk; compliance/regulatory risk; financial risk; legal risk; mission/business risk; political risk; security risk; privacy risk; project risk; reputational risk; safety risk; strategic planning risk; and supply chain risk.

Framework (RMF) to improve information security, strengthen risk management processes, and encourage reciprocity among organizations. In July 2016, the Office of Management and Budget (OMB) revised Circular A-130 to require federal agencies to apply the RMF within their privacy programs.[7] The RMF emphasizes managing risk by building security and privacy capabilities into systems through the application of security and privacy controls; maintaining awareness of the security and privacy state of systems on an ongoing basis though enhanced monitoring processes; and providing essential information to senior leaders and executives to facilitate their decisions regarding the acceptance of risk to organizational operations, organizational assets, individuals, other organizations, and the Nation arising from the operation and use of systems. The RMF:

- Provides a repeatable process designed to promote the protection of information and information systems commensurate with risk;
- Emphasizes organization-wide preparation necessary to manage security and privacy risks;
- Facilitates the categorization of information and systems; the selection, implementation, assessment, and monitoring of security and privacy controls; and the authorization of information systems and common controls;
- Promotes the concept of near real-time risk management and ongoing system and control authorization through the implementation of robust continuous monitoring processes;
- Encourages the use of automation to provide senior leaders with the necessary information to make cost-effective, risk-based decisions for information systems supporting their missions and business functions;
- Facilitates the integration of security and privacy controls into the enterprise architecture, system development life cycle, acquisition processes, and systems engineering processes;
- Connects risk management processes at the organization and mission/business process levels to risk management processes at the information system level via a risk executive (function);[8] and
- Establishes responsibility and accountability for security and privacy controls implemented within information systems and inherited by those systems.

The RMF provides a dynamic and flexible approach to effectively manage information security and privacy risks in diverse environments of complex and sophisticated threats, privacy concerns, changing missions, and system vulnerabilities.

1.2 PURPOSE AND APPLICABILITY

This publication provides guidelines for applying the RMF to information systems and organizations. The guidelines have been developed:

- To ensure that managing system-related security and privacy risk is consistent with the mission and business objectives of the organization and the risk management strategy established by the senior leadership through the risk executive (function);
- To achieve adequate security for organizational information and information systems through the implementation of appropriate risk response strategies;

[7] Office of Management and Budget Circular A-130, "Managing Federal Information as a Strategic Resource" (2016).

[8] OMB Memorandum M-17-25 defines a key organizational role of senior accountable official for risk management.

- To ensure that security and privacy requirements and controls are effectively integrated into the enterprise architecture, system development life cycle processes, acquisition processes, and systems engineering processes;[9]
- To support consistent, informed, and ongoing authorization decisions (through continuous monitoring),[10] transparency and traceability of security- and privacy-related information, and reciprocity;[11] and
- To facilitate the implementation of the Framework for Improving Critical Infrastructure Cybersecurity.[12]

This publication is intended to help organizations manage risk and to satisfy the security and privacy requirements in FISMA, the Privacy Act of 1974, OMB policies (e.g., OMB Circular A-130), and designated Federal Information Processing Standards, among others. The guidelines have been developed from a technical perspective to complement similar guidelines for national security systems and may be used for such systems with the approval of appropriate federal officials with policy authority over such systems. State, local, and tribal governments, as well as private sector organizations are encouraged to use these guidelines, as appropriate.

1.3 TARGET AUDIENCE

This publication serves individuals associated with the design, development, implementation, assessment, operation, maintenance, and disposition of systems including:

- Individuals with mission or business ownership responsibilities or fiduciary responsibilities including, for example, heads of federal agencies and chief executive officers;
- Individuals with information system development and acquisition responsibilities, including, for example, program managers, procurement officials, component product and system developers, systems integrators, and enterprise architects;
- Individuals with information system, security, or privacy management and/or oversight responsibilities including, for example, senior leaders, risk executives, authorizing officials, privacy officials, chief information officers, senior agency information security officers, and senior agency officials for privacy;
- Individuals with security or privacy assessment and information system monitoring responsibilities including, for example, system evaluators, security or privacy control assessors, auditors, and system owners; and
- Individuals with security or privacy implementation and operational responsibilities, for example, system owners, common control providers, information owners/stewards, mission or business owners, security or privacy architects, and systems security or privacy engineers.

[9] NIST Special Publication 800-160 provides guidance and considerations for a multidisciplinary approach in the engineering of trustworthy secure systems as part of the system development life cycle process.

[10] NIST Special Publication 800-137 provides guidance on information security continuous monitoring programs. Future updates to this publication will also address privacy continuous monitoring.

[11] *Reciprocity* is an agreement among participating organizations to accept each other's security and privacy assessment results to reuse system resources or to accept each other's assessed security and privacy posture to share information. Reciprocity does not apply to accepting the risk-based decisions of other organizations.

[12] See Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Draft NIST Interagency Report 8170 provides Cybersecurity Framework implementation guidance for federal agencies.

1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the concepts associated with managing system-related security and privacy risk including the establishment of a system-of-interest and the associated system elements; employment of an organization-wide view of risk management and the application of the RMF; the relationship between security and privacy and the integration of privacy into the RMF; and the allocation of security and privacy controls to systems and organizations as system-specific, hybrid, and common controls.
- **Chapter Three** describes the tasks required to implement the steps in the RMF including: organizational preparation; categorization of information and information systems; security and privacy control selection and implementation; assessment of the effectiveness of controls; system and common control authorization; and the ongoing monitoring of controls and the security and privacy state of the information system and organization.
- **Supporting Appendices** provide information and guidance for the application of the RMF including: roles and responsibilities; summary of tasks; information system and common control authorizations; and other considerations affecting RMF implementation.

CHAPTER TWO

THE FUNDAMENTALS

MANAGING SYSTEM-RELATED SECURITY AND PRIVACY RISKS IN ORGANIZATIONS

This chapter describes the basic concepts associated with managing system-related security and privacy risks in organizations. These concepts include the system-of-interest, system elements, and how system boundaries are established; risk management principles and best practices employed in organization-wide strategic planning; security and privacy considerations in system development life cycle processes; and security and privacy risk management practices and considerations associated with the supply chain. Although the above concepts are discussed independently, there is a relationship among the concepts. Successful security, privacy, and risk management programs depend on a holistic application of these concepts to ensure that there is a high degree of transparency and traceability of every programmatic element. Such transparency and traceability promote a level of trust needed by senior leaders and executives to understand and accept the security and privacy risks to organizational operations and organizational assets, individuals, other organizations, and the Nation.

2.1 SYSTEM AND SYSTEM ELEMENTS

While this publication uses the definition of *information system* in Chapter One as the primary focus for RMF execution, it is also important to be able to describe systems in the context of the system development life cycle and how security and privacy capabilities are implemented within the basic components of those systems. Therefore, the basic definition of information system is extended to provide a contextual relationship and linkage to the architectural and engineering concepts that allow security and privacy issues to be addressed early in and throughout the life cycle and at the appropriate level of detail to help ensure that such capabilities are achieved. ISO/IEC/IEEE 15288 provides the architectural and engineering view of an information system and the entities that the system interacts with in its environment of operation.

ISO/IEC/IEEE 15288 defines a *system* as a set of interacting elements organized to achieve one or more stated purposes.[13] Each of the *system elements* within the system is implemented to fulfill specified requirements. System elements can include technology or machine elements; human elements; and physical or environmental elements. Thus, system elements may be implemented via hardware, software, or firmware;[14] physical structures or devices; or people, processes, and procedures. Individual system elements or a combination of system elements may satisfy stated system requirements. Interconnections between system elements allow the elements to interact as necessary to produce a capability as specified by the requirements. Finally, every system operates within an environment that influences the system and its operation.

For a large or complex system, a system element may be regarded as a system and composed of system elements. This hierarchical and context-dependent nature of the terms system and system element allows the term system to be used when referring to a discrete component or a complex, geographically distributed system-of-systems. Because the term system can be applied across a continuum from composed elements to a discrete element, the context within which the term

[13] This definition of *system* is consistent with the definition of information system in 44 U.S.C., Sec. 3502—that is, an information system is a discrete set of information resources (or system elements), organized for the express purpose of the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[14] The term *system component* represents a subset of system elements addressing hardware, software, or firmware.

system is being used must be communicated and understood. Distinguishing context is important because one observer's system may be another observer's system element. Building on the terms system and system element, the term *system-of-interest* defines the set of system elements, system element interconnections, and the environment that provides the focus for the system boundary determination[15] and the RMF implementation. The system-of-interest may be supported by one or more *enabling systems* that provide support to the system life cycle activities associated with the system-of-interest. Enabling systems are not necessarily delivered with the system-of-interest and do not necessarily exist in the operational environment of the system of interest. Finally, there are *other systems* the system-of-interest interacts with in the operational environment. These systems may provide services to the system-of-interest or may be the beneficiaries of services provided by the system-of-interest (i.e., potential two-way dependencies). Table 1 lists the system-related constructs that are foundational to RMF implementation.

TABLE 1: FOUNDATIONAL SYSTEM-RELATED CONSTRUCTS

SYSTEM	Combination of interacting elements organized to achieve one or more stated purposes. *Examples include: general and special-purpose information systems; industrial/process control systems; weapons systems; medical devices and treatment systems; social networking systems; and financial, banking, and merchandising transaction systems.*
SYSTEM ELEMENT	Member of a set of elements that constitute a system. *Examples include: hardware; software; firmware; data; facilities; materials; humans; processes; and procedures.*
SYSTEM-OF-INTEREST	System that is the focus of the systems engineering effort. *Defines the information system that is the focus of the RMF implementation and the authorization boundary for the system.*
ENABLING SYSTEM	System that supports a system-of-interest during any of its life cycle stages but does not necessarily contribute directly to its function during operation. *Examples include: modeling, simulation, and design tools; test scenario generators and test harnesses; training system and tools; software and firmware compilers; hardware design tools, and fabrication and manufacturing systems.*
OTHER SYSTEM	System that interacts with the system-of-interest in its operational environment. *Examples include: a global positioning system space vehicle being an "other system" interacting with a GPS receiver as the "system-of-interest."*
Source: *ISO/IEC/IEEE 15288: 2015*	

The conceptual view of the system-of-interest promotes the transparency and traceability needed in defining the system requirements, architecture, and design—thus facilitating an increased level of trustworthiness in those systems to assure the resilience of critical organizational missions and business functions. This requires a fundamental understanding of security and privacy risk at the organization level—and is achieved through an end-to-end analysis of the operating environment and associated system interconnections and dependencies; by analyzing the degree of dependency among systems and system elements to identify the potential risk of cascading effects if a system is compromised; and by reducing the attack surface to minimize cascading impacts and to build system resilience.

[15] NIST Special Publication 800-18 provides guidance on system boundary determination. Future updates to this publication will also address privacy considerations for system boundary determination.

Figure 1 illustrates the conceptual view of the system-of-interest and the relationships among systems, systems elements, and the environment of operation.

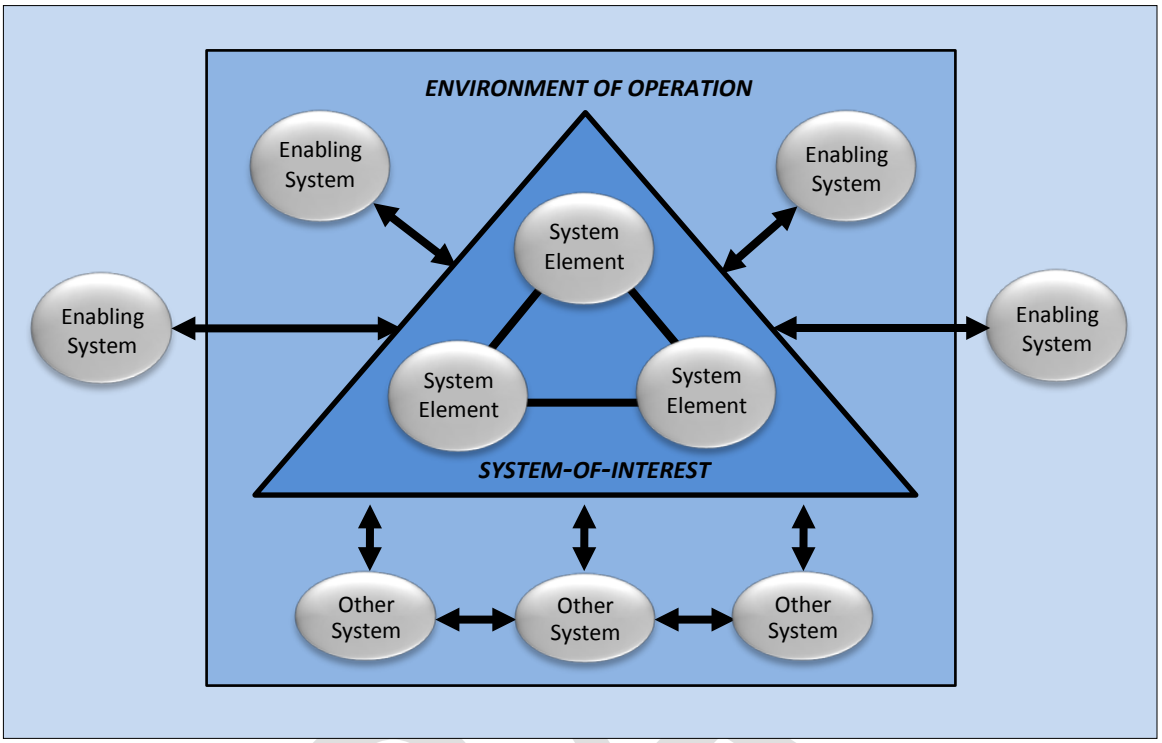

FIGURE 1: CONCEPTUAL VIEW OF THE SYSTEM-OF-INTEREST

The RMF, including the authorization process, is applied to systems-of-interest, not individual system elements. Organizations can employ "component-level" assessments for individual system elements[16] and can take advantage of the assessment results and evidence generated during that process to support risk-based decision making for the system. It is important to apply the RMF in the right circumstances and at the right level of system granularity.

2.2 ORGANIZATION-WIDE RISK MANAGEMENT

Managing system-related security and privacy risks is a complex, multifaceted undertaking that requires the involvement of the entire organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing projects, to individuals developing, implementing, operating, and maintaining the systems supporting the organization's missions and business functions. Risk management must be a holistic activity that is fully integrated into every aspect of the organization including the mission and business planning activities, the enterprise architecture, the system development life cycle processes, and the systems engineering activities that are integral to those system life cycle processes. Security and privacy requirements, key elements of risk management, must be clearly articulated and seamlesslessly communicated to each organizational entity to help ensure mission and business success.

[16] For example, the evaluation program established under ISO/IEC 15408 (Common Criteria) provides independent component-level assessments for IT products.

Figure 2 illustrates a three-level approach to risk management that addresses risk-related concerns at the *organization* level, the *mission/business process* level, and the information *system* level.[17]

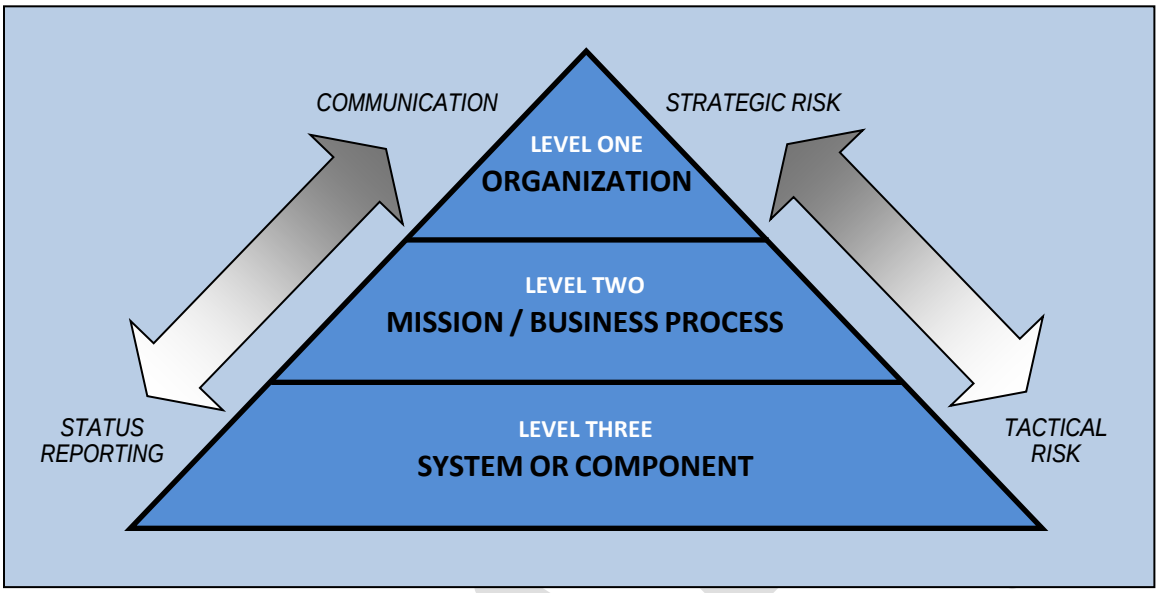

FIGURE 2: ORGANIZATION-WIDE RISK MANAGEMENT APPROACH

The activities conducted at Levels 1 and 2 are critical to preparing the organization to execute the RMF. Such preparation involves a wide range of activities that go well beyond security-related activities but are essential to achieving adequate security for the organization and managing risk appropriately.[18] In organizations that depend on information technology for their mission/business success, security and privacy decisions cannot be made in isolation—rather, such decisions are closely linked to decisions regarding the mission and business objectives of the organization; the modernization of information systems, components, and services to adopt new and innovative technologies; the enterprise architecture and the need to manage and reduce the complexity of systems through consolidation, optimization, and standardization (i.e., reducing the attack surface and technology footprint exploitable by adversaries);[19] and the allocation of resources to ensure the organization can conduct its missions and business operations with a high degree of effectiveness, efficiency, and cost-effectiveness.

Preparing the organization for a successful execution of the RMF at the information system level can include, for example, assigning key roles and responsibilities for risk management processes; establishing a risk management strategy and risk tolerance for the organization; identifying the missions, business functions, and mission/business processes the information system is intended to support; identifying key stakeholders (both internal and external to the organization) having a security or privacy interest in the information system; identifying and prioritizing stakeholder assets; understanding threats to systems and organizations; conducting an initial risk assessment;

[17] NIST Special Publication 800-39 provides guidance on organization-wide risk management.

[18] NIST Interagency Report 8170 provides guidance for organizational preparation using the Cybersecurity Framework.

[19] *Enterprise architecture* is a strategic information asset base, which defines the mission; the information and the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs. Enterprise architecture includes a baseline architecture, target architecture, and sequencing plan. The Common Approach to Federal Enterprise Architecture and Federal Enterprise Architecture Framework provide guidance for implementing enterprise architectures.

identifying and prioritizing stakeholder protection needs and security and privacy requirements;[20] determining information system and authorization boundaries; defining information systems in terms of the enterprise architecture; developing security and privacy architectures that include common controls suitable for inheritance by organizational systems; and allocating security and privacy requirements to individual systems and the environments in which those systems operate.

In contrast to the Level 1 and 2 activities that prepare the organization for RMF implementation, Level 3 addresses risk from a *system* perspective and is guided and informed by the risk decisions at the enterprise and mission/business process levels. Risk decisions at Levels 1 and 2 impact the selection and implementation of security and privacy controls at the system level. Security and privacy requirements are satisfied by the selection and implementation of security and privacy controls from NIST Special Publication 800-53. The controls are allocated to the system elements as system-specific, hybrid, or common controls in accordance with the enterprise architecture, security or privacy architecture, and any tailored control baselines or overlays developed by the organization.[21] Security and privacy controls are *traceable* respectively to the security and privacy requirements established by the organization to ensure that there is *transparency* in the development of security and privacy solutions and the requirements are fully addressed during design, development, implementation, and sustainment of the system.

Without adequate risk management preparation at the organizational level, security and privacy activities can become too costly, demand too many skilled security and privacy professionals, and produce ineffective solutions. For example, organizations that fail to define and implement an effective enterprise architecture strategy will not be able to consolidate, optimize, and standardize the information technology infrastructure—resulting in unnecessary redundancy and inefficient and costly systems, applications, and services. The effect of ill-conceived architectural and design decisions can produce a cost-multiplier effect downstream that adversely impacts the ability of the organization to implement effective security and privacy solutions. Since information systems have an initial investment cost, maintenance costs throughout the life cycle, initial authorization costs, and ongoing authorization costs, transitioning to shared or cloud-based systems, services, or applications can significantly reduce the overall cost of ownership. This can provide additional resources to protect the organization's high-value assets and simultaneously increase the overall efficiency and the effectiveness of the organization.

The RMF provides a structured and flexible process that integrates security and privacy activities into the system development life cycle. The RMF operates at all levels in the risk management hierarchy illustrated in Figure 2. There are six main steps in the RMF and a preparatory step to ensure that organizations are ready to execute the process. The steps are:

- ***Prepare*** the organization to execute the RMF by considering a variety of organizational inputs that establish the context for managing security and privacy risk for the system-of-interest.
- ***Categorize*** the system and the information processed, stored, and transmitted by the system based on an impact analysis.
- ***Select*** an initial set of baseline security and privacy controls for the system and tailor the control baseline as needed based on an organizational assessment of risk and local conditions.

[20] Security and privacy requirements can be obtained from a variety of sources including, for example, laws, Executive Orders, directives, regulations, policies, standards, guidelines, and mission/business/operational requirements.

[21] Security and privacy controls can be allocated at all three levels in the risk management hierarchy. For example, common controls may be allocated at the organization, mission/business process, or information system level.

- ***Implement*** the security and privacy controls and describe how the controls are employed within the system and its environment of operation.
- ***Assess*** the security and privacy controls 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 and privacy requirements for the system and enforcing security and privacy policy.
- ***Authorize*** the system or common controls based on a determination of risk to organizational operations and assets, individuals, other organizations, and the Nation and the decision that this risk is acceptable.
- ***Monitor*** the system and the associated security and privacy controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting security and privacy impact analyses, and reporting the security and privacy state of the system.

Figure 3 illustrates the steps in the RMF. Chapter Three provides a detailed description of each of the tasks necessary to carry out the steps in the RMF. References to the Cybersecurity Framework are indicated in the RMF tasks, where appropriate. The steps in the RMF can also be aligned with the systems security engineering processes defined in NIST Special Publication 800-160.

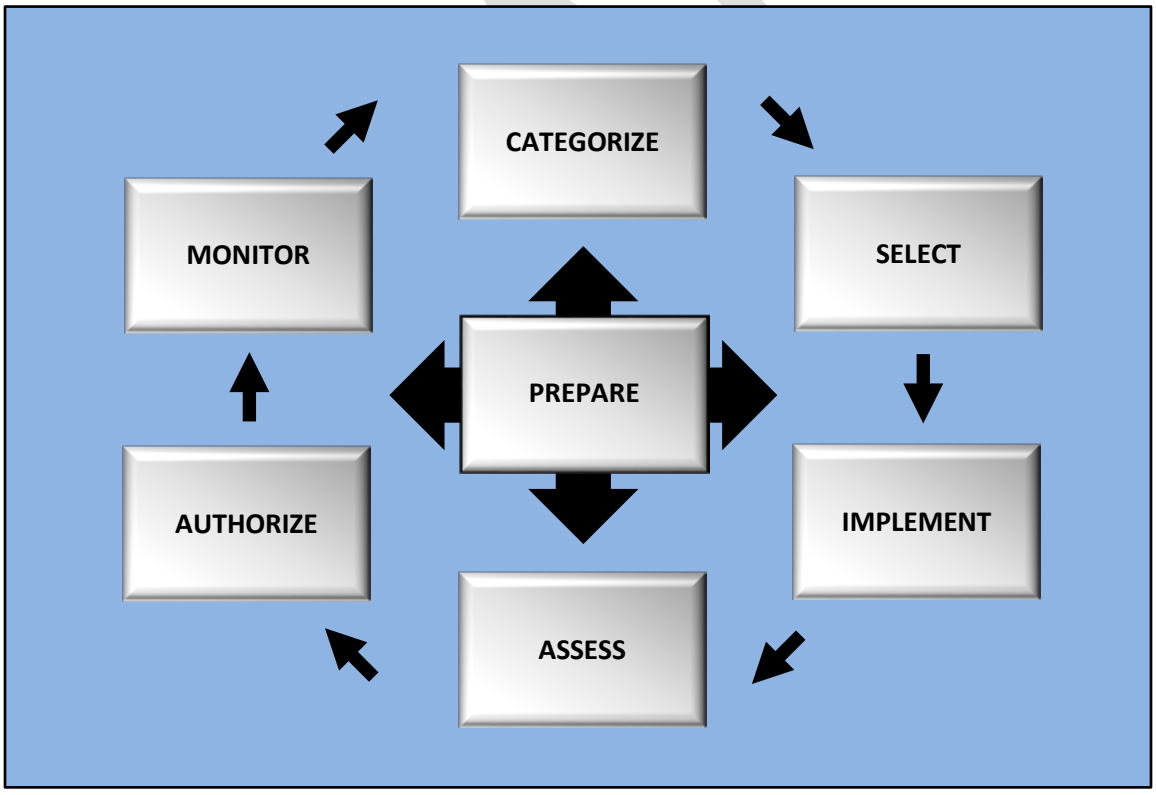

FIGURE 3: RISK MANAGEMENT FRAMEWORK

While the RMF steps are listed in sequential order above, they can be carried out in any order. Organizations executing the RMF for the first time, will typically carry out the steps in sequential order, although they may choose to revisit certain steps during initial execution. Once the system

is in the operations and maintenance phase of the system development life cycle as part of the continuous monitoring step, events may dictate nonsequential execution.

Although the risk management approach in Figure 2 is conveyed as hierarchical, project and organization dynamics are typically more complex. The risk management approach selected by an organization may vary on a continuum from top-down command to decentralized consensus among peers. However, in all cases, organizations must have a consistent and effective approach that is applied to risk management processes from the *organization* level to the *system* level. It is imperative that organizational officials identify and secure the needed resources to complete the risk management tasks described in this publication and ensure that those resources are made available to the appropriate personnel. Resource allocation includes funding to conduct risk management tasks and assigning qualified personnel needed to accomplish the tasks.

2.3 SECURITY AND PRIVACY RELATIONSHIP

As noted in OMB Circular A-130:[22]

> *"Federal information is a strategic asset subject to risks that must be managed to minimize harm; Protecting an individual's privacy is of utmost importance. The Federal Government shall consider and protect an individual's privacy throughout the information life cycle; While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements."*

Security and privacy have complementary and mutually-reinforcing objectives with respect to managing the confidentiality, integrity, and availability of personally identifiable information (PII), but individual privacy cannot be achieved solely by securing PII. Figure 4 demonstrates the overlap in objectives, and also shows that privacy risks can arise as a by-product of authorized or intentional processing of PII.[23]

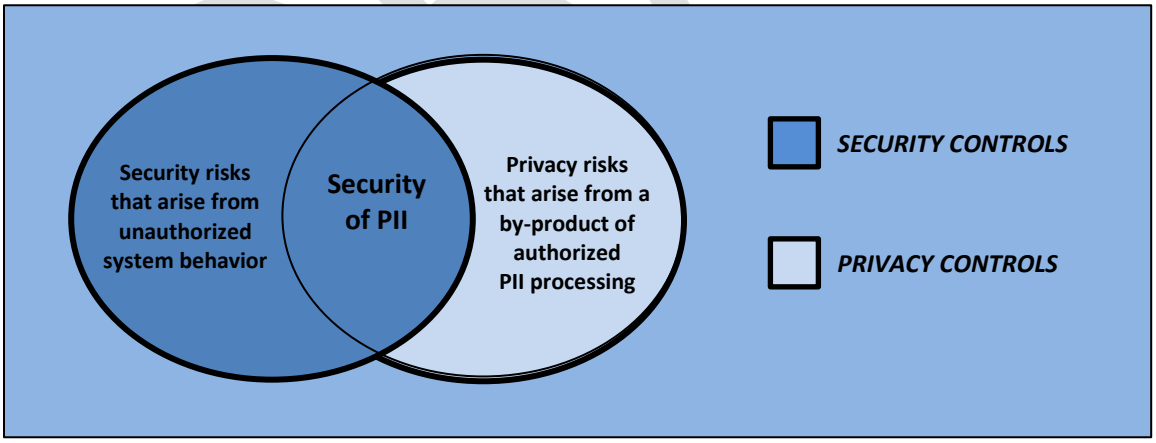

FIGURE 4: RELATIONSHIP BETWEEN SECURITY AND PRIVACY RISKS AND CONTROL SELECTION

[22] Office of Management and Budget Circular A-130, "Managing Federal Information as a Strategic Resource" (2016).

[23] Processing collectively includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII. NIST Interagency Report 8062 includes examples of systems that demonstrate various types of privacy concerns apart from data security breaches. These concerns relate to the ways in which the systems are processing PII and the effects such processing can have on individuals.

Controls for protecting confidentiality, integrity, and availability of information and information resources are defined as security controls.[24] When applied to securing PII, these controls provide privacy protections—however, from an implementation perspective of identifying and selecting controls, these controls are classified as security controls in Figure 4.[25] And for the same purpose of implementation, privacy controls address requirements and risks arising as a by-product of the authorized or intentional processing of PII.

The RMF was developed to strengthen information security and support FISMA requirements. The categorization of information and systems by impact of loss of confidentiality, integrity, and availability is the central construct and starting point for the RMF. However, as illustrated by Figure 4, not all privacy risks arise from the loss of confidentiality, integrity, and availability. Thus, categorizing systems pursuant to FISMA requirements, will not appropriately facilitate the selection of controls to meet privacy requirements and to manage the privacy risks relating to the authorized processing of PII. There are some important factors to consider when using the RMF for privacy. When managing the security risk related to PII, organizations use the entirety of the categorization step. When managing the privacy risk related to the authorized processing of PII, the categorization step is not applicable except for the system boundary determination, security and privacy requirements allocation, and the system description. Figure 5 illustrates how privacy integrates into the RMF.

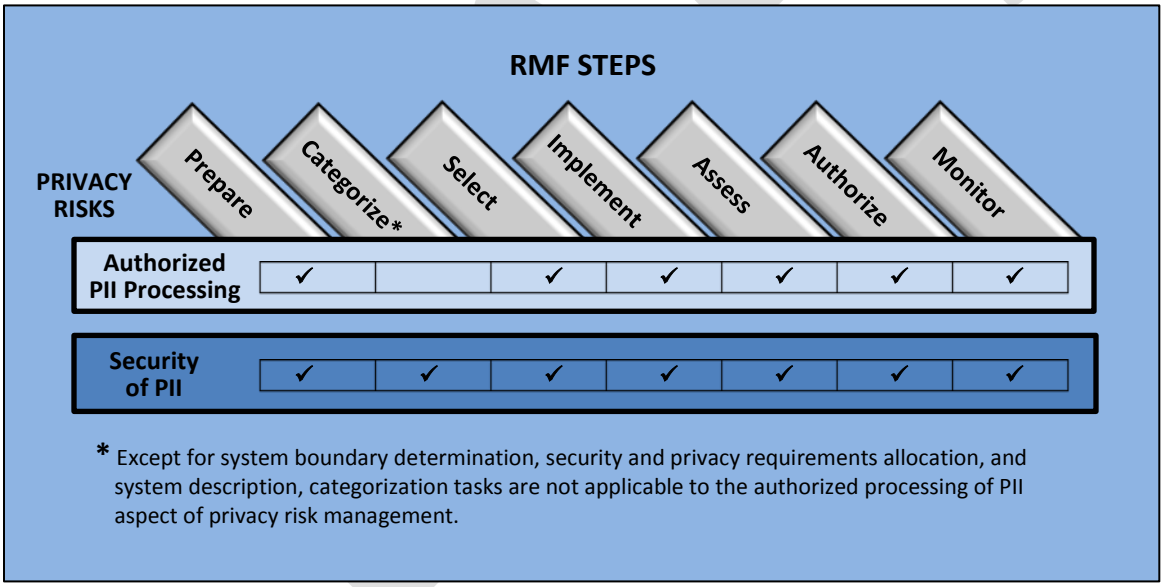

FIGURE 5: PRIVACY INTEGRATION INTO THE RISK MANAGEMENT FRAMEWORK

[24] OMB Circular A-130 defines security controls as "The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information."

[25] OMB Circular A-130 defines privacy controls as "The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks." Thus, controls that address the loss of PII security also can be classified as privacy controls. However, with the limited exception of certain types of controls such as consumer breach response controls (e.g., notifications and individual impact mitigation measures), which would not be used for systems that do not process PII, the controls that can be identified as either security or privacy controls are identical. To further effective communication between privacy and security programs, this publication avoids referring to the same control by multiple names.

RISK MANAGEMENT IN THE SYSTEM DEVELOPMENT LIFE CYCLE

Risk management activities begin early in the system development life cycle and continue throughout the life cycle. These activities are important in helping to shape the security and privacy capabilities of the system; ensuring that security and privacy risks are being adequately addressed on an ongoing basis; and ensuring that authorizing officials fully understand and accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of a defined set of security and privacy controls and the current security and privacy state of the system.

2.4 CONTROL ALLOCATION

There are three types of controls that can be selected and implemented by organizations: system-specific controls (i.e., controls that provide a security and/or privacy capability for a particular system); common controls (i.e., controls that provide a security or privacy capability for multiple systems); or hybrid controls (i.e., controls that have system-specific or common characteristics). Security and privacy controls are *allocated* to a system or to an organization consistent with the organization's enterprise architecture and security or privacy architecture.[26] This activity is carried out as an organization-wide activity that involves authorizing officials, system owners, common control providers, chief information officer, senior agency information security officer, senior agency official for privacy, system security or privacy officers, enterprise architect, security or privacy architect, and risk executive (function).[27]

Organizations are encouraged to identify and implement security and privacy controls that can support multiple systems efficiently and effectively as a common protection capability. When these common controls are used to support a specific system, they are referenced by that system as *inherited controls*. Common controls promote cost-effective, efficient, and consistent security and privacy safeguards across the organization and can also simplify risk management processes and activities. By allocating security and privacy controls to a system as system-specific controls, hybrid controls, or common controls, organizations assign responsibility and accountability to specific organizational entities for the development, implementation, assessment, authorization, and monitoring of those controls. Organizations have significant flexibility in deciding which security and privacy controls from NIST Special Publication 800-53 are appropriate for specific types of allocations.

Security and privacy controls may also be allocated to specific elements within a system. While the control selection process is conducted primarily at the system level, it may not be necessary to implement every control in the tailored baseline on every system element. Organizations can conserve resources by implementing controls only on the specific system elements that require protection or provide a related service.

[26] *Allocation* is the process an organization employs to determine whether controls are system-specific, hybrid, or common and to assign the controls to the specific system elements (i.e., machine, physical, or human components) responsible for providing a security or privacy capability.

[27] Security control allocation also occurs during the system development life cycle process as part of *requirements engineering*. NIST Special Publication 800-160 describes the systems security engineering activities associated with system life cycle processes to achieve trustworthy, secure components, systems, and services.

Figure 6 illustrates control allocation using the RMF to produce risk-related information for senior leaders and executives (including authorizing officials) on the security and privacy state of organizational systems and the mission/business processes supported by those systems.

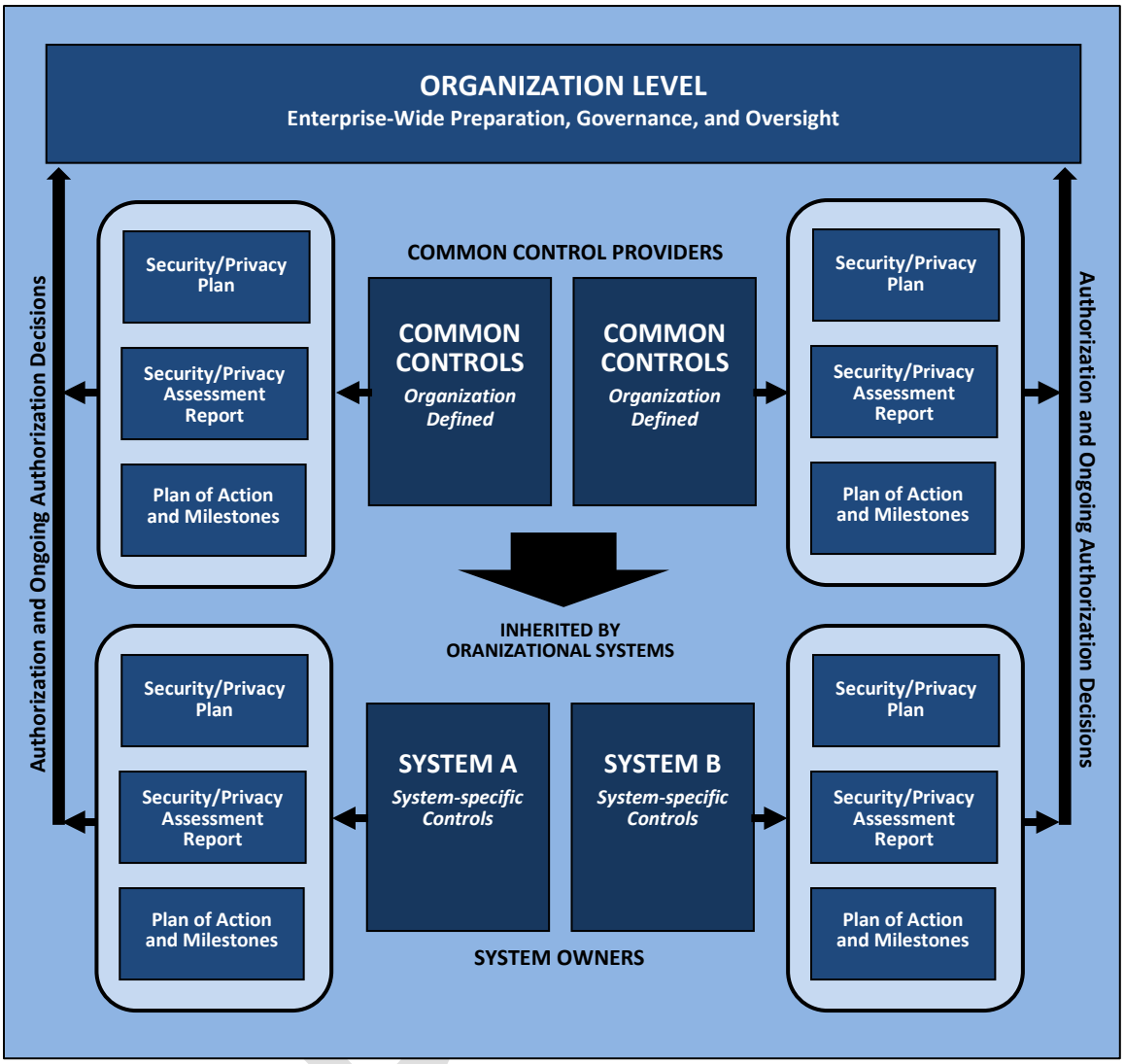

FIGURE 6: ENTERPRISE-WIDE CONTROL ALLOCATION

THE IMPORTANCE OF ARCHITECTURE AND ENGINEERING

Security architects, privacy architects, systems security engineers, and privacy engineers play an essential part in the system development life cycle process and in the successful execution of the RMF. These individuals provide *system owners* and *authorizing officials* with technical advice on the selection and implementation of security and privacy controls in organizational systems—guiding and informing risk-based decisions across the enterprise.

Security and Privacy Architects:

- Ensure that security and privacy requirements necessary to protect mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the systems supporting those missions and business processes.
- Serve as the primary liaison between the enterprise architect and the systems security and privacy engineers.
- Coordinate with system owners, common control providers, and system security and privacy officers on the allocation of security and privacy controls.
- Advise authorizing officials, chief information officers, senior accountable officials for risk management/risk executive (function), senior agency information security officers, and senior agency officials for privacy on a range of security and privacy issues.

Security and Privacy Engineers:

- Capture and refine security and privacy requirements and ensure that the requirements are effectively integrated into the component products and systems through purposeful security or privacy architecting, design, development, and configuration.
- Employ best practices when implementing security or privacy controls within a system including software engineering methodologies; system and security or privacy engineering principles; secure or privacy-enhancing design, secure or privacy-enhancing architecture, and secure or privacy-enhancing coding techniques.
- Coordinate security- and privacy-related activities with senior agency information security officers, senior agency officials for privacy, security and privacy architects, system owners, common control providers, and system security or privacy officers.

CHAPTER THREE

THE PROCESS

EXECUTING THE RISK MANAGEMENT FRAMEWORK TASKS

This chapter describes the process of applying the RMF to systems and organizations. The process includes a set of risk-based tasks that are to be carried out by selected individuals or groups within defined organizational roles.[28] Many risk management roles defined in this publication have counterpart roles defined in the system development life cycle process. Whenever possible, and consistent with missions and business functions, organizations align risk management roles with similar or complementary roles defined for the system development life cycle. RMF tasks are executed concurrently with or as part of the system development life cycle processes in the organization. This helps to ensure that organizations are effectively integrating the process of managing system-related security and privacy risks with their life cycle processes.

Each step in the RMF has a purpose statement, a defined set of outcomes, and a set of tasks that are carried out to achieve those outcomes. Each task contains a set of potential inputs needed to execute the task and a set of potential outputs generated from task execution.[29] In addition, each task describes the phase of the system development life cycle where task execution takes place and the risk management roles and responsibilities associated with the task. Finally, there are references and supplemental guidance to provide organizations with information on how to effectively execute each task.

FLEXIBILITY IN RMF IMPLEMENTATION

Organizations have significant flexibility in developing their security and privacy programs—including the *selection* of baseline security and privacy controls and *tailoring* the controls to meet organizational security and privacy needs. The implementation of common controls and thoughtful control tailoring help to ensure that security and privacy solutions are "rightsized" for the organization's missions, business functions, and operating environments.

The process of implementing RMF tasks may vary from organization to organization. The tasks are applied at appropriate phases in the system development life cycle. While the tasks appear in sequential order, there can be many points in the risk management process that require divergence from the sequential order including the need for iterative cycles between initial task execution and revisiting tasks. For example, security and privacy control assessment results can trigger a set of remediation actions by system owners and common control providers, which can in turn require the reassessment of selected controls. Monitoring security and privacy controls in a system can generate a cycle of tracking changes to the system and its environment of operation; conducting security and privacy impact analyses; taking selected remediation actions, reassessing controls, and reporting the security and privacy status of the system.

[28] Appendix A describes the roles and responsibilities of key participants involved in organizational risk management and the execution of the RMF.

[29] The *potential inputs* for a task may not always be derived from the *potential outputs* from the previous task. This can occur because the RMF steps are not always executed in sequential order—thus, breaking the sequential dependencies.

There may also be other opportunities to diverge from the sequential nature of the tasks when it is more effective, efficient, or cost-effective to do so. For example, while the security and privacy control assessment tasks are listed after the security and privacy control implementation tasks, organizations may choose to begin the assessment of controls as soon as they are implemented but prior to the complete implementation of all controls described in the security and privacy plans. This may result in some organizations assessing the physical and environmental protection controls within a facility prior to assessing the controls employed in the hardware, firmware, or software components of the system (which may be implemented later). Regardless of the task ordering, the final action before a system is placed into operation is the explicit acceptance of risk by the authorizing official.

The RMF steps and the associated tasks can be applied to new development and existing systems. For new and existing systems, organizations ensure that the designated tasks have been completed to adequately prepare for the RMF execution. For existing systems, organizations confirm that the security categorization and (for systems processing personally identifiable information) a privacy risk assessment have been completed and are appropriate; and that the needed controls have been selected and implemented. Applying these steps to existing systems can serve as a gap analysis to determine if adequate security and the required protection, including privacy protections, for the system have been achieved. Any weaknesses or deficiencies in controls can be addressed in the RMF steps addressing implementation, assessment, authorization, and monitoring in the same manner as in new development systems. If no weaknesses or deficiencies are discovered during the gap analysis and there is a current authorization in effect, the organization can move directly to the last step in the RMF, continuous monitoring. If a current authorization is not in place, the organization continues with the assessment, authorization, and monitoring steps in the RMF.

ORGANIZATIONAL PREPARATION

Organizational preparation prior to applying the Risk Management Framework can achieve more effective, efficient, and cost-effective execution of organizational risk management processes. The primary objectives of organizational preparation are:

- To facilitate better communication between senior leaders and executives at the organization and mission/business process levels and system owners—conveying acceptable limits regarding the implementation of security and privacy controls within established organizational risk tolerance;
- To facilitate organization-wide identification of common controls and the development of organization-wide tailored security and privacy control baselines, to reduce the workload on individual system owners and the cost of system development and protection;
- To reduce the complexity of the IT infrastructure by consolidating, standardizing, and optimizing systems, applications, and services through the application of enterprise architecture concepts and models; and
- To identify, prioritize, and focus resources on high-value assets and high-impact systems that require increased levels of protection—taking steps commensurate with risk such as moving lower impact systems to cloud or shared services, systems, and applications.

These objectives will significantly reduce the information technology footprint and attack surface of organizations, promote IT modernization objectives, and prioritize security and privacy activities to focus protection strategies on the most critical assets and systems.

TIPS FOR STREAMLINING RMF IMPLEMENTATION

- Maximize the use of *common controls* at the organization level to promote standardized, consistent, and cost-effective security and privacy capability inheritance.
- Maximize the use of *shared* or *cloud-based* systems, services, and applications to reduce the number of authorizations, enterprise-wide.
- Employ organization-wide *tailored* control baselines to increase the focus and consistency of security and privacy plans; and the speed of security and privacy plan development.
- Establish and publicize organization-wide *control parameters* to increase the speed of security and privacy plan development and the consistency of security and privacy plan content.
- Maximize the use of *automated tools* to manage security categorization; security and privacy control selection, assessment, and monitoring; and the authorization process.
- Decrease the level of effort and resource expenditures for *low-impact* systems if those systems cannot adversely affect higher-impact systems through system connections.
- Maximize the *reuse* of RMF artifacts (e.g., security and privacy control assessment results) for standardized hardware/software deployments, including configuration settings.
- Reduce the *complexity* of the IT infrastructure by eliminating unnecessary systems, system components, and services — employ *least functionality* principle.
- Transition quickly to *ongoing authorization* and use *continuous monitoring* approaches to reduce the cost and increase the efficiency of security and privacy programs.
- Employ common sense security and privacy controls, *rightsizing* RMF activities for mission and business success.

3.1 PREPARATION

Purpose

The purpose of the organizational *Preparation* step is to identify and carry out the necessary activities at the organization and mission/business process levels of the enterprise to prepare the organization to execute its security- and privacy-related risk management processes at the system level.

The organizational preparation step is guided and informed by the Identify Function in the NIST Cybersecurity Framework. This step is also informed by organizational Profiles developed as part of the implementation of the Framework or conversely, can be used to help create organizational Profiles where none exist.

Organizational preparation is not intended to require additional activities for implementation—rather, it emphasizes the importance of having organization-wide governance and the appropriate resources in place to enable the execution of efficient and consistent risk management processes across the organization. The tasks in the organizational preparation step are described in NIST Special Publication 800-39 and are reflected in this publication to provide a formalized connection from the enterprise-level decision making for security- and privacy-related risk to the system-level decision making at the operational level. The preparation step can also be used to align security- and privacy-related risk for organizations to the Enterprise Risk Management activities addressing the totality of risks affecting the organization.

Outcomes[30]

- Assignments are made to key roles for executing organizational risk management processes.
- A risk management strategy for the organization that includes a determination of risk tolerance is established.
- Missions, business functions, and mission/business processes that the system[31] is intended to support are identified.
- The stakeholders having a security and privacy interest in the system are identified.
- Stakeholder assets are identified and prioritized.
- For systems that process personally identifiable information, the information life cycle is identified.
- An initial risk assessment is completed or an existing risk assessment is updated.
- Stakeholder protection needs and security and privacy requirements are defined and prioritized.
- The placement of the system within the enterprise architecture is determined.

[30] The outcomes described in this publication can be achieved by different organizational levels—that is, some of the outcomes are universal to the entire enterprise, while others are system-focused or operating unit-focused.

[31] While the term *system* appears in several of the organizational preparation tasks, its use is in the context of what the organization must do to support individual system owners in the RMF steps that follow. There are typically no actions or involvement by system owners at this stage of the RMF. Systems owners become involved only after all enterprise-wide planning and decisions have occurred.

- An organization-wide security and privacy architecture is defined.
- Common controls that are available for inheritance by organizational systems are identified and published.
- A prioritization of organizational systems with the same impact level is conducted.
- Tailored security and privacy control baselines for enterprise-wide use are established and made available.
- An organization-wide strategy for monitoring security and privacy control effectiveness is developed and implemented.

Tasks

Quick link to summary table for RMF Preparation tasks

PREPARATION

RISK MANAGEMENT ROLES

Task 1 Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework.

Potential Inputs: Organizational security and privacy policies and procedures; organizational charts.

Potential Outputs: Documented Risk Management Framework role assignments.

Primary Responsibility: Head of Agency or Chief Executive Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: The roles and responsibilities of key participants in risk management processes within organizations are described in Appendix A. The roles and responsibilities may include personnel both internal or external to the organization. Since organizations have different missions, functions, and organizational structures, there may be differences in naming conventions for risk management roles and how specific responsibilities are allocated among organizational personnel including, for example, multiple individuals filling a single role or a single individual filling multiple roles. In either situation, the basic functions remain the same. The application of the RMF is flexible, allowing organizations to accomplish the intent of the specific tasks within their respective organizational structures and to manage information system-related security risks. Many risk management roles defined in this publication have counterpart roles defined in the system development life cycle processes carried out by organizations. Thus, whenever possible, organizations align the risk management roles with similar or complementary roles defined for the system development life cycle. Organizations ensure that there are no conflicts of interest when assigning the same individual to multiple risk management roles. For example, authorizing officials cannot occupy the role of system owner or common control provider for systems or common controls they are authorizing. In addition, combining multiple roles for security and privacy requires care because in some circumstances, the priorities may be competing.

References: NIST Special Publication 800-160 (Human Resource Management Process); NICE Cybersecurity Workforce Framework.

RISK MANAGEMENT STRATEGY

Task 2 Establish a risk management strategy for the organization that includes a determination of risk tolerance.

Potential Inputs: Organizational mission statement; organizational policies; organizational risk assumptions, constraints, priorities and trade-offs.

Potential Outputs: Organizational risk management strategy and statement of risk tolerance.

Primary Responsibility: Head of Agency or Chief Executive Officer.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: Risk tolerance is the level or degree of risk or uncertainty that is acceptable to an organization. Risk tolerance affects all components of the risk management process, having a direct impact on the risk management decisions made by senior leaders or executives throughout the organization and providing important constraints on those decisions. The risk management strategy guides and informs risk-based decisions including how security and privacy risk is framed, assessed, responded to, and monitored. The risk management strategy makes explicit the threats, assumptions, constraints, priorities, trade-offs, and risk tolerance used for making investment and operational decisions. This strategy includes the strategic-level decisions and considerations on how senior leaders and executives are to manage security, privacy, and supply chain risks to organizational operations and assets, individuals, other organizations, and the Nation. The risk management strategy includes an unambiguous expression of organizational risk tolerance, acceptable risk assessment methodologies, risk response strategies, a process for consistently evaluating the security, privacy, and supply chain risks across the organization with respect to the risk tolerance of the organization, and the approaches for monitoring risk over time. The risk management strategy for security and privacy is aligned with the Enterprise Risk Management strategy.

References: NIST Special Publications 800-30, 800-39 (Organization Level), 800-160 (Risk Management, Quality Assurance, Quality Management, Decision Management, Project Assessment and Control Processes), 800-161; NIST Interagency Report 8062; Cybersecurity Framework (Core [Identify Function]).

MISSIONS, BUSINESS FUNCTIONS, AND MISSION/BUSINESS PROCESSES

Task 3 Identify the missions, business functions, and mission/business processes that the system is intended to support.

Potential Inputs: Organizational mission statement; organizational policies; mission/business process information; system stakeholder information.

Potential Outputs: Information specifying the missions, business functions, and mission/business processes that the system will support.

Primary Responsibility: Head of Agency or Chief Executive Officer; Mission/Business Owner.

System Life Development Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: Organizational missions and business functions influence the design and development of the mission/business processes that are created to carry out those missions and business functions. The prioritization of missions and business functions drives investment strategies and funding decisions, and therefore, affects the development of the enterprise architecture and the security and privacy architecture. Information is elicited from stakeholders to acquire a thorough understanding of the missions, business functions, and mission/business processes of the organization from a system security and privacy perspective.

References: NIST Special Publications 800-39 (Organization and Mission/Business Process Levels), 800-64, 800-160 (Business or Mission Analysis, Portfolio Management, and Project Planning Processes); NIST Interagency Report 8179 (Criticality Analysis Process B); Cybersecurity Framework (Core [Identify Function]).

ORGANIZATIONAL STAKEHOLDERS

Task 4 Identify stakeholders who have a security and privacy interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.

Potential Inputs: Organizational mission statement; mission/business process information; organizational security and privacy policies and procedures; organizational charts; information about individuals or groups (internal and external) that have a security and privacy interest in and decision-making responsibility for the system.

Potential Outputs: List of system stakeholders.

Primary Responsibility: Head of Agency or Chief Executive Officer; Mission/Business Owner.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: Stakeholders include individuals, organizations, or representatives with security and privacy concerns across the entire life cycle of the system—for design, development, implementation, operation, and delivery of the system. It also includes all aspects of the supply chain. Stakeholders may reside in the same organization or they may reside in different organizations in situations when there is a common interest by those organizations in the system. For example, this may occur during the development and the operation of cloud-based systems, shared service systems, or any system where organizations may be adversely impacted by a breach or a compromise to the system—or for a variety considerations related to the supply chain.

References: NIST Special Publications 800-39 (Organization Level), 800-64, 800-160 (Stakeholder Needs and Requirements Definition and Portfolio Management Processes), 800-161; Cybersecurity Framework (Core [Identify Function]).

STAKEHOLDER ASSETS

Task 5 Identify stakeholder assets that require protection.

Potential Inputs: Information specifying the missions, business functions, and mission/business processes the system will support; business impact analyses; internal stakeholders; system stakeholder information; system information; information about other systems that interact with the system.

Potential Outputs: Known set of stakeholder assets to be protected.

Primary Responsibility: Head of Agency or Chief Executive Officer; Mission/Business Owner.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: Assets are identified in consideration of stakeholders and the contexts in which the assets are used by the system. This includes the missions or business functions; the other systems that interact with the system; and stakeholders whose assets are utilized by the mission or business functions or by the system. Organizational assets include tangible and intangible assets. Tangible assets are physical in nature and include the physical elements of the environment of operation (e.g., structures, facilities) and hardware elements of components, mechanisms, systems, and networks. In contrast, intangible assets are not physical in nature and include mission and business processes, functions, information, data, firmware, software, personnel, and services. Information and data assets include the information and data required to carry out organizational missions/business functions, to deliver services, and for system management and operation; classified and controlled unclassified information; and all forms of documentation associated with the system. Intangible assets also include the image or reputation of an organization. The organization defines the scope of stakeholder assets to be considered for protection.

References: NIST Special Publications 800-39 (Organization Level), 800-64, 800-160 (Stakeholder Needs and Requirements Definition Process); NIST Interagency Report 8179 (Criticality Analysis Process C); Cybersecurity Framework (Core [Identify Function]); NARA CUI Registry.

INFORMATION LIFE CYCLE

Task 6 For systems that process personally identifiable information, identify the information life cycle.

Potential Inputs: information specifying the missions, business functions, and mission/business processes the system will support; system stakeholder information; information about other systems that interact with the system; system design documentation.

Potential Outputs: Data map illustrating where individuals interact with the system and/or how personally identifiable information is being processed throughout its life cycle by the system.

Primary Responsibility: Chief Information Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of (collectively "processing") personally identifiable information (PII). A system may need to process PII in whole or in part of its life cycle to achieve its mission or business function. While the mission or business function is expected to provide benefits, an unintended consequence of the PII processing is the potential for individuals to experience privacy-related problems depending on how the processing is accomplished. The objective of a privacy risk assessment and subsequent selection and implementation of privacy controls is to minimize the likelihood and/or the impact of creating privacy-related problems, while maximizing the benefits or utility of the PII processing for the mission or business function.

Identifying the life cycle of PII through a data map enables organizations to know how PII is being processed or where individuals are interacting with the system so that they can better assess where privacy risks could arise and privacy controls can be applied most effectively. It is important for organizations to consider the appropriate delineation of the system boundary or the interaction of other systems with the system-of-interest because the way PII enters and leaves the system can affect the privacy risk assessment. The components of the system and whether the components are operated by different types of organizations (e.g., public sector, private sector), also can affect the privacy risk assessment and may be captured in the data map. Elements of PII are identified with sufficient granularity to support a meaningful privacy risk assessment. In certain contexts, it may be a particular element of PII (e.g., geolocation) that gives rise to the greatest privacy risk. Selecting appropriate privacy controls to manage this element may reduce privacy risk while maintaining the overall utility of the PII. A data map need not be a separate document, but may simply be an overlay to existing system design artifacts such as a system architecture diagram or swim lane diagram.

References: NIST Interagency Report 8062.

RISK ASSESSMENT

Task 7 Conduct an initial risk assessment of stakeholder assets and update the risk assessment on an ongoing basis.

Potential Inputs: Known set of stakeholder assets to be protected; information specifying the missions, business functions, and mission/business processes the system will support; business impact analyses or criticality analyses; system stakeholder information; information about other systems that interact with the system; current threat information; system design documentation; organizational risk management strategy.

Potential Outputs: Risk assessment report.

Primary Responsibility: Senior Accountable Official for Risk Management or Risk Executive (Function).

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: Assessment of risk includes identification of threat sources and threat events affecting stakeholder assets, whether and how the assets are vulnerable to the threats,[32] likelihood that an

[32] In addition, the use of threat intelligence, threat analysis, and threat modelling can help agencies develop the security and privacy capabilities necessary to reduce agency susceptibility to a variety of threats including hostile cyber-attacks, natural disasters, equipment failures, and errors of omission and commission.

asset vulnerability will be exploited by a threat source/event, and the impact (consequence) of loss of the assets. As part of the risk assessment, stakeholder assets are prioritized based on the adverse consequence of asset loss. The meaning of loss is defined for each stakeholder asset to enable a determination of loss consequence (i.e., the adverse impact of the loss). Loss consequences constitute a continuum that spans from partial loss to total loss relative to the asset. The consequence of losing an asset is determined relative to the concerns of the stakeholders. Interpretations of data loss may include loss of possession, destruction, or loss of precision or accuracy. The loss of a function or service may be interpreted as a loss of control, loss of accessibility, loss of the ability to deliver normal function, performance, or behavior, or a limited loss of capability resulting in a level of degradation of function, performance, or behavior. Prioritization of assets is based on the stakeholder assessment of acceptance of the adverse consequence of loss. This is reflected in terms of asset value, criticality, cost of replacement, impact on image or reputation, or trust by users, by mission or business partners, or by collaborating organizations. The asset priority translates to precedence in allocating resources, determining strength of mechanisms, and defining levels of assurance. Asset valuation is a precondition for defining stakeholder protection needs and security requirements.

Another aspect of risk assessment is the determination of asset susceptibility to adversity and uncertainty. Adversity includes all forms of potential disruptions, threats, and hazards across all human, physical, technology/machine, and environmental forms throughout the system's life cycle. Adversity consists of those events and preexisting or emergent conditions that combine to produce the loss of assets and the associated adverse consequences to stakeholders. Adversity comes in malicious and non-malicious forms and can emanate from a variety of sources including, for example, simple or sophisticated attacks (i.e., cyber, electronic, supply chain, physical, social); human error (i.e., commission or omission); abuse and misuse; accidents and incidents; component fault or failure; and natural or man-made disasters. The identification and assessment of adversity characterizes the events and conditions that are anticipated throughout the life cycle of the system and correlates those events and conditions to the asset loss concerns of stakeholders. The correlation of asset susceptibility to adversity with loss consequence considers what is known, what is possible, what is likely, and what is uncertain.

The uncertainty about how an asset loss consequence might occur is not sufficient grounds to dismiss such a consequence. Uncertainty, as it relates to adversity, is addressed by considerations of those situations where there are known consequences that can be forecast and deemed unacceptable and for which there is an absence of direct, specific, or credible knowledge of an adverse event-to-consequence relationship, or for which there is insufficient basis to forecast such a relationship. There are also limits on what specific knowledge is obtainable and thus, adverse consequences can occur for reasons that are unknown until the actual event occurs. Nonetheless, adverse impact can be minimized and the uncertainty-to-consequence relationship addressed as part of the determination of susceptibility to threats.

In addition to security risk assessments, privacy risk assessments are conducted to address how individuals interact with the system or how personally identifiable information is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of by the system and what the likelihood and impact are if such activities create privacy-related problems for individuals.

Risk assessments are conducted throughout the system development life cycle and support various RMF steps and tasks. Risk assessment results can be used to guide and inform potential courses of action for risk responses. Organizations determine the form of risk assessment conducted (including the scope, rigor, and formality of such assessments) and the method of reporting results.

References: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-39 (Organization Level), 800-59, 800-60, 800-64, 800-160 (Stakeholder Needs and Requirements Definition and Risk Management Processes), 800-161 (Assess); NIST Interagency Reports 8062, 8179; Cybersecurity Framework (Core [Identify Function]); CNSS Instruction 1253.

STAKEHOLDER PROTECTION NEEDS — SECURITY AND PRIVACY AND REQUIREMENTS

Task 8 Define the stakeholder protection needs and stakeholder security and privacy requirements.

Potential Inputs: System design documentation; risk assessment report; known set of stakeholder assets to be protected; information specifying the missions, business functions, and mission/business processes the system will support; business impact analyses or criticality analyses; system stakeholder information; data

map of the information life cycle for personally identifiable information; supply chain information; information about other systems that interact with the system; current threat information; laws, regulations, or policies that apply to the system; organizational risk management strategy.

Potential Outputs: Documented stakeholder protection needs and stakeholder security and privacy requirements.

Primary Responsibility: Head of Agency or Chief Executive Officer; Mission/Business Owner; Information Owner/Steward.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: The stakeholder protection needs are an informal expression of the protection capability required in the system. Protection needs include the security and privacy characteristics of the system and the security and privacy behavior of the system in its intended operational environment and across all life cycle phases. The protection needs reflect the relative priorities of stakeholders, the results of negotiations among stakeholders in response to conflicts, opposing priorities, contradictions, and stated objectives, and therefore, are inherently subjective. The stakeholder protection needs are captured to ensure that the reasoning, assumptions, and constraints associated with those needs are available—if the basis of the decisions or the objectives that drive the definition of the protection needs, changes.

Stakeholder security and privacy requirements constitute a formal expression of stakeholder protection needs across all system development life cycle phases, the associated life cycle processes, and protections for the assets associated with the system. Security and privacy requirements can be obtained from laws, Executive Orders, directives, regulations, policies, standards, or organizational mission and business requirements. Stakeholder security and privacy requirements are a part of the formal expression of required quality characteristics of the system—encompassing security, privacy, and assurance. The security and privacy requirements guide and inform the selection of controls for a system and the tailoring activities associated with those controls.

Organizations can use the Cybersecurity Framework to consolidate stakeholder security requirements and express those requirements in Framework profiles defined for the organization. The profiles can be used to inform the development of tailored security control baselines described in Task 10 of the organizational preparation step.

References: NIST Special Publications 800-39 (Organization Level); 800-64, 800-160 (Stakeholder Needs and Requirements Definition Process), 800-161 (Multi-Tiered Risk Management); NIST Interagency Report 8179; Cybersecurity Framework (Core [Protect, Detect, Respond, Recover Functions]; Profiles).

ENTERPRISE ARCHITECTURE

Task 9 Determine the placement of the system within the enterprise architecture.

Potential Inputs: Stakeholder security and privacy requirements; asset information; enterprise architecture information; security and privacy architecture information.

Potential Outputs: Updated enterprise architecture and security and privacy architecture; plans to use cloud-based systems and shared systems, services, or applications.

Primary Responsibility: Enterprise Architect; Security or Privacy Architect.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: A significant risk regarding the ability of organizations to successfully carry out their missions and business functions is system complexity. Providing greater understanding of information and operational technologies included in the initial design and development of systems is a prerequisite for achieving resilience and survivability of those systems in the face of increasingly sophisticated threats. This can be effectively achieved through the development of enterprise architecture. Enterprise architecture is a management practice used by organizations to maximize the effectiveness of mission/business processes

and information resources and to achieve mission and business success. Enterprise architecture establishes a clear and unambiguous connection from investments to measurable performance improvements for an organization. Enterprise architecture provides an opportunity to consolidate, standardize, and optimize information and operational technology assets. An effectively implemented enterprise architecture produces systems that are more transparent and therefore, easier to understand and protect.

The security and privacy architecture is an integral part of the enterprise architecture. It represents that portion of the enterprise architecture specifically addressing system resilience and providing architectural information for the implementation of security and privacy requirements. The primary purpose of the security and privacy architecture is to help ensure that mission/business process-driven security and privacy requirements are consistently and cost-effectively achieved in organizational systems and are aligned with the risk management strategy. Ultimately, the security and privacy architecture provides a roadmap that facilitates traceability from the strategic goals and objectives of organizations, through stakeholder protection needs and stakeholder security and privacy requirements, to specific security and privacy solutions provided by people, processes, and technologies.

References: NIST Special Publications 800-39 (Mission/Business Process Level), 800-64, 800-160 (System Requirements Definition Process); Cybersecurity Framework (Core [Identify Function]; Profiles); Common Approach to Federal Enterprise Architecture; Federal Enterprise Architecture Framework.

ORGANIZATION-WIDE TAILORED CONTROL BASELINES AND PROFILES (OPTIONAL)

Task 10 Establish and publish organization-wide tailored control baselines and profiles.

Potential Inputs: Documented stakeholder protection needs and security and privacy requirements; applicable laws, Executive Orders, directives, regulations, policies, or standards requiring the use of specific tailored security and privacy control baselines; NIST Special Publication 800-53 control baselines.

Potential Outputs: List of organization-approved or mandated tailored baselines; Cybersecurity Framework profiles.

Primary Responsibility: Mission/Business Owner; Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: To address the need for specialized sets of security and privacy controls, *tailored* control baselines may be developed for organization-wide use.[33] An organization-wide tailored baseline provides a fully specified set of controls, control enhancements, and supplemental guidance derived from established control baselines described in NIST Special Publication 800-53. The tailoring process can also be guided and informed by the requirements engineering process described in NIST Special Publication 800-160. Organizations can use the tailored control baseline concept when there is divergence from the fundamental assumptions used to create the initial control baselines in NIST Special Publication 800-53. This would include situations when the organization faces specific threats and vulnerabilities not addressed in the initial baselines.

Tailored baselines complement the initial control baselines by providing an opportunity to add or eliminate controls. Organizations can use tailored baselines to customize security and privacy control baselines by describing control applicability and providing interpretations for specific technologies; types of missions, operations, systems, operating modes, or operating environments; and statutory or regulatory requirements. Organization-wide tailored baselines can establish parameter values for assignment or selection statements in controls and control enhancements that are agreeable to communities of interest and can also extend the supplemental guidance where necessary. Tailored baselines may be more stringent or less stringent than the original control baselines and can be applied to multiple systems. Tailored baselines may be mandated for

[33] Tailored baselines may also be known as *overlays*. Thus, an organization-wide tailored baseline is analogous to an organization-wide overlay since an overlay is a tailored baseline that services a community of interest, in this case, the organization.

use by laws, Executive Orders, directives, regulations, policies, or standards. In certain situations, tailoring actions may be restricted or limited by the developer of the tailored baseline or by the issuing authority for the tailored baseline. Tailored baselines (overlays) have been developed for cloud and shared systems, services, and applications; national security systems; weapons and space-based systems; high-value assets; mobile device management; federal public key infrastructure; and privacy applications.

Organizations may also benefit from the creation of a Cybersecurity Framework *profile*. A profile is a prioritization of the Framework Core Categories and/or Subcategory outcomes based on business/mission functions, security requirements, and risk determinations. Many of the tasks in organizational preparation provide an enterprise-level view of these considerations and can serve as inputs to a profile. The resulting prioritized list of cybersecurity outcomes developed at the Enterprise and Mission/Business Process levels of an organization can be helpful in driving consistent, risk-based decisions at the system level during the execution of the RMF steps. The profile can be used to guide and inform the development of the tailored security and privacy control baselines described above.

References: NIST Special Publications 800-53, 800-160 (Business or Mission Analysis, Stakeholder Needs and Requirements Definition Process); Cybersecurity Framework (Core, Profiles).

COMMON CONTROL IDENTIFICATION

Task 11 Identify and publish organization-wide common controls that are available for inheritance by organizational systems.

Potential Inputs: Documented stakeholder protection needs and stakeholder security and privacy requirements; existing common control providers and associated system security and privacy plans; organizational information security and privacy program plans.

Potential Outputs: List of common control providers and common controls available for inheritance; security and privacy plans (or equivalent documents) providing a functional description of the common control implementation (including inputs, expected behavior, and expected outputs).

Primary Responsibility: Chief Information Officer; Senior Information Agency Security Officer; Senior Agency Official for Privacy; Senior Accountable Official for Risk Management or Risk Executive (Function).

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: Common controls are security and privacy controls that can be inherited by one or more organizational systems. Such controls can include, for example, physical and environmental protection controls, personnel security controls, or complaint management controls for receiving privacy-related inquiries from the public. Organizations identify and select the set of common controls and assign those controls to organizational entities designated as common control providers. Common controls may differ based upon a variety of factors, such as hosting location, system architecture, and structure of the organization. The list of common controls should take these factors into account. Common controls can also be identified at different levels of the organization, including, for example, corporate or agency level; bureau or subcomponent level; or individual department level. Organizations may establish one or more lists of common controls that can be inherited by organizational systems.

When there are multiple sources of common controls, organizations specify the common control provider (i.e., who is providing the controls and through what venue, for example, shared services, specific systems, or within a specific type of architecture) and which systems or types of systems can inherit the controls. Common control listings are communicated to system owners so they are aware of the security and privacy capabilities that are available from the enterprise through inheritance. System owners are not required to assess common controls that are inherited by their systems or document common control implementation details. That is the responsibility of the common control providers. Likewise, common control providers are not required to have visibility into the system-level details of those systems that are inheriting the common controls they are providing.

Risk assessment results can be used when identifying common controls for organizations to determine if the controls available for inheritance meet the security and privacy requirements for organizational systems and the environments in which those systems operate (including the identification of potential single points of failure). When the common controls provided by the organization are determined to be insufficient for the systems inheriting those controls, system owners can supplement the common controls with system-specific or hybrid controls to achieve the required protection for their systems or accept greater risk with the acknowledgement and approval of the organization.

Common control providers execute the steps in the RMF to implement, assess, and monitor the security and privacy controls designated as common controls. Common control providers may also be system owners when the common controls are resident within a system. Organizations select senior officials or executives to serve as authorizing officials for common controls. Authorizing officials are responsible for accepting security and privacy risk resulting from the use of common controls inherited by organizational systems. Common control providers are responsible for documenting common controls in a security and privacy plans (or equivalent documents prescribed by the organization); ensuring that the controls are implemented and assessed for effectiveness by qualified assessors; ensuring that assessment findings are documented in a security and privacy assessment reports; producing a plan of action and milestones for common controls determined to be less than effective (i.e., having unacceptable weaknesses or deficiencies) and targeted for remediation; receiving authorization for the common controls from the designated authorizing official; and monitoring control effectiveness on an ongoing basis. Plans, assessment reports, and plans of action and milestones for common controls (or a summary of such information) are made available to system owners. This information can be used by authorizing officials to inform authorization decisions for systems inheriting common controls.

References: NIST Special Publication 800-53.

IMPACT-LEVEL PRIORITIZATION (OPTIONAL)

Task 12 Prioritize organizational systems with the same impact level.

Potential Inputs: System categorization information for organizational systems.

Potential Outputs: Prioritized list of organizational systems for low, moderate, and high impact.

Primary Responsibility: Mission/Business Owner; Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Senior Accountable Official for Risk Management or Risk Executive (Function).

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: This task is an *optional* enterprise-level task and is carried out *only* after all organizational systems have been categorized in Task 4 of the RMF Categorization step. Task 4 requires organizations to apply the "high water mark" concept to each of their systems categorized in accordance with FIPS Publication 199. This process results in systems designated as low impact, moderate impact, or high impact. Organizations desiring additional granularity in the system impact designations for risk-based decision making can use this task to prioritize their systems within each impact level. For example, an organization may decide to prioritize its moderate-impact systems by assigning each moderate system to one of three new subcategories: low-moderate systems, moderate-moderate systems, and high-moderate systems. This prioritization of moderate systems gives organizations an opportunity to make more informed decisions regarding security control selection and the tailoring of security control baselines in responding to identified risks. Impact-level prioritization can also be used to determine those systems that are critical to organizational missions and business operations (sometimes referred to as high-value assets) and therefore, organizations can focus on the important factors of complexity, aggregation, and system interconnections. Such systems can be identified for example, by prioritizing high-impact systems into low-high systems, moderate-high systems, and high-high systems. Impact-level prioritizations can be conducted at any organizational level and are based on system categorization data reported by individual system owners.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39 (Organization and System Levels), 800-59, 800-60, Vol. I, 800-60, Vol. II, 800-160 (System Requirements Definition Process); CNSS Instruction 1253; Cybersecurity Framework (Core [Identify Function]).

ORGANIZATIONAL MONITORING STRATEGY

Task 13 Develop and implement an organization-wide strategy for monitoring security and privacy control effectiveness.

Potential Inputs: Organizational risk management strategy; organizational and system risk assessments; organizational security and privacy policies.

Potential Outputs: An implemented organizational continuous monitoring strategy.

Primary Responsibility: Senior Agency Information Security Officer; Senior Agency Official for Privacy; Senior Accountable Official for Risk Management/Risk Executive (Function); Chief Information Officer.

System Development Life Cycle Phase: New – Development/Acquisition.
Existing – Operations/Maintenance.

Supplemental Guidance: An important aspect of risk management is the ongoing monitoring of security and privacy controls employed within or inherited by organizational systems. An effective organizational monitoring strategy is essential to efficiently and cost-effectively assessing the effectiveness of security and privacy controls that are implemented in systems and environments of operation. Continuous monitoring strategies can also include supply chain risk considerations, for example, requiring suppliers to be audited on an ongoing basis. The implementation of a robust and comprehensive continuous monitoring program helps an organization to understand the security and privacy state of organizational systems over time and to maintain the initial system or common control authorizations in a dynamic environment of operation. This includes the potential for changing missions/business functions, stakeholders, technologies, vulnerabilities, threats, privacy risks, and suppliers of systems, components, or services.

The organizational continuous monitoring strategy addresses monitoring requirements at the organization, mission/business process, and system levels to the greatest extent possible. The monitoring strategy also identifies the minimum frequency of monitoring for implemented controls across the organization and defines the organizational control assessment approach. The organizational monitoring strategy may also define how changes to systems are to be monitored, how security and privacy impact analyses are to be conducted, and security and privacy status reporting requirements including recipients of the status reports.

The criteria for determining the minimum frequency with which security and privacy controls are to be monitored post deployment is established in collaboration with selected organizational officials including, for example, the senior accountable official for risk management/risk executive (function); senior agency information security officer; senior agency official for privacy; chief information officer; authorizing officials or designated representatives; system owners; and common control providers. An organizational risk assessment can also be used to guide and inform the frequency of monitoring. The use of automation facilitates a greater frequency and volume of control assessments as part of the monitoring process. The ongoing monitoring of security and privacy controls using automated tools and supporting databases at the facilitates near real-time risk management for organizational systems, and supports ongoing authorization and more efficient use of resources. The senior accountable official for risk management/risk executive (function) approves the organizational monitoring strategy including the minimum frequency with which controls are to be monitored.

References: NIST Special Publications 800-30, 800-39 (Organization, Mission/Business Process, System Levels), 800-53, 800-53A, 800-161, 800-137; NIST Interagency Report 8062; Cybersecurity Framework (Core [Detect Function]); CNSS Instruction 1253.

3.2 CATEGORIZATION

Purpose

The purpose of the *Categorization* step is to guide and inform subsequent risk management processes and tasks by determining the adverse impact or consequences to the organization with respect to the compromise or loss of organizational assets—including the confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.

Outcomes

- The system boundary is determined.
- Security and privacy requirements are allocated to the system and to the environment in which the system operates.
- The types of information processed, stored, and transmitted by the system are identified.
- A security categorization of the system including the information represented by the information types identified by the organization is completed.
- Impact-level prioritization results are obtained from the organization, if available.
- Security categorization results are documented as system requirements.
- Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes.
- Security categorization results reflect the organization's risk management strategy.
- The characteristics of the system are described and documented.
- The system is registered for purposes of management, accountability, coordination, and oversight.

Tasks

Quick link to summary table for RMF Categorization tasks

CATEGORIZATION

SYSTEM BOUNDARY

Task 1 Determine the boundary of the system.

Potential Inputs: System design documentation; system stakeholder information; asset information; organizational structure information/charts.

Potential Outputs: Documented system boundary information.

Primary Responsibility: System Owner; Authorizing Official or Designated Representative; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: System boundaries establish the scope of protection for systems (i.e., what the organization agrees to protect under its management control or within the scope of its responsibilities). A common area of concern for organizations is the often-blurred lines with respect to system boundaries and the frequent dependencies between systems. This area of concern is heightened in situations where low-impact systems are connected to higher-impact systems, either knowingly or unknowingly. In the absence of clearly defined system boundaries, the security categorization cannot be determined with any degree of accuracy. Therefore, the responsibility and accountability for the security of the system cannot be assigned. Each system consists of a set of interacting elements organized to achieve one or more stated purposes and supporting the organization's missions and business processes. Each system element is implemented to fulfill specified requirements including security and privacy requirements. System elements include human elements, technology/machine elements, and physical/environmental elements.[34] System elements are implemented via hardware, software, or firmware; physical structures or devices; or people, processes, and procedures.

For a large or complex system, a system element may be regarded as a system and will itself be composed of system elements. The hierarchical and context-dependent nature of the terms system and system element allows the term system to be used when referring to a discrete component or a complex, geographically distributed system-of-systems. Because the term system can be applied across a continuum from composed elements to a discrete element, the context in which the term system is being used must be communicated and understood. The term system-of-interest is used to define the set of system elements, system element interconnections, and the environment that is the focus of the RMF implementation. For systems processing personally identifiable information, it is essential that privacy and security programs collaborate to develop a common and shared understanding of the system boundary. Privacy risks arise from the processing of PII, which may occur outside of what the security program typically considers the system boundary. Privacy programs cannot effectively conduct the privacy risk assessment that underpins the selection of controls if the privacy and security programs have a materially different understanding of what constitutes a system. System boundaries are determined by authorizing officials based on mission, management, or budgetary responsibility.

References: NIST Special Publications 800-18, 800-39 (System Level), 800-47, 800-64, 800-160 (System Requirements Definition Process); Cybersecurity Framework (Core [Identify Function]).

SECURITY AND PRIVACY REQUIREMENTS ALLOCATION

Task 2 Identify the security and privacy requirements allocated to the system and to the organization (environment of operation).

Potential Inputs: System categorization; organizational policy on system registration; system description; system element information; system component inventory; relevant privacy legislation, regulation and policy.

Potential Outputs: List of security and privacy requirements allocated to the system and to specific system elements; list of security and privacy requirements allocated to the environment of operation.

Primary Responsibility: Security or Privacy Architect; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: The allocation of security and privacy requirements to the system, organization, or to the system and the organization will determine which security and privacy controls are designated as system-specific, common, and hybrid during the control selection and specification process. Common controls that satisfy security and privacy requirements allocated to the organization provide a security and privacy capability that is inherited by one or more systems. Hybrid controls that satisfy security and privacy requirements allocated to the system and organization provide a security and privacy capability that is

[34] System *components* (i.e., hardware, software, and firmware) are a subset of system elements.

partially inherited by one or more systems. And finally, system-specific controls that satisfy security and privacy requirements allocated to the system provide a security and privacy capability only for that system. It is important for organizations to determine the security and privacy requirements that are allocated to the organization and the associated common controls available for inheritance by systems.

References: NIST Special Publications 800-39 (Organization, Mission/Business Process, and System Levels), 800-64, 800-160 (System Requirements Definition Process); Cybersecurity Framework (Core [Identify Function]; Profiles); Common Approach to Federal Enterprise Architecture; Federal Enterprise Architecture Framework.

INFORMATION TYPES

Task 3 Identify the types of information to be processed, stored, and transmitted by the system.

Potential Inputs: Stakeholder assets to be protected; mission/business process information.

Potential Outputs: A list of information types for the system.

Primary Responsibility: System Owner; Information Owner/Steward.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: Identifying the types of information needed to support organizational missions, business functions, and mission/business processes is an important step in developing comprehensive security and privacy plans for the system and a precondition for conducting a security categorization process. The National Archives and Records Administration (NARA) has defined a comprehensive set of information types as part of its Controlled Unclassified Information (CUI) program. Organizations may also define mission/business-specific information types that are needed to support organizational missions, business functions, and mission/business processes.

References: NIST Special Publications 800-39 (System Level), 800-60, Vol. I, 800-60, Vol. II, 800-122; Cybersecurity Framework (Core [Identify Function]); NARA CUI Registry.

SECURITY CATEGORIZATION

Task 4 Categorize the system and document the security categorization results as part of system requirements.

Potential Inputs: Organizational risk management strategy; organizational risk tolerance; system boundary information; system risk assessment; information types processed/stored/transmitted by the system; list of security requirements allocated to the system and to specific system elements; list of security requirements allocated to the environment of operation; business impact analyses or criticality analyses.

Potential Outputs: Impact levels determined for each information type and for each security objective (confidentiality, integrity, availability); system categorization based on high water mark of information type impact levels.

Primary Responsibility: System Owner; Information Owner/Steward.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: Security categorization determinations consider potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation. The security categorization process is carried out by the system owner and the information owner/steward in cooperation and collaboration with senior leaders and executives with mission/business function or risk management responsibilities. The categorization process takes into consideration the enterprise architecture and the security architecture. This ensures that individual systems are categorized based on the mission and business objectives of the organization. The system owner and information owner/steward consider the results from the risk assessment as a part of the security categorization decision. The decision is consistent

with the risk management strategy and identifies the potential adverse impact to mission/business functions resulting from the loss of confidentiality, integrity, or availability. The results of the security categorization process influence the selection of security controls for the system. Security categorization information is documented in the security plan or included as an attachment to the plan, and could be cross-referenced in a privacy plan when personally identifiable information is involved.

The organization may consider decomposing the system into multiple subsystems to more efficiently and effectively allocate security controls to subsystem components. This may in turn facilitate categorization. For example, given that the system is composed of a set of system elements, each defined subsystem contains a subset of those system elements. One approach is to separately categorize each subsystem. Separately categorizing each subsystem does not change the overall categorization of the system. Rather, it allows the subsystems to receive a separate and tailored allocation of security controls instead of deploying higher-impact controls across every subsystem. Another approach is to bundle smaller subsystems into larger subsystems within the system, categorize each of the aggregated subsystems, and allocate security controls to the subsystems.

The security categorization results for the system can be consolidated by the organization to facilitate an impact-level prioritization of all organizational systems with the same impact level. See RMF Preparation Step, Task 12. Results from the impact-level prioritization conducted by the organization can be used to help system owners in control selection and tailoring decisions.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39 (System Level), 800-59, 800-60, Vol. I, 800-60, Vol. II, 800-160 (System Requirements Definition Process); NIST Interagency Report 8179; CNSS Instruction 1253; Cybersecurity Framework (Core [Identify Function]).

SYSTEM DESCRIPTION

Task 5 Describe the characteristics of the system.

Potential Inputs: System design and requirements documentation; system boundary information; list of security and privacy requirements allocated to the system and to specific system elements; list of security and privacy requirements allocated to the environment of operation; system element information/system component inventory; system categorization; information on system use, users, and roles; data map of the information life cycle for personally identifiable information.

Potential Outputs: Documented system description.

Primary Responsibility: System Owner.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: Descriptive information about the system is documented in the security and privacy plans, included in attachments to the plans, or referenced in other standard sources for information generated as part of the system development life cycle. Duplication of information is avoided, whenever possible. The level of detail in the security and privacy plans is determined by the organization and is commensurate with the security categorization and the privacy risk assessment of the system. Information may be added to the system description as it becomes available during the system life cycle and execution of the Risk Management Framework tasks.

Some examples of the different types of descriptive information that organizations can include in security and privacy plans include: descriptive name of the system and system identifier; system version or release number; individual responsible for the system and contact information; organization that manages, owns, or controls the system; system location; purpose of the system and missions/business processes supported; how the system is integrated into the enterprise architecture; system development life cycle phase; results of the security categorization process and privacy risk assessment; types of information processed, stored, and transmitted; system boundary; laws, directives, policies, regulations, or standards affecting the privacy for individuals and the security of the system; architectural description of the system including network topology; hardware, firmware, and software components that are part of the system; hardware, software, and system interfaces (internal and external); subsystems associated with the system; information flows and

within the system; network connection rules for communicating with external systems; interconnected systems and identifiers for those systems; system users (including affiliations, access rights, privileges, citizenship); system provenance in the supply chain; system or system element sources; maintenance or other relevant agreements; ownership or operation of system (government-owned, government-operated; government-owned, contractor-operated; contractor-owned, contractor-operated; nonfederal [state and local governments, grantees]); authorization date and authorization termination date; ongoing authorization status; and incident response points of contact.

References: NIST Special Publication 800-18; Cybersecurity Framework (Core [Identify Function]).

SYSTEM REGISTRATION

Task 6 Register the system with appropriate organizational program/management offices.

Potential Inputs: System categorization; organizational policy on system registration; system description.

Potential Outputs: Registered system in accordance with organizational policy.

Primary Responsibility: System Owner.

System Development Life Cycle Phase: New – Initiation (concept/requirements definition).
Existing – Operations/Maintenance.

Supplemental Guidance: The registration process begins by identifying the system (and subsystems, if appropriate) in the organization-wide system inventory and establishes a relationship between the system and the parent or governing organization that owns, manages, or controls the system. System registration, in accordance with organizational policy, uses the information in the system identification section of the security plan to inform the parent or governing organization of plans to develop the system or the existence of the system; the key characteristics of the system; and expected security implications for the organization due to the ongoing operation of the system. System registration provides organizations with an effective management/tracking tool that is necessary to ensure implementation of protections commensurate with risk and for security and privacy status reporting in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, or guidelines. Subsystems are registered as a subset of a system or a method of registration for subsystems is implemented that includes as much information as feasible.

References: Cybersecurity Framework (Core [Identify Function]).

3.3 SELECTION

Purpose

The purpose of the *Selection* step is to identify, select, tailor, and document the security and privacy controls necessary to protect the system and the organization commensurate with the risk to organizational operations and assets, individuals, other organizations, and the Nation.

Outcomes

- Security and privacy controls necessary to protect the system commensurate with risk are identified, selected, and tailored.
- Security and privacy controls are documented in the security and privacy plans or equivalent documents.
- Security and privacy controls are assigned as system-specific, hybrid, or common controls.
- A continuous monitoring strategy for the system is developed that reflects the organizational risk management strategy.
- Security and privacy plans reflecting the system-specific, hybrid, and common controls necessary to protect the system commensurate with risk are approved by the authorizing official.

Tasks

Quick link to summary table for RMF Selection tasks

SELECTION

SECURITY AND PRIVACY CONTROL SELECTION

Task 1 Select the security and privacy controls for the system and document the functional description of the planned control implementations in the security and privacy plans.

Potential Inputs: System categorization information; system risk assessment; stakeholder security and privacy requirements; system element information/system component inventory; list of security and privacy requirements allocated to the system and to system elements; list of security and privacy requirements allocated to the environment of operation; business impact analysis or criticality analysis; organizational risk management strategy; organizational security and privacy policy.

Potential Outputs: System security and privacy plans.

Primary Responsibility: System Owner; Common Control Provider.

System Development Life Cycle Phase: New – Development/Acquisition.
Existing – Operations/Maintenance.

Supplemental Guidance: Security controls are selected based on the security categorization of the system and the security requirements derived from stakeholder protection needs, laws, Executive Orders, policies, regulations, directives, instructions, and standards. Privacy controls are selected based on a privacy risk assessment and privacy requirements derived from stakeholder protection needs, laws, Executive Orders,

policies, regulations, directives, instructions, standards, and guidelines.[35] After selecting the applicable control baseline, organizations apply the tailoring process to align the controls with the specific conditions within the organization. Such conditions can include, for example, missions or business functions, threats, privacy risks, type of system, risk tolerance, or potential environments of operation.[36] The tailoring process includes identifying and designating common controls in the security and privacy control baselines (See Task 11, Preparation Step); applying scoping considerations to the remaining baseline security and privacy controls; selecting compensating controls, if needed; assigning specific values to organization-defined control parameters through explicit assignment and selection statements; supplementing baselines with additional security and privacy controls; and providing any essential specification information for control implementation. Organizations have the flexibility to determine the extent of justifications or supporting rationale required for tailoring decisions. Such determinations are consistent with organizational missions and business functions; stakeholder needs and requirements; and any laws, Executive Orders, regulations, directives, or policies.

Organizations use risk assessments to inform and guide the tailoring process for systems and organizations. Threat information from security risk assessments provides information on adversary capabilities, intent, and targeting that may affect organizational decisions regarding the selection of security controls, including the associated costs and benefits. Contextual factors can materially alter the privacy risk assessment and shape the selection of privacy controls.[37] Risk assessment results are also leveraged when identifying common controls to determine if the controls available for inheritance meet the security and privacy requirements for the system and its environment of operation. When common controls provided by the organization are not sufficient for systems inheriting the controls, system owners either supplement the common controls with system-specific or hybrid controls to achieve the required protection for the system or accept greater risk.

The security and privacy plans contain an overview of the security and privacy requirements for the system in sufficient detail to determine that the security and privacy controls selected by the organization would meet those requirements if implemented correctly. In addition to the list of security and privacy controls, the security and privacy plans describe the intended application of each control in the context of the system with sufficient detail to enable a compliant implementation of the control and subsequent assessment of control effectiveness. Specifically, the security and privacy control documentation describes how system-specific and hybrid controls are implemented and the plans and expectations regarding the functionality of the system. The functional description of the planned security and privacy control implementation includes planned inputs, expected behavior, and expected outputs where appropriate, typically for those technical controls that are employed in the hardware, software, or firmware components of the system. Inherited controls are annotated in the security and privacy plans. There is no requirement to provide common control implementation details in security and privacy plans. Rather, those details are provided in the security and privacy plans for common control providers and are available to system owners upon request. Organizations may develop a single, integrated security and privacy plan or maintain separate plans.

Privacy programs collaborate on the development of the security aspect of plans in two principal respects. When security controls provide privacy protections with respect to managing the confidentiality, integrity, and availability of personally identifiable information, privacy programs collaborate to ensure that the plan reflects the appropriate selection of these controls. When programs have separate privacy plans, they may cross-reference these controls to maintain appropriate awareness and accountability. In other contexts, security controls can be implemented in ways that give rise to privacy risks. The privacy program supports documentation of these privacy risk considerations and specific implementations intended to mitigate them.

[35] NIST Interagency Report 8062 introduces privacy risk management and a privacy risk model for conducting privacy risk assessments.

[36] NIST Special Publication 800-53 includes a privacy control baseline that addresses federal privacy requirements and privacy risks relating to the authorized processing of personally identifiable information. Security control baselines can be used to manage the confidentiality, integrity, and availability of personally identifiable information. Together, a privacy control baseline and a security control baseline (with appropriate tailoring) provide a comprehensive set of safeguards to manage individuals' privacy.

[37] NIST Interagency Report 8062 provides a discussion of context and its function in a privacy risk model.

Security and privacy plans also describe how joint (security and privacy) controls are to be implemented, and clearly delineate roles and responsibilities for their implementation and assessment.[38]

Documentation of planned security and privacy control implementations allows for traceability of decisions prior to and after the deployment of the system. To the extent possible, organizations reference existing documentation (either by vendors or other organizations that have employed the same or similar systems), use automated support tools, and maximize communications to increase the overall efficiency and cost-effectiveness of security and privacy control documentation. The documentation also addresses platform dependencies and includes any additional information necessary to describe how the security and privacy capability required is to be achieved at the level of detail sufficient to support control implementation and assessment. Documentation for security and privacy control implementations follows best practices for hardware and software development as well as for systems security and privacy engineering disciplines and is consistent with established organizational policies and procedures for documenting system development life cycle activities.

For security and privacy controls that are mechanism-based, organizations take maximum advantage of the functional specifications provided by or obtainable from hardware and software developers and systems integrators. This includes any security- or privacy-relevant documentation that may assist the organization during the development, implementation, assessment, and monitoring of security and privacy controls. For management and operational controls, organizations obtain security and privacy control implementation information from the appropriate organizational entities including, for example, physical security offices, facilities offices, records management offices, and human resource offices. Since the enterprise architecture and the security and privacy architectures established by the organization influence the organizational approach used to plan for and implement security and privacy controls, documenting the process helps to ensure traceability in meeting the stakeholder's security and privacy requirements.

References: FIPS Publications 199, 200; NIST Special Publications 800-18, 800-30, 800-53, 800-160 (System Requirements Definition, Architecture Definition, and Design Definition Processes), 800-161 (Respond and Chapter 3); NIST Interagency Report 8179; CNSS Instruction 1253; Cybersecurity Framework (Core [Identify, Protect, Detect, Respond, Recover Functions]; Profiles).

SYSTEM-LEVEL MONITORING STRATEGY

Task 2 Supplement the organizational continuous monitoring strategy at the system level, as needed.

Potential Inputs: Organizational risk management strategy; organizational continuous monitoring strategy; organizational and system risk assessments; system security and privacy plans; organizational security and privacy policies.

Potential Outputs: Continuous monitoring strategy for the system.

Primary Responsibility: System Owner; Common Control Provider.

System Development Life Cycle Phase: New – Development/Acquisition.
Existing – Operations/Maintenance.

Supplemental Guidance: An important aspect of risk management is the ongoing monitoring of security and privacy controls employed within or inherited by the system. An effective monitoring strategy at the system level is developed and implemented in coordination with the organizational continuous monitoring strategy early in the system development life cycle (i.e., during system design or COTS procurement decision). The system-level monitoring strategy supplements the organizational monitoring strategy—that is, the system-level strategy addresses monitoring only the security and privacy controls for which monitoring is not provided as part of the organizational strategy and implementation. The system-level monitoring strategy identifies the frequency of monitoring for security and privacy controls not addressed

[38] NIST Special Publication 800-53 defines joint controls as controls and control enhancements that can address security and privacy requirements. Organizations may opt to do a joint implementation or alternatively, the privacy program and security program may implement the respective privacy and security aspects of the control or enhancement separately.

by the organizational strategy and defines the approach for assessing those controls. The system-level strategy, consistent with the organizational strategy, may also define how changes to the system are to be monitored, how security and privacy impact analyses are to be conducted, and the security and privacy status reporting requirements including recipients of the status reports. The system level monitoring strategy can be included in security and privacy plans.

For implemented security and privacy controls not addressed by the organizational monitoring strategy, the criteria for determining the frequency with which controls are monitored post-deployment is established by the system owner or common control provider in collaboration with organizational officials including, for example, the authorizing official or designated representative; chief information officer; senior agency information security officer; senior agency official for privacy; and senior accountable official for risk management/risk executive (function). The frequency criteria at the system level reflect the priorities and the importance of the system to organizational operations and assets, individuals, other organizations, and the Nation. Security and privacy controls that are volatile (i.e., most likely to change over time), critical to certain aspects of the protection strategy for the organization, or identified in plans of action and milestones may require more frequent assessment. The approach to security and privacy control assessments during continuous monitoring may include detection of the status of system components; analysis of historical and operational data; and the reuse of assessment procedures and results that supported the initial authorization decision.

The authorizing official or designated representative approves the system-level monitoring strategy including the minimum frequency with which each security and privacy control is to be monitored. The approval of the strategy can be obtained in conjunction with the security and privacy plan approval. The monitoring of security and privacy controls continues throughout the system development life cycle.

References: NIST Special Publications 800-30, 800-39 (Organization, Mission/Business Process, System Levels), 800-53, 800-53A, 800-161, 800-137; Cybersecurity Framework (Core [Detect Function]); CNSS Instruction 1253.

SECURITY AND PRIVACY PLAN APPROVAL

Task 3 Review and approve the security and privacy plans.

Potential Inputs: Completed system security and privacy plans; system risk assessment.

Potential Outputs: System security and privacy plans approved by the authorizing official.

Primary Responsibility: Authorizing Official or Designated Representative.

System Development Life Cycle Phase: New – Development/Acquisition.
Existing – Operations/Maintenance.

Supplemental Guidance: The independent review of the security and privacy plans by the authorizing official or designated representative with support from the chief information officer, senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management/risk executive (function), helps determine if the plan is complete, consistent, and satisfies the stated security and privacy requirements for the system. Based on the results of this independent review and analysis, the authorizing official or designated representative may recommend changes to the security and privacy plans. If the security and privacy plans are unacceptable, the system owner or common control provider makes appropriate changes to the plans. If the security and privacy plans are acceptable, the authorizing official or designated representative approves the plans. The acceptance of the security and privacy plans represents an important milestone in the system development life cycle and risk management process. The authorizing official or designated representative, by approving the security and privacy plans, agrees to the set of security and privacy controls (i.e., system-specific, hybrid, or common controls) and the functional description of the planned control implementations proposed to meet the security and privacy requirements for the system and the environment in which the system operates. This approval allows the risk management process to advance to the next step in the RMF (i.e., the implementation of the security and privacy controls). The approval of the security and privacy plans also establishes the appropriate level of effort required to successfully complete the remainder of the RMF steps and provides the basis of the security and privacy specifications for the acquisition of the system, subsystems, or components.

References: NIST Special Publications 800-30, 800-53, 800-160 (System Requirements Definition, Architecture Definition, and Design Definition Processes); CNSS Instruction 1253.

3.4 IMPLEMENTATION

Purpose

The purpose of the *Implementation* step is to implement the security and privacy controls described in the security and privacy plans for the system and the organization and to document in a baseline configuration, the specific details of the control implementation.

Outcomes

- Security and privacy controls specified in the system security and privacy plans are implemented.
- Systems security and privacy engineering methodologies are used to implement the security and privacy controls specified in the system security and privacy plans.
- The security and privacy configuration baseline is established.
- The system security and privacy plans are updated based on specific information obtained during the implementation of the security and privacy controls.

Tasks

Quick link to summary table for RMF Implementation tasks

IMPLEMENTATION

SECURITY AND PRIVACY CONTROL IMPLEMENTATION

Task 1 Implement the security and privacy controls specified in the security and privacy plans or other system documentation.

Potential Inputs: Approved system security and privacy plans; system design documents; organizational security and privacy policy and procedures; enterprise architecture information; security and privacy architecture information; list of security and privacy requirements allocated to the system and to system elements; list of security and privacy requirements allocated to the environment of operation; business impact or criticality analyses; system element information and system component inventory.

Potential Outputs: Fully implemented security and privacy controls.

Primary Responsibility: System Owner; Common Control Provider.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Supplemental Guidance: Security and privacy control implementation is consistent with the organization's enterprise architecture and security and privacy architecture. The security and privacy architecture serves as a resource to allocate security and privacy controls to a system and any organization-defined subsystems. Security and privacy controls targeted for deployment within the system are allocated to specific system components (i.e., system elements) providing a security and privacy capability. Not all security and privacy controls are allocated to every subsystem or to all system components or subsystem. The categorization of subsystems, the security and privacy architectures, and the allocation of security and privacy controls work together to help achieve a suitable balance. Allocating a subset of security and privacy controls as common controls or hybrid controls is part of the security and privacy architecture.

Organizations use best practices when implementing the security and privacy controls including systems and security and privacy engineering methodologies, concepts, and principles. Risk assessments may guide and inform decisions regarding the cost, benefit, and risk trade-offs in using different technologies or policies for control implementation. In addition, organizations ensure that mandatory configuration settings are established and implemented on information technology products in accordance with federal and organizational policies. When there is no direct control over what security and privacy controls are implemented in a system component, for example, in commercial off-the-shelf products, organizations consider the use of system components that have been tested, evaluated, or validated by approved, independent, third-party assessment facilities. In addition, organizations address, where applicable, assurance requirements when implementing security and privacy controls. Assurance requirements are directed at the activities and actions that security and privacy control developers and implementers define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system. Assurance requirements address quality of the design, development, and implementation of the security and privacy functions in the system.[39]

For the common controls inherited by the system, systems security and privacy engineers with support from system security and privacy officers, coordinate with the common control provider to determine the most appropriate way to apply the common controls to organizational systems. System owners can refer to the authorization packages prepared by common control providers when making determinations regarding the adequacy of the implementations of common controls for their systems. For common controls that do not meet the protection needs of the systems inheriting the controls or that have unacceptable weaknesses or deficiencies, the system owners identify compensating or supplementary controls to be implemented. Risk assessments may determine how gaps in protection needs between systems and common controls affect the overall risk associated with the system, and how to prioritize the need for compensating or supplementary controls to mitigate specific risks.

Consistent with the flexibility allowed in applying the tasks in the RMF, organizations conduct initial control assessments during system development and implementation. Conducting such assessments in parallel with the development and implementation phases of the system development life cycle facilitates early identification of weaknesses and deficiencies and provides a cost-effective method for initiating corrective actions. Issues discovered during these assessments can be referred to authorizing officials for resolution. The results of the initial control assessments can also be used during the authorization process to avoid delays or costly repetition of assessments. Assessment results that are subsequently reused in other phases of the system development life cycle meet the reuse requirements (including independence) established by the organization.

References: FIPS Publication 200; NIST Special Publications 800-30, 800-53, 800-53A, 800-160 (Implementation, Integration, Verification, and Transition Processes), 800-161; NIST Interagency Reports 8062, 8179; CNSS Instruction 1253.

BASELINE CONFIGURATION

Task 2 Document changes to planned security and privacy control implementation and establish the configuration baseline for the system.

Potential Inputs: System security and privacy plans; information from security and privacy control implementation efforts.

Potential Outputs: System security and privacy plans updated with implementation detail sufficient for use by assessors; system configuration baseline.

Primary Responsibility: System Owner; Common Control Provider.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

[39] NIST Special Publication 800-53 provides a list of assurance related security and privacy controls.

Supplemental Guidance: Despite the specific security and privacy control implementation details in the security and privacy plans and the system design documents, it is not always possible to implement controls as planned. Thus, as control implementations are finalized, the security and privacy plans are updated with the as-deployed control implementation details. The updates include revised functional descriptions of the implemented controls including any changes to planned inputs, expected behavior, and expected outputs with sufficient detail to support control assessments. Configuration baselines are established for all aspects of the system including hardware, software, and firmware configurations. These baselines are essential when implementing a continuous monitoring process to have the capability to determine when there are changes to the system, whether those changes are authorized, and the impact of the changes on the security and privacy state of the system and organization.

References: NIST Special Publications 800-53, 800-160 (Implementation, Integration, Verification, and Transition, Configuration Management Processes); CNSS Instruction 1253.

3.5 ASSESSMENT

Purpose

The purpose of the *Assessment* step is to determine if the security and privacy controls selected are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system.

Outcomes

- Security and privacy assessment plans are developed and documented.
- Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and to bind the level of effort.
- The appropriate level of independence is obtained by the assessment teams.
- Documentation needed to conduct the assessments is provided to the assessment teams.
- Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered.
- Use of automation to conduct security and privacy control assessments is maximized to increase the speed, effectiveness, and efficiency of the assessments.
- Security and privacy control assessments are conducted in accordance with the security and privacy assessment plans.
- Security and privacy assessment reports that provides findings and recommendations are completed.
- Remediation actions to address weaknesses or deficiencies in controls implemented in the system and its environment of operation are taken.
- The system security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions.

Tasks

Quick link to summary table for RMF Assessment tasks

ASSESSMENT

ASSESSMENT PREPARATION

Task 1 Develop, review, and approve a plan to assess the security and privacy controls in the system and the organization.

Potential Inputs: System security and privacy plans; supply chain risk management plan; system design documentation; enterprise, security, and privacy architecture information; policies and procedures applicable to the system.

Potential Outputs: Security and privacy assessment plans approved by the authorizing official.

Primary Responsibility: Control Assessor.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Supplemental Guidance: The security and privacy assessment plans are based on the implementation details in the system security and privacy plans and provides the objectives for the security and privacy control assessments, a detailed roadmap of how to conduct such an assessment, and the assessment procedures. The security assessment plan reflects the type of assessment the organization is conducting, for example, developmental testing and evaluation; independent verification and validation; audits, including supply chain; assessments supporting system and common control authorization or reauthorization; continuous monitoring; and assessments conducted after remediation actions. Conducting security and privacy control assessments during the development, acquisition, implementation, and assessment phases of the system development life cycle permits the early identification of weaknesses and deficiencies and provides the most cost-effective method for initiating corrective actions. The issues discovered during these assessments can be referred to authorizing officials for resolution. The results of control assessments during the system development life cycle can also be used (consistent with reuse criteria) during the authorization process to avoid system fielding delays or costly repetition of assessments.

The security and privacy assessment plans are reviewed and approved by appropriate organizational officials to ensure that the plan is consistent with the security and privacy objectives of the organization; employs procedures, techniques, tools, and automation to support the concept of continuous monitoring and near real-time risk management; and is cost-effective with respect to the resources allocated for the assessment. The purpose of the security and privacy assessment plan approval is two-fold: to establish the expectations for the control assessment and to bind the level of effort for the assessment. Approved security and privacy assessment plans help to ensure that an appropriate level of resources is applied toward determining security and privacy control effectiveness. When controls are provided by an external provider through contracts, interagency agreements, lines of business arrangements, licensing agreements, or supply chain arrangements, the organization can request security and privacy assessment plans from the provider.

Organizations consider both the technical expertise and level of independence required in selecting control assessors. Organizations ensure that control assessors possess the required skills and technical expertise to carry out assessments of system-specific, hybrid, and common controls. This includes knowledge of and experience with the specific hardware, software, and firmware components employed by the organization. Security and privacy control assessments in support of initial and subsequent system and common control authorizations are conducted by independent assessors if the system is categorized as moderate or high impact. An independent assessor is an individual/group capable of conducting an impartial assessment of security and privacy controls employed within or inherited by a system. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with respect to the determination of security and privacy control effectiveness or the development, operation, or management of the system.

Independent 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 assessment services are considered independent if the system owner or common control provider is not directly involved in the contracting process or cannot influence the independence of the assessors conducting the assessment of the security and privacy controls. The authorizing official or designated representative determines the required level of independence for control assessors based on the results of the security categorization process or privacy risk assessments for the system and the risk to organizational operations and assets, individuals, other organizations, and the Nation. In special situations, for example when the organization that owns the system is small or the organizational structure requires that the security and privacy control assessments be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner, 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 consults with the Office of the Inspector General, chief information officer, senior agency information security officer, and senior agency official for privacy, to discuss the implications of decisions regarding assessor independence in the types of special circumstances described above.

References: NIST Special Publications 800-53A, 800-160 (Verification and Validation Processes), 800-161.

SECURITY AND PRIVACY CONTROL ASSESSMENTS

Task 2 Assess the security and privacy controls in accordance with the assessment procedures defined in the security and privacy assessment plans.

Potential Inputs: Security and privacy assessment plans; system security and privacy plans; assessment objects as specified in the assessment plan; external assessment or audit results (if applicable).

Potential Outputs: Completed security and privacy control assessments and associated assessment evidence.

Primary Responsibility: Control Assessor.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Supplemental Guidance: Security and privacy 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 and privacy requirements for the system. Security and privacy control assessments occur as early as practicable in the system development life cycle, preferably during the development phase of the system. These types of assessments are referred to as developmental testing and evaluation and are intended to validate that the required security and privacy controls are implemented correctly and are consistent with the established information security and privacy architecture. Developmental testing and evaluation activities include, for example, design and code reviews, application scanning, and regression testing. Security weaknesses and deficiencies identified early in the system development life cycle can be resolved more quickly and in a more cost-effective manner. Assessments may be needed prior to source selection during the procurement process to assess potential suppliers or providers before the organization enters agreements or contracts to begin the development phase.

The system owner relies on the technical expertise of assessors to assess the security and privacy controls employed within or inherited by the system using the assessment procedures specified in the security and privacy assessment plans and provide recommendations on how to correct weaknesses or deficiencies in the controls and reduce or eliminate identified vulnerabilities. The assessor findings are intended to be a factual reporting of the weaknesses and deficiencies in the security and privacy controls discovered during the assessment. Organizations are encouraged to maximize the use of automation to conduct security and privacy control assessments to increase the speed, effectiveness, and efficiency of the assessments, and to support the concept of ongoing monitoring of the security and privacy state of organizational systems.

When iterative development processes such as agile development are employed, this typically results in an iterative assessment as each cycle is conducted. A similar process is used for assessing security and privacy controls in commercial information technology products employed within the system. Organizations may choose to begin assessing security and privacy controls prior to the complete implementation of all controls in the security and privacy plans. This type of incremental assessment is appropriate if it is more efficient or cost-effective to do so. Common controls (i.e., security and privacy controls that are inherited by the system) are assessed by common control providers and need not be assessed by system owners.

Organizations ensure that assessors have access to the system and environment of operation where the security and privacy controls are employed and to the appropriate documentation, records, artifacts, test results, and other materials needed to assess the controls. This includes situations when security and privacy controls are provided by external providers through contracts, interagency agreements, lines of business arrangements, licensing agreements, or supply chain arrangements. In addition, assessors have the required degree of independence as determined by the authorizing official. Security and privacy control assessments in support of initial and subsequent system and common control authorizations are conducted by independent assessors if the system is categorized as moderate or high impact. Assessor independence during continuous monitoring, although not specifically mandated, facilitates reuse of assessment results to support ongoing authorization and reauthorization, if required.

To make the risk management process as timely and cost-effective as possible, organizations can reuse previous assessment results when reasonable and appropriate and when conducted in accordance with the established organizational criteria for reuse. For example, a recent audit of a system may have produced

information about the effectiveness of selected security and privacy controls. Another opportunity to reuse previous assessment results comes from programs that test and evaluate security and privacy features of commercial information technology products. Additionally, if prior assessment results from the system developer are available, the control assessor, under appropriate circumstances, may incorporate those results into the control assessment. And finally, assessment results are reused to support reciprocity where possible.

References: NIST Special Publications 800-53A, 800-160 (Verification and Validation Processes).

SECURITY AND PRIVACY ASSESSMENT REPORTS

Task 3 Prepare the security and privacy assessment reports documenting the issues, findings, and recommendations from the security and privacy control assessments.

Potential Inputs: Completed security and privacy control assessments and associated assessment evidence.

Potential Outputs: Completed security and privacy assessment reports detailing findings and recommendations.

Primary Responsibility: Control Assessor.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Supplemental Guidance: The results of the security and privacy control assessments, including the recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the security and privacy assessment reports. The security and privacy assessment reports are key documents in the system or common control authorization package developed for authorizing officials. The assessment report includes information from the assessor necessary to determine the effectiveness of the security and privacy controls employed within or inherited by the system based upon the assessor's findings. The security and privacy assessment reports are an important factor in an authorizing official's determination of risk to organizational operations and assets, individuals, other organizations, and the Nation. The reporting format and level of detail provided in the assessment report is appropriate for the type of control assessment conducted, for example, self-assessments; developmental testing and evaluation; independent verification and validation; independent assessments supporting the system or common control authorization process or subsequent reauthorizations; assessments subsequent to remediation actions; assessments during continuous monitoring; and independent audits or evaluations. The reporting format may also be prescribed by the organization.

Security and privacy control assessment results obtained during system development are brought forward in an interim report and included in the final security and privacy assessment reports. This reinforces the concept that the security and privacy assessment reports are evolving documents that include assessment results from all relevant phases of the system development life cycle including the results generated during continuous monitoring. Organizations may choose to develop an executive summary from the security and privacy control assessment findings. The executive summary provides authorizing officials and other interested individuals with an abbreviated version of the security and privacy assessment reports focusing on the highlights of the assessment, synopsis of key findings, and the recommendations for addressing weaknesses and deficiencies in the security and privacy controls.

References: NIST Special Publications 800-53A, 800-160 (Verification and Validation Processes).

REMEDIATION ACTIONS

Task 4 Conduct initial remediation actions on security and privacy controls based on the findings and recommendations of the security and privacy assessment reports; reassess remediated controls.

Potential Inputs: Completed security and privacy assessment reports detailing findings and recommendations; system security and privacy plans; security and privacy assessment plans.

Potential Outputs: Completed initial remediation actions based on the security and privacy assessment reports; changes to implementations reassessed by the assessment team; updated security and privacy

assessment reports and system security and privacy plans including changes to the security and privacy control implementations.

Primary Responsibility: System Owner; Common Control Provider; Control Assessor.

System Development Life Cycle Phase: New – Development/Acquisition; Implementation/Assessment.
Existing – Operations/Maintenance.

Supplemental Guidance: The security and privacy assessment reports provide visibility into weaknesses and deficiencies in the security and privacy controls employed within or inherited by the system that could not reasonably be resolved during system development or that are discovered post-development. Such weaknesses and deficiencies are potential vulnerabilities if exploitable by a threat source or are creating privacy risks. The findings generated during the security and privacy control assessments provide information that facilitates a disciplined and structured approach to responding to risks in accordance with organizational priorities. An updated assessment of risk based on the results of the findings produced during the security and privacy control assessments and any inputs from the senior accountable official for risk management/risk executive (function), determines the initial remediation actions and the prioritization of such actions. System owners and common control providers may decide, based on an initial or updated risk assessment, that certain findings are inconsequential and present no significant risk to the organization. Such findings constitute accepted (or residual) risk and are retained in the security and privacy assessment reports and monitored during the continuous monitoring step. Alternatively, organizational officials may decide that certain findings are in fact, significant, requiring immediate remediation actions.

In all cases, organizations review assessor findings and determine 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 sufficiently significant to be worthy of further investigation or remediation. Senior leadership involvement in the mitigation process may be necessary to ensure that the organization's resources are effectively allocated in accordance with organizational priorities, providing resources to the systems that are supporting the most critical and sensitive missions and business functions for the organization or correcting the deficiencies that pose the greatest risk. If weaknesses or deficiencies in security and privacy controls are corrected, assessors reassess the remediated controls. Security and privacy control reassessments 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 and privacy requirements for the system and organization. The assessors update the security and privacy assessment reports with the findings from the reassessment, exercising caution not to change the original assessment results. The security and privacy plans are updated based on the findings of the security and privacy control assessments and any remediation actions taken. The updated security and privacy plans reflect the state of the controls after the initial assessment and any modifications by the system owner or common control provider in addressing recommendations for corrective actions. At the completion of the security and privacy control assessments, the security and privacy plans contain an accurate description of the security and privacy controls implemented including compensating controls.

Organizations can prepare an addendum to the security and privacy assessment reports that provide system owners and common control providers an opportunity to respond to the initial findings of assessors. The addendum may include, for example, information regarding initial remediation actions taken by system owners or common control providers in response to assessor findings. The addendum can also provide the system owner or common control provider perspective on the findings, including additional explanatory material, rebutting certain findings, and correcting the record. The addendum does not change or influence in any manner, the initial assessor findings provided in the report. Information provided in the addendum is considered by authorizing officials in their risk-based authorization decisions. Organizations may choose to employ an issue resolution process to help determine the appropriate actions to take regarding the security and privacy control weaknesses and deficiencies identified during the assessment. Issue resolution can help address vulnerabilities and associated risk, false positives, and other factors that provide useful information to authorizing officials regarding the security and privacy state of the system and organization including the ongoing effectiveness of system-specific, hybrid, and common controls. The issue resolution process can also ensure that only substantive items are identified and transferred to the plan of actions and milestones.

References: NIST Special Publications 800-53A, 800-160 (Verification and Validation Processes).

3.6 AUTHORIZATION

Purpose

The purpose of the *Authorization* step is to provide strict accountability by requiring a senior management official to determine if the security and privacy risk to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable.

Outcomes

- A plan of action and milestones detailing remediation plans for unacceptable risks identified in the security and privacy assessment reports is developed.
- An authorization package or comparable report from a security/privacy management tool for submission to the authorizing official is generated.
- A risk determination by the authorizing official that reflects the organizational risk management strategy including risk tolerance, is rendered.
- The authorization for the system or the common controls is approved or denied.
- Authorization decisions and significant vulnerabilities are reported to organizational officials.

Tasks

Quick link to summary table for RMF Authorization tasks

AUTHORIZATION

PLAN OF ACTION AND MILESTONES

Task 1 Prepare the plan of action and milestones based on the findings and recommendations of the security and privacy assessment reports excluding any remediation actions taken.

Potential Inputs: Updated security and privacy assessment reports; updated system security and privacy plans; system and organizational risk assessment results; organizational risk management strategy and risk tolerance.

Potential Outputs: A plan of action and milestones detailing the findings from the security and privacy assessment reports that are to be remediated.

Primary Responsibility: System Owner; Common Control Provider.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

Supplemental Guidance: The plan of action and milestones, prepared for the authorizing official by the system owner or the common control provider, is a key document in the authorization package. It describes the specific tasks that are planned to correct any weaknesses or deficiencies in the security and privacy controls noted during the assessment and continuous monitoring and to address unacceptable vulnerabilities in the system. The plan of action and milestones identifies the specific tasks to be accomplished with a recommendation for completion either before or after system implementation; the resources required to accomplish the tasks; milestones established to meet the tasks; and the scheduled completion dates for the milestones. The plan of action and milestones is used by the authorizing official to monitor progress in

correcting weaknesses or deficiencies noted during the security and privacy control assessments. Plan of action and milestones entries are not required when the identified weaknesses or deficiencies are accepted as residual risk or remediated during the assessment or prior to the submission of the authorization package to the authorizing official. However, all security and privacy weaknesses and deficiencies identified during assessment and monitoring are documented in the security and privacy assessment reports or are retained within an automated security/privacy management and reporting tool to maintain an effective audit trail. Organizations develop plans of action and milestones based on the results of assessment and monitoring and in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, or guidance.

Organizations 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 ensures that plans of action and milestones are based on the security categorization of the system and privacy risk assessments; the specific weaknesses or deficiencies in the security and privacy controls; the criticality of the identified control weaknesses or deficiencies (i.e., the direct or indirect effect the weaknesses or deficiencies may have on the security and privacy state of the system, and therefore, on the risk exposure of the organization, or ability of the organization to perform its mission or business functions); and the organization's proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security and privacy controls, including, for example, prioritization of risk mitigation actions and allocation of risk mitigation resources. A risk assessment guides the prioritization process for items included in the plan of action and milestones.

References: NIST Special Publications 800-30, 800-53A, 800-160 (Verification and Validation Processes); NIST Interagency Report 8062.

AUTHORIZATION PACKAGE

Task 2 Assemble the authorization package with an executive summary and submit the package to the authorizing official for adjudication.

Potential Inputs: Updated system security and privacy plans; updated security and privacy assessment reports; plan of action and milestones; supporting assessment evidence or other documentation, as required.

Potential Outputs: Authorization package (with an executive summary) or comparable report from a security/privacy management tool for submission to the authorizing official.[40]

Primary Responsibility: System Owner; Common Control Provider.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

Supplemental Guidance: The system and common control authorization packages contain the security and privacy plans, security and privacy assessment reports, plans of action and milestones, and an executive summary. Additional information can be included in the authorization package at the request of the authorizing official. The authorization package documents may be provided to the authorizing official in hard copy or electronically, or may be generated using an automated security/privacy management and reporting tool. The contents of the authorization package are protected appropriately in accordance with federal and organizational policies. Organizations maintain strict version control as the documents in the authorization package are updated.

The information in the authorization documents is used by authorizing officials to make informed, risk-based decisions. When security and privacy controls are provided to an organization by an external provider through contracts, interagency agreements, lines of business arrangements, licensing agreements,

[40] Organizations are encouraged to maximize the use of automated tools in the preparation, assembly, and transmission of authorization packages and security- and privacy-related information supporting the authorization process. Many commercially available governance, risk, and compliance (GRC) tools can be employed by organizations to reduce or eliminate hard copy documentation.

or supply chain arrangements, the organization ensures that the information needed by authorizing officials to make risk-based decisions, is made available by the provider.

Organizations are encouraged to use automated support tools, for example, an automated security/privacy management and reporting tool, in preparing and managing the content of the authorization package. Such tools help provide an effective vehicle for maintaining and updating information for authorizing officials regarding the ongoing security and privacy status of systems within the organization. Providing timely updates to the security and privacy plans, security and privacy assessment reports, and plans of action and milestones on an ongoing basis, supports the concept of near real-time risk management and ongoing authorization. It also facilitates cost-effective and meaningful reauthorization actions, if required.

When the system is under ongoing authorization, the authorizing official requires information from the security and privacy plans, security and privacy assessment reports, and the plans of action and milestones to make ongoing risk determinations and risk acceptance decisions. To support ongoing authorization and to provide information to the authorizing official in the most efficient and timely manner possible, the authorization package is presented to the authorizing official via automated reports.[41] Information to be presented in security and privacy assessment reports is generated using the near-real time security- and privacy-related information from the information security and information privacy continuous monitoring programs, respectively. The information from the assessment reports is presented to the authorizing official in a report using an automated security/privacy management and reporting tool, the format and frequency of which is determined by the organization.

The security and privacy assessment reports presented to the authorizing official includes security- and privacy-related information regarding implemented system-specific, hybrid, and common controls. The authorizing official uses automated security/privacy management and reporting tools or other automated methods to access the security and privacy plans and the plans of action and milestones. The currency of the authorization documents is maintained in accordance with the risk management objectives of the organization using automated or manual update processes. While the initial data entry for the authorization package may be automated, procedural/manual, or both, to support ongoing authorization and near real-time risk management objectives, it is important that such information be accessible to the authorizing official in an automated fashion.[42]

References: NIST Special Publications 800-18, 800-160 (Risk Management Process).

RISK DETERMINATION

Task 3 Determine the risk from the operation or use of the system or the provision of common controls.

Potential Inputs: Authorization package or comparable report from a security/privacy management tool for submission to the authorizing official; supporting assessment evidence or other documentation as required; organizational risk management strategy and risk tolerance.

Potential Outputs: Risk determination.

Primary Responsibility: Authorizing Official or Designated Representative.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

[41] While the objective is to fully automate all components of the authorization package, organizations may be in various states of transition to such a fully automated state—that is, with certain sections of the authorization package available via automated means and other sections available only through procedural/manual means.

[42] Organizations decide on the level of detail and the presentation format of security- and privacy-related information that is made available to authorizing officials through automation. These decisions are based on organizational needs with the automated presentation of security- and privacy-related information tailored to the decision-making needs of the authorizing officials. For example, very detailed security- and privacy-related information may be generated and collected at the operational level of the organization with information subsequently analyzed, distilled, and presented to authorizing officials in a summarized or highlighted format using automation.

Supplemental Guidance: The authorizing official or designated representative, in collaboration with the senior agency information security officer and senior agency official for privacy, analyzes the information provided by the system owner or common control provider regarding the current security and privacy state of the system or the common controls inherited by the system and the recommendations for addressing any residual risks. Risk assessments are employed at the discretion of the organization to provide information on threats, vulnerabilities, privacy risks, and potential impacts and the analyses for the risk mitigation recommendations. The senior accountable official for risk management and/or risk executive (function) may also provide information to the authorizing official that is considered in the final determination of risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation or use of the system or the provision of common controls. Risk-related information includes the criticality of the missions/business functions supported by the system and the risk management strategy for the organization. The authorizing official considers information obtained from the senior accountable official for risk management/risk executive (function) and information provided by the system owner or common control provider in the authorization package when making a risk determination. Conversely, the security- and privacy-related risk information derived from execution of the RMF is available to the senior accountable official for risk management/risk executive (function) for use in formulating and updating the organization-wide risk management strategy.

When the system is under ongoing authorization, the risk determination task is effectively unchanged. The authorizing official assesses the security- and privacy-related information provided by the automated security/privacy management and reporting tool regarding the current security and privacy state of the system and the inherited common controls. The authorizing official also assesses the recommendations for responding to the identified risks based on the risk management strategy (including organizational risk tolerance).

References: NIST Special Publications 800-30, 800-39 (Organization, Mission/Business Process, and System Levels), 800-160 (Risk Management Process); NIST Interagency Report 8062.

RISK RESPONSE

Task 4 Identify and implement a preferred course of action in response to the risk determined.

Potential Inputs: Authorization documents/reports; risk determination.

Potential Outputs: Risk responses for determined risks.

Primary Responsibility: Authorizing Official or Designated Representative.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

Supplemental Guidance: After risk is analyzed and determined, organizations can respond to risk in a variety of ways, including accepting risk; avoiding risk; mitigating risk; sharing risk; transferring risk; or a combination of the above. Decisions on the most appropriate course of action for responding to risk include some form of prioritization. Some risks may be of greater concern to organizations than other risks. In that case, more resources may need to be directed at addressing higher-priority risks versus lower-priority risks. This does not necessarily mean that the lower-priority risks are ignored. Rather, it could mean that fewer resources are directed at the lower-priority risks, or that the lower-priority risks are addressed later. A key part of the risk-based decision process is the recognition that regardless of the risk decision, there remains a degree of residual risk. Organizations determine acceptable degrees of residual risk based on organizational risk tolerance. When the response to risk is mitigation, the planned mitigation actions are included in and tracked using the plan of action and milestones. When the response to risk is acceptance, the risk finding remains documented in the security and privacy assessment reports and is monitored for changes to risk factors.

References: NIST Special Publications 800-30, 800-39 (Organization, Mission/Business Process, and System Levels), 800-160 (Risk Management Process); NIST Interagency Reports 8062, 8179; Cybersecurity Framework (Core [Respond Function]).

AUTHORIZATION DECISION

Task 5 Determine if the risk from the operation or use of the system or the provision or use of common controls is acceptable.

Potential Inputs: Risk responses for determined risks.

Potential Outputs: Authorization to operate, authorization to use, common control authorization; denial of authorization to operate, denial of authorization to use, denial of common control authorization.

Primary Responsibility: Authorizing Official.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

Supplemental Guidance: The explicit acceptance of risk is the responsibility of the authorizing official. This responsibility cannot be delegated to other officials within the organization. The authorizing official considers many factors when deciding if the risk to organizational operations (including mission, function, image, and reputation), organizational assets, individuals, other organizations, or the Nation, is acceptable. Balancing security and privacy considerations with mission and business needs is paramount to achieving an acceptable risk-based authorization decision. The authorizing official issues an authorization decision for the system or for organizational common controls after reviewing the relevant information and, where appropriate, consulting with other organizational officials. The authorization decision is based on content in the authorization package and any inputs from other organizational officials. The authorization package provides information on the security and privacy state of the system or the common controls. Inputs from the senior accountable official for risk management/risk executive (function), including established risk guidance to the authorizing official, provide additional organization-wide information that may be relevant and affect the authorization decision. Such information includes, for example, organizational risk tolerance, mission and business requirements, dependencies among systems and security and privacy controls, and other types of risks not directly associated with the system or common controls. The inputs from the senior accountable official for risk management/risk executive (function) are documented and become part of the authorization decision. Authorization decisions are conveyed to system owners and common control providers and made available to interested parties within the organization.

The authorization decision document conveys the final authorization decision from the authorizing official to the system owner or common control provider, and other organizational officials, as appropriate.[43] The authorization decision document contains the authorization decision; terms and conditions; authorization termination date or time-driven authorization frequency; input from the senior accountable official for risk management/risk executive (function), if provided; and for common control authorizations, the impact level supported by the common controls. For systems, the authorization decision indicates to the system owner whether the system is authorized to operate or authorized to use, or not authorized to operate or authorized to use. For common controls, the authorization decision indicates to the common control provider and to inheriting systems, whether the common controls are authorized to be provided or not authorized to be provided. The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the system or the controls that must be followed by the system owner or common control provider. The authorization termination date, established by the authorizing official, indicates when the authorization expires. Organizations may eliminate the authorization termination date if the system is executing an ongoing authorization approach—that is, the continuous monitoring program is sufficiently robust to provide the authorizing official with the needed information to conduct ongoing risk determination and risk acceptance activities regarding the security and privacy state of the system and the ongoing effectiveness of security and privacy controls employed within and inherited by the system.

[43] Organizations are encouraged to employ automated security/privacy management and reporting tools to develop the authorization packages for systems and common controls and to maintain those packages during ongoing authorization. Automated tools can significantly reduce documentation costs, provide increased speed and efficiency in generating important information for decision makers, and provide more effective means for updating critical risk management information.

The authorization decision document is attached to the original authorization package containing the supporting documentation and transmitted to the system owner or common control provider. Upon receipt of the authorization decision document and original authorization package, the system owner or common control provider acknowledges and implements the terms and conditions of the authorization and notifies the authorizing official. The organization ensures that authorization documents for systems and common controls are made available to organizational officials including, for example, system owners inheriting common controls; chief information officers; senior accountable officials for risk management/risk executive (function); senior agency information security officers; senior agency officials for privacy; and system security and privacy officers. Authorization documents, including vulnerability information, are appropriately marked and protected in accordance with federal and organizational policies, and are retained in accordance with the record retention policy of the organization. The authorizing official verifies on an ongoing basis, that the terms and conditions established as part of the authorization are being followed by the system owner or common control provider.

When the system is under ongoing authorization, the authorizing official continues to be responsible and accountable for explicitly understanding and accepting the risk of continuing to operate or use the system or to provide common controls. Under ongoing authorization, the authorization termination date need not be specifically stated. Rather, the organization defines in its continuous monitoring strategy, the frequency, level of effort, and event triggers that inform the generation of information needed to make ongoing risk determinations and risk acceptance decisions. The authorizing official reviews the security- and privacy-related information with the specific time-driven authorization frequency defined by the organization as part of the continuous monitoring strategy and acknowledges that the risk of continued system operation or the provision of common controls remains acceptable—or indicates that the risk is no longer acceptable and requires a further risk response.

The organization determines the level of formality required for the acknowledgement of continuing risk acceptance by the authorizing official. The authorizing official may continue to convey the terms and conditions to be followed by the system owner or common control provider for continued authorization to operate, continued common control authorization, or continued authorization to use. The terms and conditions of the authorization may be conveyed through an automated security management and reporting tool, thus creating an automated authorization decision document. The authorizing official may also use the tool to annotate senior accountable official for risk management/risk executive (function) input.

If the security and privacy control assessments are conducted by qualified assessors with the required independence based on federal/organizational policies, appropriate security and privacy standards and guidelines, and the needs of the authorizing official, the assessment results support ongoing authorization and may also be cumulatively applied to a reauthorization. Organizational policies regarding ongoing authorization and reauthorization are consistent with laws, Executive Orders, directives, regulations, and policies.

Appendix C provides additional guidance on authorization decisions, the types of authorizations, and the preparation of the authorization packages.

References: NIST Special Publications 800-39 (Organization, Mission/Business Process, and System Levels), 800-160 (Risk Management Process).

AUTHORIZATION REPORTING

Task 6 Report the authorization decision and any weaknesses or deficiencies in security and privacy controls that represent significant vulnerabilities to the system or the organization.

Potential Inputs: Authorization decision document.

Potential Outputs: A report indicating the authorization decision for a system or set of common controls; report containing weaknesses or deficiencies in systems or security and privacy controls described in the Cybersecurity Framework functions, categories, and subcategories.

Primary Responsibility: Authorizing Official or Designated Representative.

System Development Life Cycle Phase: New – Implementation/Assessment.
Existing – Operations/Maintenance.

Supplemental Guidance: Authorizing officials report authorization decisions for systems and common controls to designated organizational officials so the individual risk decisions can be viewed in the context of organization-wide security and privacy risk to organizational operations and assets, individuals, other organizations, and the Nation. Reporting occurs only in situations where organizations have delegated the authorization functions to levels of the organization below the Agency Head or Chief Executive Officer. Authorizing officials also report any weaknesses or deficiencies in security and privacy controls noted during the assessment and continuous monitoring to address significant vulnerabilities in the system or the common controls. Such weaknesses or deficiencies that result in significant vulnerabilities are reported using the subcategories, categories, and functions described in the Cybersecurity Framework.

References: NIST Special Publications 800-39 (Organization, Mission/Business Process, and System Levels), 800-160 (Decision Management and Project Assessment and Control Processes); Cybersecurity Framework (Core [Identify, Protect, Detect, Respond, Recover Functions]).

3.7 MONITORING

Purpose

The purpose of the *Monitoring* step is to maintain an ongoing situational awareness about the security and privacy posture of the system and the organization in support of risk management decisions.

Outcomes

- Changes to the system and environment of operation are monitored in accordance with the continuous monitoring strategy.
- Security and privacy impact of changes to the system and environment of operation is analyzed.
- Ongoing assessments of security and privacy control effectiveness are conducted in accordance with the continuous monitoring strategy.
- The output of continuous monitoring activities is analyzed and responded to appropriately.
- A process is in place to report the security and privacy status to the authorizing official and other senior leaders and executives.
- Risk management documents are updated based on monitoring activities.
- Authorizing officials are conducting ongoing authorizations using the results of continuous monitoring activities and communicating changes in risk determination and acceptance decisions.
- A system decommissioning strategy is developed and implemented as needed.

Tasks

Quick link to summary table for RMF Monitoring tasks

MONITORING

SYSTEM AND ENVIRONMENT CHANGES

Task 1 Monitor changes to the system and its environment of operation.

Potential Inputs: Organizational continuous monitoring strategy; system security and privacy plans; configuration change requests/approvals; results from testing proposed changes; system design documentation; security and privacy assessment reports; plans of action and milestones; automated and manual monitoring tools.

Potential Outputs: Updated system security and privacy plans; updated plans of action and milestones; updated security and privacy assessment reports.

Primary Responsibility: System Owner; Common Control Provider; Senior Agency Information Security Officer.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

Supplemental Guidance: 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. A disciplined and structured approach to managing, controlling, and documenting changes to systems and environments of operation is an essential element of an effective security and privacy monitoring program. Organizations establish configuration management and control processes to support such monitoring activities. It is important to record relevant information about specific changes to hardware, software, and firmware such as version or release numbers, descriptions of new or modified features or capabilities, and security and privacy implementation guidance. It is also important to record changes to the environments of operation for systems, including, for example, modifications to hosting networks and facilities; new mission/business processes supported by systems; new or evolving threats; or modifications to the organizational risk management strategy. System owners and common control providers use this information in determining or assessing the potential security and privacy impact of the changes. Documenting proposed or actual changes to systems or environments of operation and subsequently assessing the potential impact those changes may have on the security and privacy state of systems or the organization is an important aspect of security and privacy control monitoring and maintaining system or common control authorization over time. Changes to systems or environments of operation may affect the security and privacy controls currently in place, produce new vulnerabilities or privacy risks in systems, or generate requirements for new controls that were not needed previously. Therefore, system changes are generally not undertaken prior to assessing the security and privacy impact of such changes. Organizations are encouraged to maximize the use of automation when managing changes to systems and environments of operation.

System owners and common control providers consult with appropriate organizational officials/entities prior to implementing changes to systems and environments of operation. This includes, for example, consulting with the configuration control board, senior agency information security officer, senior agency official for privacy, or system security officer. Authorizing officials or designated representatives review the security and privacy posture of systems via output from automated security/privacy management and reporting tools or updated security and privacy assessment reports. This review occurs in collaboration with the senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management/risk executive (function) to determine if a reauthorization action is necessary. Most changes to systems and environments of operation can be handled by the continuous monitoring program for the organization, thus supporting the concept of ongoing authorization and near real-time risk management. As risk assessments are updated, organizations use the findings and results to modify security and privacy plans based on the most recent threat, vulnerability, and privacy risk information available. Updated risk assessments provide a foundation for prioritizing and planning risk responses resulting from change. Authorizing officials or designated representatives, along with the senior accountable official for risk management/risk executive (function), confirm as needed, determinations of residual risk. The senior accountable official for risk management/risk executive (function) notifies the authorizing official of any significant changes in the organizational risk posture.

References: NIST Special Publications 800-30, 800-128; NIST Interagency Report 8062.

ONGOING ASSESSMENTS

Task 2 Assess the security and privacy controls employed within and inherited by the system in accordance with the organization-defined monitoring strategy.

Potential Inputs: Organizational continuous monitoring strategy; system security and privacy plans; security and privacy assessment plans; security and privacy assessment reports; plans of action and milestones; continuous monitoring strategy; risk assessment results; external assessment or audit results (if applicable); automated and manual monitoring tools.

Potential Outputs: Updated security and privacy assessment reports or updated equivalent report from a security/privacy management and reporting tool.

Primary Responsibility: Control Assessor.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

Supplemental Guidance: After the initial system or common control authorization, the organization assesses all security and privacy controls employed within and inherited by systems on an ongoing basis. The frequency of monitoring is based on the organizational monitoring strategy and supplemented by the system-level strategy as needed. The system-level monitoring strategy is approved by the authorizing official, senior agency information security officer, and senior agency official for privacy, and is consistent with the organizational monitoring strategy. For ongoing security and privacy control assessments, control assessors have the required degree of independence as determined by the authorizing official. Security and privacy control assessments in support of the initial and subsequent authorizations are conducted by independent assessors. Assessor independence during continuous monitoring, although not mandated, introduces efficiencies into the process and allows for reuse of assessment results in support of ongoing authorization and when reauthorization is required.

To satisfy the annual FISMA security assessment requirement, organizations can draw upon the assessment results from any of the following sources, including, for example, security control assessments conducted as part of authorization, ongoing authorization, or reauthorization; continuous monitoring; or testing and evaluation of systems as part of the system development life cycle or audit (provided that the assessment results are current, relevant to the determination of control effectiveness, and obtained by assessors with the required degree of independence). Existing security assessment results are reused to the extent that the results are still valid and are supplemented with additional assessments as needed. Reuse of security control assessment information is critical in achieving a cost-effective, fully integrated security program capable of producing the evidence necessary to determine the security status of systems and the organization. The use of automation to support security control assessments facilitates a greater frequency, volume, and coverage of assessments that is consistent with the monitoring strategy established by the organization.

References: NIST Special Publications 800-53A, 800-137, 800-160 (Verification, Validation, Operation, and Maintenance Processes).

ONGOING RISK RESPONSE

Task 3 Respond to risk based on the results of ongoing monitoring activities, assessments of risk, and outstanding items in plans of action and milestones.

Potential Inputs: Security and privacy assessment reports or reports from a security/privacy management and reporting tool; risk assessment results; system security and privacy plans; plans of action and milestones.

Potential Outputs: Updated security and privacy assessment reports or updated equivalent reports from a security/privacy management and reporting tool.

Primary Responsibility: System Owner; Common Control Provider.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

Supplemental Guidance: Assessment information produced by an assessor during continuous monitoring is provided to the system owner and the common control provider, respectively, in updated security and privacy assessment reports or via reports from automated security/privacy management and reporting tools. The system owner and common control provider determine and implement the appropriate risk response to the assessment findings. When the response to risk is acceptance, the findings remain documented in the security and privacy assessment reports and are monitored for changes to risk factors. When the response to risk is mitigation, the planned mitigation actions are included in and tracked using the plans of action and milestones. Control assessors may provide recommendations for remediation actions. Recommendations may also be provided by an automated security/privacy management and reporting tool. An organizational assessment of risk informs the decisions regarding ongoing risk response. Security and privacy controls that are modified, enhanced, or added during continuous monitoring are reassessed by assessors to ensure that the changes to the controls have been correctly implemented and the controls are operating effectively.

References: NIST Special Publications 800-30, 800-53, 800-53A, 800-160 (Risk Management Process); NIST Interagency Report 8062; Cybersecurity Framework (Core [Respond Functions]); CNSS Instruction 1253.

AUTHORIZATION UPDATES

Task 4 Update security and privacy plans, security and privacy assessment reports, and plans of action and milestones based on the results of the continuous monitoring process.

Potential Inputs: Security and privacy assessment reports or equivalent reports from a security/privacy management and reporting tool; risk assessment results; system security and privacy plans; plans of action and milestones.

Potential Outputs: Updated security and privacy assessment reports or updated equivalent reports from a security/privacy management and reporting tool; updated plans of action and milestones; updated risk assessment results; updated system security and privacy plans.

Primary Responsibility: System Owner; Common Control Provider.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

Supplemental Guidance: To achieve near real-time risk management, the organization updates security and privacy plans, security and privacy assessment reports, and plans of action and milestones on an ongoing basis. The security and privacy plan update reflects any modifications to security and privacy controls based on risk mitigation activities carried out by the system owner or common control provider. The security and privacy assessment report update reflects the additional assessment activities carried out to determine security and privacy control effectiveness based on modifications to the security and privacy plans and deployed controls. The plan of action and milestones update reports progress made on the current outstanding items listed in the plan; addresses vulnerabilities and privacy risks discovered during security and privacy impact analysis or control monitoring; and describes how the system owner or common control provider intends to address those vulnerabilities and privacy risks. The information provided by the updates helps to raise awareness of the current security and privacy state of the system and the common controls inherited by the system, thereby supporting the process of ongoing authorization and near real-time risk management.

The frequency of updates to risk management-related information is at the discretion of the system owner, common control provider, and authorizing officials in accordance with federal and organizational policies and consistent with the organizational continuous monitoring strategy. Updates to information regarding the security and privacy state of the system and the common controls inherited by the system are accurate and timely since the information provided influences ongoing security and privacy actions and decisions by authorizing officials and other senior leaders within the organization. With the use of automated support tools and organization-wide security and privacy program management practices, authorizing officials can readily access the current security and privacy state of the system including the ongoing effectiveness of security and privacy controls. This promotes the near real-time management of risk to organizational operations and assets, individuals, other organizations, and the Nation, and provides essential information for continuous monitoring and ongoing authorization.

Organizations ensure that information needed for oversight, management, and auditing purposes is not modified or destroyed when updating security and privacy plans, security and privacy assessment reports, and plans of action and milestones. Providing an effective method of tracking changes to information through strict configuration management and control procedures is necessary to achieve transparency and traceability in the security and privacy activities of the organization; to obtain individual accountability for security- and privacy-related actions; and to understand the emerging trends in the security and privacy programs of the organization.

References: NIST Special Publication 800-53A.

SECURITY AND PRIVACY STATUS REPORTING

Task 5 Report the security and privacy status of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational monitoring strategy.

Potential Inputs: Security and privacy assessment reports or equivalent reports from a security/privacy management and reporting tool; plans of action and milestones; risk assessment results; system security and privacy plans.

Potential Outputs: Authorizing officials and other organizational officials possess the information needed to make risk management decisions.

Primary Responsibility: System Owner; Common Control Provider; Senior Agency Information Security Officer.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

Supplemental Guidance: The results of monitoring activities are recorded and reported to the authorizing official and other officials on an ongoing basis in accordance with the organizational monitoring strategy. Security and privacy status reporting can be event-driven, time-driven, or event- and time-driven. Security and privacy status reports provide the authorizing official and other senior leaders and executives essential information regarding the security and privacy state of systems including the effectiveness of deployed security and privacy controls. Security and privacy status reports describe the ongoing monitoring activities employed by system owners or common control providers. Security and privacy status reports also address vulnerabilities and privacy risks in systems and environments of operation discovered during the security and privacy control assessments, security and privacy impact analysis, and security and privacy control monitoring and how system owners or common control providers intend to address those vulnerabilities and privacy risks.

Organizations have significant flexibility in the breadth, depth, and formality of security and privacy status reports. Security and privacy status reports can take whatever form the organization deems appropriate. The goal is cost-effective and efficient ongoing communication with senior leaders and executives conveying the current security and privacy state of systems and environments of operation regarding organizational missions and business functions. At a minimum, security and privacy status reports summarize key changes to security and privacy plans, security and privacy assessment reports, and plans of action and milestones. The use of automated security/privacy management and reporting tools by the organization facilitates the effectiveness and timeliness of security and privacy status reporting.

The frequency of security and privacy status reports is at the discretion of the organization and in compliance with federal and organizational policies. Status reports occur at appropriate intervals to transmit security- and privacy-related information about systems or common controls but not so frequently as to generate unnecessary work or expense. Authorizing officials use the security and privacy status reports and consult with the senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management/risk executive (function) to determine if a formal reauthorization action is necessary. Security and privacy status reports are appropriately marked, protected, and handled in accordance with federal and organizational policies. These status reports can be used to satisfy FISMA reporting requirements for documenting remedial actions for security- and privacy-related weaknesses or deficiencies. Such status reporting is intended to be ongoing and should not interpreted as requiring the time, expense, and formality associated with the information provided for the initial authorization. Rather, reporting is conducted in a cost-effective manner consistent with achieving the reporting objectives.

References: NIST Special Publications 800-53A, 800-137; Cybersecurity Framework (Core [Identify, Protect, Detect, Respond, Recover Functions]).

ONGOING AUTHORIZATION

Task 6 Review the security and privacy status of the system on an ongoing basis to determine whether the risk remains acceptable.

Potential Inputs: Security and privacy assessment reports or equivalent reports from a security/privacy management and reporting tool; plans of action and milestones; risk assessment results; system security and privacy plans.

Potential Outputs: A determination of risk; ongoing authorization to operate, ongoing authorization to use, ongoing common control authorization; denial of ongoing authorization to operate, denial of ongoing authorization to use, denial of ongoing common control authorization.

Primary Responsibility: Authorizing Official.

System Development Life Cycle Phase: New – Operations/Maintenance.
Existing – Operations/Maintenance.

Supplemental Guidance: The authorizing official or designated representative reviews the security and privacy status of the system (including the effectiveness of deployed security and privacy controls) on an ongoing basis, to determine the current risk to organizational operations and assets, individuals, other organizations, or the Nation. The authorizing official determines whether the current risk is acceptable and provides appropriate direction to the system owner or common control provider. The authorizing official may receive inputs from the senior accountable official for risk management/risk executive (function), senior agency information security officer, and senior agency official for privacy. The use of automated support tools to capture, organize, quantify, visually display, and maintain security and privacy status information promotes the concept of near real-time risk management regarding the risk posture of the organization.

The use of metrics and dashboards increases an organization's capability to make risk-based decisions by consolidating data from automated tools and providing the data to decision makers at different levels within the organization in an easy-to-understand format. The risks being incurred may change over time based on the information provided in the security and privacy status reports. Determining how changing conditions affect the mission or business risks is essential for maintaining adequate security. By carrying out ongoing risk determination and risk acceptance, authorizing officials can maintain the system and common control authorizations over time and transition to ongoing authorization. Formal reauthorization actions occur only in accordance with federal or organizational policies. The authorizing official conveys the updated risk determination and acceptance results to the senior accountable official for risk management/risk executive (function).

References: NIST Special Publications 800-30, 800-39 (Organization, Mission/Business Process, and System Levels), 800-160 (Risk Management Process); NIST Interagency Report 8062.

SYSTEM DISPOSAL

Task 7 Implement a system disposal strategy which executes required actions when a system is removed from service.

Potential Inputs: System security and privacy plans; risk assessment results; system component inventory.

Potential Outputs: Decommissioning strategy; updated system component inventory; updated system security and privacy plans.

Primary Responsibility: System Owner.

System Development Life Cycle Phase: New – Not Applicable.
Existing – Disposal.

Supplemental Guidance: When a system is removed from operation, several risk management-related actions are required. Organizations ensure that security and privacy controls addressing system removal and disposal are implemented. Examples include media sanitization; configuration management and control; and record retention. Organizational tracking and management systems (including inventory

systems) are updated to indicate the specific system components that are being removed from service. Security and privacy status reports reflect the status of the system. Users and application owners hosted on the decommissioned system are notified as appropriate, and any security and privacy control inheritance relationships are reviewed and assessed for impact. This task also applies to subsystems (including any associated system elements) that are removed from systems or decommissioned.

References: NIST Special Publications 800-30, 800-88; NIST Interagency Reports 8062.

APPENDIX A

ROLES AND RESPONSIBILITIES

KEY PARTICIPANTS IN THE RISK MANAGEMENT PROCESS

The following sections describe the roles and responsibilities of key participants involved in an organization's risk management process.[44] Recognizing that organizations have varying missions, business functions, and organizational structures, there may be differences in naming conventions for risk management roles and how risk management responsibilities are allocated among organizational personnel. This includes, for example, multiple individuals filling a single role or one individual filling multiple roles.[45] However, the basic functions remain the same. The application of the RMF described in this publication is flexible, allowing organizations to effectively accomplish the intent of the specific tasks within their respective organizational structures to best manage security risks. Many risk management roles defined in this publication have counterpart roles defined in the routine system development life cycle processes carried out by organizations. Whenever possible, organizations align the risk management roles with similar (or complementary) roles defined for the system development life cycle.[46]

AUTHORIZING OFFICIAL

The *authorizing official* is a senior official or executive with the authority to formally assume responsibility and accountability for operating a system; providing common controls inherited by organizational systems; or using a system, service, or application from an external provider—and accepting the security and privacy risk to organizational operations, organizational assets, and individuals.[47] Authorizing officials typically have budgetary oversight for the system or are responsible for the mission and/or business operations supported by the system. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such security and privacy risks. Authorizing officials approve security and privacy plans, memorandums of agreement or understanding, plans of action and milestones, and determine whether significant changes in the systems or environments of operation require reauthorization.

Authorizing officials coordinate their activities with common control providers, system owners, chief information officers, senior agency information security officers, senior agency official for privacy, system security and privacy officers, control assessors, senior accountable officials for risk management/risk executive (function), and other interested parties during the authorization process. With the increasing complexity of mission/business processes, partnership arrangements, and the use of shared services, it is possible that a system may involve multiple authorizing officials. If so, agreements are established among the authorizing officials and documented in the security plan. Authorizing officials are responsible for ensuring that activities and functions associated with authorization that are delegated to authorizing official designated representatives

[44] Organizations may define other roles to support the risk management process.

[45] Caution is exercised when one individual fills multiples roles in the risk management process to ensure that the individual retains an appropriate level of independence and remains free from conflicts of interest. Combining multiple roles for security and privacy requires care because in some circumstances the priorities may be competing.

[46] For example, the system development life cycle role of system developer or program manager can be aligned with system owner; and mission or business owner can be aligned with authorizing official.

[47] The responsibility and accountability of authorizing officials described in FIPS Publication 200 was extended in NIST Special Publication 800-53 to include risks to other organizations and the Nation.

are carried out. The role of authorizing official has inherent U.S. Government authority and is assigned to government personnel only.

AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE

The *authorizing official designated representative* is an organizational official that acts on behalf of an authorizing official to coordinate and conduct the required day-to-day activities associated with the authorization process. Authorizing official designated representatives can be empowered by authorizing officials to make certain decisions regarding the planning and resourcing of the authorization process; approval of the security and privacy plans; approval and monitoring the implementation of plans of action and milestones; and the assessment and determination of risk. The designated representative may be called upon to prepare the authorization package; obtain the authorizing official's signature on the authorization decision document; and transmit the authorization package to the appropriate organizational officials. The only activity that cannot be delegated to the authorizing official designated representative is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk).

CHIEF INFORMATION OFFICER

The *chief information officer*[48] is an organizational official responsible for designating a senior agency information security officer; developing and maintaining security policies, procedures, and control techniques to address applicable requirements; overseeing personnel with significant responsibilities for security and ensuring that the personnel are adequately trained; assisting senior organizational officials concerning their security responsibilities; and reporting to the head of the agency on the effectiveness of the organization's security program, including progress of remedial actions. The chief information officer, with the support of the risk executive (function) and the senior agency information security officer, works closely with authorizing officials and their designated representatives to help ensure that:

- An organization-wide security program is effectively implemented resulting in adequate security for all organizational systems and environments of operation;
- Security considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, and acquisition/system development life cycles;
- Organizational systems and common controls are covered by approved security plans and possess current authorizations;
- Security-related activities required across the organization are accomplished in an efficient, cost-effective, and timely manner; and
- There is centralized reporting of security-related activities.

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

[48] When an organization has not designated a formal chief information officer position, FISMA requires that the associated responsibilities be handled by a comparable organizational official. For organizations in which the senior agency official for privacy reports to the chief information officer, the chief information officer has equivalent responsibilities for privacy.

COMMON CONTROL PROVIDER

The *common control provider* is an individual, group, or organization that is responsible for the implementation, assessment, and monitoring of common controls (i.e., security and privacy controls inherited by organizational systems).[49] Common control providers are responsible for documenting the organization-defined common controls in security and privacy plans (or equivalent documents prescribed by the organization); ensuring that required assessments of the common controls are conducted by qualified assessors with an appropriate level of independence; documenting assessment findings in security and privacy assessment reports; and producing plans of action and milestones for controls having weaknesses or deficiencies. Security and privacy plans, security and privacy assessment reports, and plans of action and milestones for common controls (or a summary of such information) is made available to system owners inheriting those controls after the information is reviewed and approved by authorizing officials with oversight responsibility and accountability for those controls.

CONTRACTING OFFICER REPRESENTATIVE

The *contracting officer representative* (sometimes known as the contracting officer technical representative) is an individual tasked by the contracting officer to ensure that functional and security/privacy requirements are appropriately addressed in the contract and that the contractor meets the functional and security/privacy requirements as stated in the contract.

CONTROL ASSESSOR

The *control assessor* is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical controls and control enhancements employed within or inherited by a system to determine the effectiveness of the controls (i.e., the extent to which the security and privacy controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system).[50] Control assessors provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities. In addition to the above responsibilities, control assessors also prepare the final security and privacy assessment reports containing the results and findings from the assessment. Prior to initiating the control assessment, assessors review the security and privacy plans to ensure that the plans provide the security and privacy controls for the system that meet the stated security and privacy requirements.

The required level of assessor independence is determined by the conditions of the security and privacy control assessment. For example, when the assessment is conducted in support of an authorization decision or ongoing authorization, 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 preserving the impartial and unbiased nature of the assessment process; determining the credibility of the assessment results; and ensuring that the authorizing official receives objective information to make an informed, risk-based authorization decision. The system owner and common control provider rely on the security and/or privacy expertise and the technical judgment of the assessor

[49] Organizations can have multiple common control providers depending on how security and privacy responsibilities are allocated organization-wide. Common control providers may be *system owners* when the common controls are resident within an organizational system.

[50] Organizations can have multiple control assessors who may be differentiated by their expertise in security or privacy assessments.

to assess the security and privacy controls employed within and inherited by the system using the assessment procedures specified in the security and privacy assessment plans; and provide specific recommendations on how to correct weaknesses or deficiencies in the controls and address identified vulnerabilities.

ENTERPRISE ARCHITECT

The *enterprise architect* is an individual, group, or organization responsible for working with organizational stakeholders, both leadership and subject matter experts, to build a holistic view of the organization's strategy, processes, information, and information technology assets. The role of the enterprise architect is to take this knowledge and ensure that the business and information technology are in alignment. The enterprise architect links the organizational missions, business functions, strategy, and processes of an organization to its information technology strategy, and documents this using multiple architectural models or views that show how the current and future needs of an organization will be met in an efficient, sustainable, agile, and adaptable manner. Enterprise architects operate across organizational lines to drive common approaches and expose information assets and processes across the enterprise. The objective is to deliver an architecture that supports the most efficient, cost-effective, and secure information technology environment meeting the mission/business needs of the organization. Enterprise architects:

- Align the organization’s information technology strategy and planning with the mission and business goals and objectives of the organization;
- Optimize information management through an understanding of evolving business needs and technology capabilities;
- Promote shared infrastructure and applications to reduce costs and improve information flow;
- Ensure projects do not duplicate functionality or diverge from mission/business and information technology strategies; and
- Work with solutions architects to provide a consensus based enterprise solution that is scalable, adaptable, and in synchronization with ever-changing mission and business needs.

HEAD OF AGENCY

The *head of agency* (or chief executive officer) is the senior official or chief executive within an organization with the responsibility to provide security protections commensurate with the risk and magnitude of harm to organizational operations and assets, individuals, other organizations, and the Nation—that is, risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.[51] Agency heads or chief executives ensure that:

- Information security management processes are integrated with strategic and operational planning processes;
- Senior officials within the organization provide information security for the information and systems that support the operations and assets under their control; and

[51] Although the responsibilities of agency heads do not address privacy because they are derived from FISMA, OMB Circular A-130 does require agencies to manage privacy risk throughout the system development life cycle. Therefore, organizations can consider privacy to be a part of these enumerated responsibilities as well.

- The organization has adequately trained personnel to assist in complying with security requirements in legislation, Executive Orders, policies, directives, instructions, standards, and guidelines.

The head of agency or chief executive establishes the organizational commitment to security and the actions required to effectively manage security risk and protect the missions and business functions being carried out by the organization. The head of agency or chief executive establishes security accountability and provides active support and oversight of monitoring and improvement for the security program. Senior leadership commitment to security establishes a level of due diligence within the organization that promotes a climate for mission and business success.

INFORMATION OWNER OR STEWARD

The *information owner/steward* is an organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. In information-sharing environments, the information owner/steward is responsible for establishing the rules for appropriate use and protection of the information 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 a system may or may not be the same individual as the system owner. An individual system may contain information from multiple information owners/stewards. Information owners/stewards provide input to system owners regarding the security and privacy requirements and security and privacy controls for the systems where the information is processed, stored, or transmitted.

MISSION OR BUSINESS OWNER

The *mission or business owner* is the senior official or executive within an organization with specific mission or line of business responsibilities and that has a security and privacy interest in the organizational systems supporting those missions or lines of business. Mission or business owners are key stakeholders that have a significant role in defining organizational mission and business processes and the protection needs and security and privacy requirements that ensure the successful conduct of the organization's missions and business operations. Mission and business owners provide essential inputs to the organizational risk management strategy, play an active part in the system development life cycle, and may also serve in the role of authorizing official.

SECURITY OR PRIVACY ARCHITECT

The *security or privacy architect* is an individual, group, or organization responsible for ensuring that the stakeholder security and privacy requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the systems supporting those missions and business processes. The security or privacy architect serves as the primary liaison between the enterprise architect and the systems security or privacy engineer and coordinates with system owners, common control providers, and system security or privacy officers on the allocation of security or privacy controls. Security or privacy architects, in coordination with system security or privacy officers, advise authorizing officials, chief information officers, senior agency information security officers, senior agency officials for privacy, and senior accountable officials for risk management/risk executive (function), on a range of security- or privacy-related issues. Examples include establishing system boundaries; assessing the severity of weaknesses and deficiencies in the system; developing effective plans of action and milestones; creating risk

mitigation approaches; establishing security or privacy alerts; and potential adverse effects of identified vulnerabilities or privacy risks.

SENIOR ACCOUNTABLE OFFICIAL FOR RISK MANAGEMENT

The *senior accountable official for risk management*[52] is the individual that leads the risk executive (function) within an organization. The senior accountable official for risk management is the agency head or an individual designated by the agency head. The risk executive (function) helps to ensure that risk-related considerations for individual systems, to include authorization decisions, are viewed from an organization-wide perspective with regard to the strategic goals and objectives of the organization in carrying out its core missions and business functions; and managing security risk is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risk in order to ensure mission/business success. The risk executive (function) coordinates with the senior leadership of an organization to:

- Provide a comprehensive, organization-wide, holistic approach for addressing risk—an approach that provides a greater understanding of the integrated operations of the organization;
- Develop a risk management strategy for the organization providing a strategic view of security-related risks for the organization;[53]
- Facilitate the sharing of risk-related information among authorizing officials and other senior leaders within the organization;
- Provide oversight for all risk management-related activities across the organization to help ensure consistent and effective risk acceptance decisions;
- Ensure that authorization decisions consider all factors necessary for mission and business success;
- Provide an organization-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and the Nation;
- Promote cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility;
- Ensure that the shared responsibility for supporting organizational mission/business functions using external providers of systems, services, and applications receives the needed visibility and is elevated to the appropriate decision-making authorities; and
- Identify the organizational risk posture based on the aggregated risk from the operation and use of the systems for which the organization is responsible.

The senior accountable official for risk management determines the organizational structure and responsibilities of the risk executive (function). The head of the agency or chief executive, in coordination with the senior accountable official for risk management, may choose to retain the risk executive (function) or to delegate the function to another official or group. The senior

[52] OMB Memorandum M-17-25 requires the designation of a senior accountable official for risk management. Although M-17-25 enumerates responsibilities specific to information security, OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, requires agencies to consider privacy risk among other risks. Organizations have the discretion to add privacy to the responsibilities of the senior accountable official for risk management if it would support greater consideration of privacy risk in the enterprise risk management process.

[53] Authorizing officials may have narrow or localized perspectives in rendering authorization decisions without fully understanding or explicitly accepting the organization-wide risks being incurred from such decisions.

accountable official for risk management and the risk executive (function) have inherent U.S. Government authority and are assigned to government personnel only.

SENIOR AGENCY INFORMATION SECURITY OFFICER

The *senior agency information security officer* is an organizational official responsible for carrying out the chief information officer security responsibilities under FISMA, and serving as the primary liaison for the chief information officer to the organization's authorizing officials, system owners, common control providers, and system security officers. The senior agency information security officer is also responsible for coordinating with the senior agency official for privacy to ensure coordination between privacy and information security programs. The senior agency information security officer possesses the professional qualifications, including training and experience, required to administer security program functions; maintains security duties as a primary responsibility; and heads an office with the specific mission and resources to assist the organization in achieve trustworthy, secure information and systems in accordance with the requirements in FISMA. The senior agency information security officer may serve as authorizing official designated representative or as a security control assessor. The role of senior agency information security officer has inherent U.S. Government authority and is therefore assigned to government personnel only. Organizations may also refer to the senior agency information security officer as the senior information security officer or chief information security officer.

SENIOR AGENCY OFFICIAL FOR PRIVACY

The senior agency official for privacy is a senior official or executive with agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risk. The senior agency official for privacy is responsible for: coordinating with the senior information security officer to ensure coordination of privacy and information security activities; ensuring the privacy program plan addresses the privacy controls in place or planned for meeting applicable privacy requirements and managing privacy risk; reviewing and approving the categorization of systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information; designating which controls will be treated as program management, common, system-specific, and hybrid privacy controls; identifying assessment methods to determine if privacy controls are implemented correctly, operating as intended, and sufficient to ensure privacy requirements and privacy risks are addressed; reviewing and approving privacy plans for systems prior to authorization, reauthorization, or ongoing authorization; reviewing authorization information for systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information to ensure privacy requirements and privacy risks have been addressed; and developing and maintaining a privacy continuous monitoring program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure privacy requirements and privacy risks have been addressed.

SYSTEM ADMINISTRATOR

The *system administrator* is an individual, group, or organization responsible for setting up and maintaining a system or specific components of a system. System administrator responsibilities include, for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security and privacy controls; and adhering to organizational security and privacy policies and procedures.

SYSTEM OWNER

The *system owner* is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an organizational system.[54] The system owner is responsible for addressing the operational interests of the user community (i.e., users who require access to the system to satisfy mission, business, or operational requirements) and for ensuring compliance with security requirements. In coordination with the system security and privacy officers, the system owner is responsible for the development and maintenance of the security and privacy plans and ensures that the system is deployed and operated in accordance with the selected and implemented security and privacy controls. In coordination with the information owner/steward, the system owner is responsible for deciding who has access to the system (and with what types of privileges or access rights)[55] and ensures that system users and support personnel receive the requisite security and privacy training. Based on guidance from the authorizing official, the system owner informs organizational officials of the need to conduct the authorization, ensures that the necessary resources are available for the effort, and provides the required system access, information, and documentation to control assessors. The system owner receives the security and privacy assessment results from the control assessors. After taking appropriate steps to reduce or eliminate vulnerabilities or privacy risks, the system owner assembles the authorization package and submits the package to the authorizing official or the authorizing official designated representative for adjudication.[56]

SYSTEM SECURITY OR PRIVACY OFFICER

The *system security or privacy officer*[57] is an individual responsible for ensuring that the operational security and privacy posture is maintained for an organizational system and as such, works in close collaboration with the system owner. The system security or privacy officer also serves as a principal advisor on all matters, technical and otherwise, involving the security or privacy controls for the system. The system security or privacy officer has the knowledge and expertise to manage the security or privacy aspects of an organizational system and, in many organizations, is assigned responsibility for the day-to-day system security or privacy operations. This responsibility may also include, but is not limited to, physical and environmental protection; personnel security; incident handling; and security and privacy training and awareness. The system security or privacy officer may be called upon to assist in the development of the security or privacy policies and procedures and to ensure compliance with those policies and procedures. In close coordination with the system owner, the system security or privacy officer often plays an active role in the monitoring of a system and its environment of operation to include developing

[54] The *system owner* serves as the focal point for the organizational system. In that capacity, the system owner serves as the central point of contact between the authorization process and the owners of components of the system including, for example: applications, networking, servers, or workstations; owners/stewards of information processed, stored, or transmitted by the system; and owners of the missions and business functions supported by the system. Organizations may refer to system owners as program managers or business/asset owners.

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

[56] The authorizing official may choose to designate an individual other than the system owner to compile and assemble the information for the authorization package. In this situation, the designated individual coordinates the compilation and assembly activities with the system owner.

[57] Organizations may define a *system security manager* or *security manager* role with similar responsibilities as a system security officer or with oversight responsibilities for a security program. In these situations, system security officers may, at the discretion of the organization, report directly to system security managers or security managers. Organizations may assign equivalent responsibilities for privacy to separate individuals with appropriate subject matter expertise.

and updating security and privacy plans, managing and controlling changes to the system, and assessing the security or privacy impact of those changes.

SYSTEM USER

The *system user* is an individual or (system) process acting on behalf of an individual that is authorized to access organizational information and systems to perform assigned duties. System user responsibilities include, but are not limited to, adhering to organizational policies that govern acceptable use of organizational systems; using the organization-provided information technology resources for defined purposes only; and reporting anomalous or suspicious system behavior.

SYSTEMS SECURITY OR PRIVACY ENGINEER

The *systems security or privacy engineer* is an individual, group, or organization responsible for conducting systems security or privacy engineering activities as part of the system development life cycle. Systems security and privacy engineering is a process that captures and refines security or privacy requirements and ensures that the requirements are effectively integrated into the component products and systems through purposeful security or privacy architecting, design, development, and configuration. Systems security or privacy engineers are an integral part of the development team—designing and developing organizational systems or upgrading existing systems. Systems security or privacy engineers employ best practices when implementing security or privacy controls within a system including software engineering methodologies; system and security or privacy engineering principles; secure or privacy-enhancing design, secure or privacy-enhancing architecture, and secure or privacy-enhancing coding techniques. Systems security or privacy engineers coordinate security- and privacy-related activities with senior agency information security officers, senior agency officials for privacy, security and privacy architects, system owners, common control providers, and system security or privacy officers.

RISK EXECUTIVE (FUNCTION)

The *risk executive (function)* is an individual or group within an organization that provides a comprehensive, organization-wide approach to risk management. The risk executive (function) serves as the common risk management resource for senior leaders/executives, mission/business owners, chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, common control providers, enterprise architects, security architects, systems security or privacy engineers, system security or privacy managers/officers, and any other stakeholders having a vested interest in the mission/business success of organizations. The risk executive (function) coordinates with senior leaders and executives to:

- Establish risk management roles and responsibilities;
- Develop and implement an organization-wide *risk management strategy* that guides and informs organizational risk decisions (including how risk is framed, assessed, responded to, and monitored over time);
- Manage threat, vulnerability, and security/privacy risk information for organizational systems and the environments in which the systems operate;
- Establish organization-wide forums to consider all types and sources of risk (including aggregated risk);
- Determine organizational risk based on the aggregated risk from the operation and use of systems and the respective environments of operation;

- Provide oversight for the risk management activities carried out by organizations to ensure consistent and effective risk-based decisions;
- Develop a broad-based understanding of risk regarding the strategic view of organizations and their integrated operations;
- Establish effective vehicles and serve as a focal point for communicating and sharing risk-related information among key stakeholders internally and externally to organizations;
- Specify the degree of autonomy for subordinate organizations permitted by parent organizations regarding framing, assessing, responding to, and monitoring risk;
- Promote cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility (e.g., joint/leveraged authorizations);
- Ensure that authorization decisions consider all factors necessary for mission and business success; and
- Ensure shared responsibility for supporting organizational missions and business functions using external providers receives the needed visibility and is elevated to appropriate decision-making authorities.

The risk executive (function) presumes neither a specific organizational structure nor formal responsibility assigned to any one individual or group within the organization. Heads of agencies or organizations may choose to retain the risk executive (function) or to delegate the function. The risk executive (function) requires a mix of skills, expertise, and perspectives to understand the strategic goals and objectives of organizations, organizational missions/business functions, technical possibilities and constraints, and key mandates and guidance that shape organizational operations. To provide this needed mixture, the risk executive (function) can be filled by a single individual or office (supported by an expert staff) or by a designated group (e.g., a risk board, executive steering committee, executive leadership council). The risk executive (function) fits into the organizational governance structure in such a way as to facilitate efficiency and effectiveness.

APPENDIX B

SUMMARY OF RMF TASKS

RMF TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

TABLE B-1: PREPARATION TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **Risk Management Roles** Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework.	• Head of Agency or Chief Executive Officer	• Senior Accountable Official for Risk Management • Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 2 **Risk Management Strategy** Establish a risk management strategy for the organization that includes a determination of risk tolerance.	• Head of Agency or Chief Executive Officer	• Mission/Business Owner • Senior Accountable Official for Risk Management • Risk Executive (Function) • Authorizing Official or Designated Representative • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 3 **Missions, Business Functions, and Mission/Business Processes** Identify the missions, business functions, and mission/business processes that the system is intended to support.	• Head of Agency or Chief Executive Officer • Mission/Business Owner	• Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 4 **Organizational Stakeholders** Identify stakeholders who have a security and privacy interest in the development, implementation, operation, or sustainment of the system.	• Head of Agency or Chief Executive Officer • Mission/Business Owner	• Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 5 **Stakeholder Assets** Identify stakeholder assets that require protection.	• Head of Agency or Chief Executive Officer • Mission/Business Owner	• Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 6 **Information Life Cycle** For systems that process personally identifiable information, identify the information life cycle.	• Chief Information Officer • Senior Agency Official for Privacy	• Mission/Business Owner • Senior Agency Information Security Officer • System Owner • Enterprise Architect • Security or Privacy Architect • Systems Security or Privacy Engineer
TASK 7 **Risk Assessment** Conduct an initial risk assessment of stakeholder assets and update the risk assessment on an ongoing basis.	• Senior Accountable Official for Risk Management • Risk Executive (Function)	• Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 8 **Stakeholder Protection Needs—Security and Privacy Requirements** Define the stakeholder protection needs and stakeholder security and privacy requirements.	• Head of Agency (Chief Executive Officer) • Mission/Business Owner • Information Owner/Steward	• Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 9 **Enterprise Architecture** Determine the placement of the system within the enterprise architecture.	• Enterprise Architect • Security or Privacy Architect	• System Owner • Systems Security or Privacy Engineer • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 10 **Organization-Wide Tailored Control Baselines and Profiles (Optional)** Establish and publish organization-wide tailored control baselines and profiles.	• Mission/Business Owner • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy	• Senior Accountable Official for Risk Management • Risk Executive (Function)
TASK 11 **Common Control Identification** Identify organization-wide common controls that are available for inheritance by organizational systems.	• Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Senior Accountable Official for Risk Management • Risk Executive (Function)	• Authorizing Official or Designated Representative • Common Control Provider • System Owner • Security or Privacy Architect • Systems Security or Privacy Engineer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 12 **Impact-Level Prioritization (Optional)** Prioritize organizational systems with the same impact level.	• Mission/Business Owner • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Senior Accountable Official for Risk Management • Risk Executive (Function)	• Authorizing Official or Designated Representative • Common Control Provider • System Owner • Security or Privacy Architect • Systems Security or Privacy Engineer
TASK 13 **Organizational Monitoring Strategy** Develop and implement an organization-wide strategy for monitoring security and privacy control effectiveness.	• Senior Agency Information Security Officer • Senior Agency Officer for Privacy • Senior Accountable Official for Risk Management • Risk Executive (Function) • Chief Information Officer	• Mission/Business Owner • Authorizing Official or Designated Representative • Common Control Provider • System Owner • Security or Privacy Architect • Systems Security or Privacy Engineer

TABLE B-2: CATEGORIZATION TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **System Boundary** Determine the boundary of the system.	• System Owner • Authorizing Official or Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy	• Senior Accountable Official for Risk Management • Risk Executive (Function) • Chief Information Officer • Information Owner/Steward • System Security or Privacy Officer
TASK 2 **Security and Privacy Requirements Allocation** Identify the security and privacy requirements allocated to the system and to the organization.	• Security or Privacy Architect • Senior Agency Information Security Officer • Senior Agency Official for Privacy	• Enterprise Architect • Chief Information Officer • Systems Security or Privacy Engineer
TASK 3 **Information Types** Identify the types of information to be processed, stored, or transmitted by the system.	• System Owner • Information Owner/Steward	• Authorizing Official or Designated Representative • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Security or Privacy Officer
TASK 4 **Security Categorization** Categorize the system and document the security categorization results as part of system requirements.	• System Owner • Information Owner/Steward	• Senior Accountable Official for Risk Management • Risk Executive (Function) • Authorizing Official or Designated Representative • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Security or Privacy Officer
TASK 5 **System Description** Describe the characteristics of the system.	• System Owner	• Authorizing Official or Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Information Owner/Steward • System Security or Privacy Officer
TASK 6 **System Registration** Register the system with appropriate organizational program/management offices.	• System Owner	• System Security or Privacy Officer

TABLE B-3: SELECTION TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **Security and Privacy Control Selection** Select the security and privacy controls for the system and document the functional description of the planned control implementations in the security and privacy plans.	• System Owner • Common Control Provider	• Authorizing Official or Designated Representative • Information Owner/Steward • Security or Privacy Architect • Systems Security or Privacy Engineer • System Security or Privacy Officer • Contracting Officer Representative
TASK 2 **System-Level Monitoring Strategy** Supplement the organizational continuous monitoring strategy at the system level, as needed.	• System Owner • Common Control Provider	• Senior Accountable Official for Risk Management • Risk Executive (Function) • Authorizing Official or Designated Representative • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Information Owner/Steward • System Security or Privacy Officer
TASK 3 **Security and Privacy Plan Approval** Review and approve the security and privacy plans.	• Authorizing Official or Designated Representative	• Senior Accountable Official for Risk Management • Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy

TABLE B-4: IMPLEMENTATION TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **Security and Privacy Control Implementation** Implement the security and privacy controls specified in the security and privacy plans or other system documentation.	• System Owner • Common Control Provider	• Information Owner/Steward • System Security or Privacy Officer • Systems Security or Privacy Engineer • System Administrator
TASK 2 **Baseline Configuration** Document changes to planned security and privacy control implementation and establish the configuration baseline for the system.	• System Owner • Common Control Provider	• Information Owner/Steward • System Security or Privacy Officer • Systems Security or Privacy Engineer • System Administrator

TABLE B-5: ASSESSMENT TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **Assessment Preparation** Develop, review, and approve a plan to assess the security and privacy controls in the system and the organization.	• Control Assessor	• Authorizing Official or Designated Representative • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner or Common Control Provider • Information Owner/Steward • System Security or Privacy Officer
TASK 2 **Security and Privacy Control Assessments** Assess the security and privacy controls in accordance with the assessment procedures defined in the security and privacy assessment plans.	• Control Assessor	• System Owner • Common Control Provider • Information Owner/Steward • System Security or Privacy Officer • System Administrator • Contracting Officer Representative • System User
TASK 3 **Security and Privacy Assessment Reports** Prepare the security and privacy assessment reports documenting the issues, findings, and recommendations from the security and privacy control assessments.	• Control Assessor	• System Owner • Common Control Provider • System Security or Privacy Officer
TASK 4 **Remediation Actions** Conduct initial remediation actions on security and privacy controls based on the findings and recommendations of the security and privacy assessment reports; reassess remediated controls.	• System Owner • Common Control Provider • Control Assessor	• Authorizing Official or Designated Representative • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Information Owner/Steward • System Security or Privacy Officer • Systems Security or Privacy Engineer • Control Assessor • System Administrator

TABLE B-6: AUTHORIZATION TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **Plan of Action and Milestones** Prepare the plan of action and milestones based on the findings and recommendations of the security and privacy assessment reports excluding any remediation actions taken.	• System Owner • Common Control Provider	• Information Owner/Steward • System Security or Privacy Officer
TASK 2 **Authorization Package** Assemble the authorization package and submit the package to the authorizing official for adjudication.	• System Owner • Common Control Provider	• System Security or Privacy Officer
TASK 3 **Risk Determination** Determine the risk from the operation or use of the system or the provision of common controls.	• Authorizing Official or Designated Representative	• Senior Accountable Official for Risk Management • Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 4 **Risk Response** Identify and implement a preferred course of action in response to the risk determined.	• Authorizing Official or Designated Representative	• Senior Accountable Official for Risk Management • Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner • Common Control Provider • System Security or Privacy Officer • Systems Security or Privacy Engineer
TASK 5 **Authorization Decision** Determine if the risk from the operation or use of the system or the provision or use of common controls is acceptable.	• Authorizing Official	• Senior Accountable Official for Risk Management • Risk Executive (Function) • Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 6 **Authorization Reporting** Report the authorization decision and significant vulnerabilities to designated organizational officials.	• Authorizing Official or Designated Representative	• Senior Accountable Official for Risk Management • Risk Executive (Function) • Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy

TABLE B-7: MONITORING TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **System and Environment Changes** Monitor changes to the system and its environment of operation.	• System Owner • Common Control Provider	• Authorizing Official or Designated Representative • Information Owner/Steward • System Security or Privacy Officer
TASK 2 **Ongoing Assessments** Assess the security and privacy controls employed within and inherited by the system in accordance with the organization-defined monitoring strategy.	• Control Assessor	• Authorizing Official or Designated Representative • System Owner • Common Control Provider • Information Owner/Steward • System Security or Privacy Officer
TASK 3 **Ongoing Risk Response** Respond to risk based on the results of ongoing monitoring activities, assessments of risk, and outstanding items in plans of action and milestones.	• System Owner • Common Control Provider	• Authorizing Official or Designated Representative • Information Owner/Steward • System Security or Privacy Officer • Systems Security or Privacy Engineer • Control Assessor
TASK 4 **Authorization Updates** Update the security and privacy plans, security and privacy assessment reports, and plans of action and milestones based on the results of the continuous monitoring process.	• System Owner • Common Control Provider	• Information Owner/Steward • System Security or Privacy Officer
TASK 5 **Security and Privacy Status Reporting** Report the security and privacy status of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational monitoring strategy.	• System Owner • Common Control Provider	• System Security or Privacy Officer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 6 **Ongoing Authorization** Review the security and privacy status of the system on an ongoing basis to determine whether the risk remains acceptable.	• Authorizing Official	• Senior Accountable Official for Risk Management • Risk Executive (Function) • Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 7 **System Disposal** Implement a system disposal strategy which executes required actions when a system is removed from service.	• System Owner	• Senior Accountable Official for Risk Management • Risk Executive (Function) • Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Information Owner/Steward • System Security or Privacy Officer

APPENDIX C

SYSTEM AND CONTROL AUTHORIZATIONS

AUTHORIZATION DECISIONS AND SUPPORTING EVIDENCE

This appendix provides information on the system and common control authorization processes to include: types of authorizations; content of authorization packages; authorization decisions; authorization decision documents; ongoing authorization; reauthorization; event-driven triggers and significant changes; type and facility authorizations; and authorization approaches.

TYPES OF AUTHORIZATIONS

Authorization is the process by which a senior management official, the authorizing official, reviews security- and privacy-related information describing the current security and privacy state of a system or common controls that are inherited by systems. The authorizing official uses this information to determine if the mission/business risk of operating a system or providing common controls is acceptable—and if it is, explicitly accepts the risk. Security- and privacy-related information is presented to the authorizing official either in an authorization package or by retrieving a report from an automated security/privacy management and reporting tool.[58] System and common control authorization occurs as part of the RMF Authorization step. A system authorization or common control authorization can be the initial authorization, ongoing authorization, or a reauthorization as defined below:

- *Initial authorization* is defined as the initial (start-up) risk determination and risk acceptance decision based on a zero-base review of the system or the common controls inherited by the system. The zero-base review includes an assessment of *all* security and privacy controls contained in the security and privacy plans and implemented within the system or the environment in which the system operates. The initial authorization for the system and the common controls inherited by the system may have different authorizing officials.
- *Ongoing authorization* is defined as the subsequent (i.e., follow-on) risk determinations and risk acceptance decisions taken at agreed-upon and documented frequencies in accordance with the organization's mission/business requirements and organizational risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process whereby the authorizing official is provided with the necessary and sufficient information regarding the near real-time security state of the system (including the effectiveness of the security and privacy controls employed within and inherited by the system) to determine whether the mission/business risk of continued system operation or the provision of common controls is acceptable. Ongoing authorization is fundamentally related to the ongoing understanding and ongoing acceptance of security and privacy risk. It is also closely related to the dynamic, organization-wide risk management process that provides a refined and articulated situational awareness of the security, privacy, and risk posture of the organization based on the ongoing assessment, response to, and monitoring of security and privacy risk and thus is dependent on a robust continuous monitoring program.
- *Reauthorization* is defined as the static, single point-in-time risk determination and risk acceptance decision that occurs after initial authorization. In general, reauthorization actions

[58] NIST Special Publication 800-137 provides information on automated security management and reporting tools. Future updates to this publication will also address privacy management and reporting tools.

may be time-driven or event-driven. However, under ongoing authorization, reauthorization is typically an event-driven action initiated by the authorizing official or directed by the Senior Accountable Official for Risk Management/Risk Executive (function) in response to an event that results in security and privacy risk above the previously agreed-upon risk tolerance. Reauthorization consists of a review of the system and/or common controls like the review carried out during the initial authorization. The reauthorization process differs from the initial authorization because the authorizing official can initiate a complete zero-base review of the system or common controls or a targeted review based on the type of event that triggered the reauthorization; the assessment of risk related to the event; the risk response of the organization; and the organizational risk tolerance. Reauthorization is a separate activity from the ongoing authorization process. However, security- and privacy-related information generated from the organization's continuous monitoring program may still be leveraged to support reauthorization. Reauthorization actions may necessitate a review of and changes to the continuous monitoring strategy which may in turn, affect ongoing authorization.

AUTHORIZATION PACKAGE

The *authorization package* documents the results of the security and privacy control assessments and provides the authorizing official with the information needed to make a risk-based decision on whether to authorize the operation of a system or a set of common controls. The system owner or common control provider is responsible for the assembly, compilation, and submission of the authorization package or for ensuring that the information is available from reports generated by an automated security/privacy management and reporting tool. The system owner or common control provider receives inputs from many sources during the preparation of the authorization package including, for example: control assessors; senior agency information security officer; senior agency official for privacy, senior accountable official for risk management/risk executive (function); system security or privacy officer; and the continuous monitoring program. The authorization package[59] contains the following documents.

- Executive summary;
- Security and privacy plans;[60]
- Security and privacy assessment reports; [61] and
- Plans of action and milestones.

The executive summary provides a consolidated view of the detailed security- and privacy-related information in the authorization package. The executive summary helps to identify and highlight important risk management issues associated with protecting organizational systems and the environments in which the systems operate. It also provides the necessary and sufficient information needed by the authorization official to understand the security and privacy risks to the organization's operations and assets, individuals, other organizations, and the Nation—and to use that information to make informed, risk-based decisions regarding the operation and use of the system or the provision of common controls that can be inherited by organizational systems.

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

[60] NIST Special Publication 800-18 provides guidance on security plans. Guidance on privacy plans will be addressed in future updates to this publication.

[61] NIST Special Publication 800-53A provides guidance on security assessment reports. Guidance on privacy assessment reports will be addressed in future updates to this publication.

The security and privacy plans, prepared by the system owner or the common control provider, provides an overview of the security and privacy requirements and describes the security and privacy controls in place or planned for meeting those requirements. The plan provides sufficient information to understand the intended or actual implementation of the security and privacy controls employed within or inherited by the system. The security and privacy plans may also include as supporting appendices or as references, additional security- and privacy-related documents such as the privacy impact assessment, interconnection security agreements, security and privacy configurations, contingency plan, configuration management plan, incident response plan, and system-level monitoring strategy. The security and privacy plans are updated whenever events dictate changes to the security and privacy controls employed within or inherited by the system.

The security and privacy assessment reports, prepared by the control assessor or generated by an automated security/privacy management and reporting tool, provides the findings and results of assessing the implementation of the security and privacy controls identified in the security and privacy plans 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 and privacy requirements. The security and privacy assessment reports may contain recommended corrective actions for weaknesses or deficiencies identified in the security and privacy controls.[62] Supporting the near real-time risk management objectives of the authorization process, the security and privacy assessment reports are updated on an ongoing basis whenever changes are made to the security and privacy controls employed within or inherited by the system.[63] Updates to the security and privacy assessment reports help to ensure that the system owner, common control provider, and authorizing officials maintain an awareness regarding security and privacy control effectiveness. The effectiveness of the security and privacy controls directly affects the security and privacy state of the system and decisions regarding explicit acceptance of risk.

The plan of action and milestones, prepared by the system owner or common control provider, describes the specific measures planned to correct weaknesses or deficiencies identified in the security and privacy controls during the assessment; and to address known vulnerabilities or privacy risks in the system.[64] The content and structure of plans of action and milestones are informed by the organizational risk management strategy developed as part of the risk executive (function) and are consistent with the plans of action and milestones process established by the organization which include any specific requirements defined in federal laws, Executive Orders, policies, directives, or standards. If systems and the environments in which those systems operate have more vulnerabilities than available resources can realistically address, organizations develop and implement plans of action and milestones that facilitate a prioritized approach to risk mitigation and that is consistent across the organization. This ensures that plans of action and milestones are based on:

- The security categorization of the system and privacy risk assessment;
- The specific weaknesses or deficiencies in the security and privacy controls;

[62] An executive summary provides an authorizing official with an abbreviated version of the security and privacy assessment reports focusing on the highlights of the assessment, synopsis of findings, and recommendations for addressing weaknesses and deficiencies in the security and privacy controls.

[63] Because the desired outcome of ongoing tracking and response to assessment findings to facilitate risk management decisions is the focus (rather than the specific process used), organizations have the flexibility to manage and update security assessment report information using any format or method consistent with internal organizational processes.

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

- The criticality of the security and privacy control weaknesses or deficiencies (i.e., the direct or indirect effect the weaknesses or deficiencies may have on the overall security and privacy state of the system and hence on the risk exposure[65] of the organization);
- The risk mitigation approach of the organization to address the identified weaknesses or deficiencies in the security and privacy controls; and
- The rationale for accepting certain weaknesses or deficiencies in the security and privacy controls.

Organizational strategies for plans of action and milestones are guided by the security categories of the respective systems affected by the risk mitigation activities. Organizations may decide, for example, to allocate their risk mitigation resources initially to the *highest-impact* systems or other high-value assets because a failure to correct the weaknesses or deficiencies in those systems or system components could potentially have the most significant adverse effects on their missions or business functions. Organizations also prioritize weaknesses or deficiencies using information from organizational assessments of risk and the risk management strategy developed as part of the risk executive (function). Therefore, 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 always addresses the highest-priority weaknesses or deficiencies within those prioritized systems.

AUTHORIZATION DECISIONS

Authorization decisions are based on the content of the authorization package. There are three types of authorization decisions that can be rendered by authorizing officials:

- Authorization to Operate;
- Common Control Authorization; and
- Authorization to Use.

Authorization to Operate

If the authorizing official, after reviewing the authorization package, determines that the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation is acceptable, an *authorization to operate* is issued for the system. The system is authorized to operate for a specified period in accordance with the terms and conditions established by the authorizing official. An *authorization termination date* is established by the authorizing official as a condition of the authorization. The authorization termination date can be adjusted by the authorizing official to reflect an increased level of concern regarding the security and privacy state of the system including the security and privacy controls employed within or inherited by the system. If the system is under ongoing authorization, a time-driven authorization frequency is specified. Additionally, within any authorization type, an adverse event could occur that triggers the need to review the authorization to operate.[66]

Common Control Authorization

A *common control authorization* is similar to an authorization to operate for systems. It is the responsibility of the common control provider to indicate that the common controls selected by

[65] 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.

[66] Additional information on event-driven triggers is provided below.

the organization have been implemented and assessed and are available for inheritance by organizational systems. Common control providers are also responsible for ensuring that the system owners inheriting the controls have access to appropriate documentation and tools. If the authorizing official, after reviewing the authorization package submitted by the common control provider, determines that the security and privacy risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable, a common control authorization is issued. Common controls are authorized for a specific time period in accordance with the terms and conditions established by the authorizing official. An *authorization termination date* is established by the authorizing official as a condition of the initial common control authorization. The termination date can be adjusted to reflect the level of concern by the authorizing official regarding the security and privacy state of the common controls available for inheritance. If the controls are under ongoing authorization, a time-driven authorization frequency is specified. Additionally, within any authorization type, an adverse event could occur that triggers the need to review the common control authorization. Common controls that are implemented within a system receive an authorization to operate which also serves as a common control authorization.[67]

Authorization to Use

An *authorization to use* is employed when an organization (hereafter referred to as the customer organization) chooses to accept the information in an existing authorization package generated by another organization (hereafter referred to as the provider organization).[68] This acceptance is based on a need to use the same information resources, for example, a system, an application, or a service provided by a system. A customer organization can issue an authorization to use only after a valid authorization to operate has been issued by the provider organization.[69] The provider authorization (to operate) is a statement of the provider's acceptance of risk for the system, service, or application being provided. The customer authorization (to use) is a statement of the customer's acceptance of risk for the system, service, or application being used with respect to the customer's information.[70] An authorization to use provides opportunities for significant cost savings and avoids a potentially costly and time-consuming authorization process by the customer organization.

An authorization to use requires the customer organization to review the authorization package from the provider as the basis for determining risk to its organization.[71] When reviewing the authorization package, the customer organization considers risk factors such as the time elapsed since the authorization results were produced; the environment of operation (if different from the environment reflected in the authorization package); the criticality/impact of the information to be

[67] In certain situations, system owners may inherit security or privacy controls from other organizational systems that may not be designated officially as common controls. System owners inheriting controls from other than approved common control providers ensure that the system providing such controls has a valid authorization to operate. The authorizing official of the system inheriting the security or privacy controls is also made aware of the inheritance.

[68] The term *service providing* organization refers to the federal agency or subordinate organization that provides the system and/or service and/or owns and maintains the authorization package (i.e., has granted an Authorization to Operate for the shared system/service). The system/service itself may not be owned by the organization that owns the authorization package, for example, in situations where the system/service is provided by an external provider.

[69] A provisional authorization (to operate) issued by the General Services Administration (GSA) as part of the Federal Risk and Authorization Management Program (FedRAMP) is considered a valid authorization to operate for customer organizations desiring to issue an authorization to use for cloud-based systems, services, or applications.

[70] An *authorization to use* is issued by an organizational official with the same level of risk management responsibility and authority as an organizational official issuing an authorization to operate or a common control authorization.

[71] The sharing of the authorization package (including security and privacy plans, security and privacy assessment reports, plans of action and milestones, and the authorization decision document) is accomplished under terms and conditions agreed-upon by all parties (i.e., the customer organization and the service provider organization).

processed, stored, or transmitted; and the overall risk tolerance of the customer organization. If the customer organization plans to integrate the shared system, application, or service with one or more of its systems, the customer organization considers the additional risk in doing so.

If the customer organization determines that there is insufficient information in the authorization package or inadequate security and privacy controls in place for establishing an acceptable level of risk, the customer organization may negotiate with the provider organization to provide additional security and privacy controls or security- and privacy-related information. Security and privacy controls may also include supplementing security and privacy controls with additional controls relevant to risk reduction; implementing compensating controls; conducting additional or more rigorous assessments; or establishing constraints on the use of the system, application, or service provided. Security- and privacy-related information may include, for example, other information that the provider organization may have produced or discovered in the use or assessment of the system that is not reflected in the authorization package. When the provider organization is unable to provide the requested security and privacy controls, the customer organization may choose to implement additional controls to reduce risk to an acceptable level.

Once the customer organization is satisfied with the security and privacy posture of the provider organization (as reflected in the current authorization package), the customer organization issues an authorization to use in which the customer organization explicitly understands and accepts the security and privacy risk incurred by using the shared system, service, or application.[72] The customer organization is responsible and accountable for the security and privacy risks that may impact the customer organization's operations and assets, individuals, other organizations, or the Nation. The authorization to use is issued by a designated authorizing official from the customer organization in lieu of an authorization to operate.

The authorization to use remains in effect while the customer organization continues to accept the security and privacy risk of using the system, application, or service; and the authorization to operate issued by the provider organization meets the requirements established by federal and organizational policies. This requires ongoing information sharing from the monitoring activities conducted by the provider organization and notification when there are significant changes to the system, application, or service that may affect the risk posture of the provider. The provider organization notifies the customer organization if there is a significant event that compromises the customer organization's information.

Denial of Authorization

If the authorizing official, after reviewing the authorization package and any inputs provided by the senior accountable official for risk management/risk executive (function), determines 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, the authorization is not granted. A *denial of authorization* means that the system is not authorized to operate and is not placed into operation, or if the system is currently in operation, activity is halted. A denial of authorization for common controls means that the controls are not authorized to be provided to system owners for purposes of inheritance. If the common controls are active, all activity is halted including for the systems inheriting those controls. A denial of authorization

[72] In accordance with FISMA, the head of each agency is responsible for providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency. OMB Circular A-130 describes organizational responsibilities for accepting security and privacy risk.

to use means that the use of the system, service, or application by the customer organization is not approved or is halted.

Failure to receive an authorization indicates that there are significant weaknesses or deficiencies in the security and privacy controls. The authorizing official or designated representative works with the system owner or common control provider to revise the plan of action and milestones to ensure that appropriate measures are taken to correct the weaknesses or deficiencies. A special case of a denial of authorization is an *authorization rescission*. Authorizing officials can rescind a previous authorization decision at any time in situations where there is a violation of federal or organizational policies, directives, regulations, standards, or guidance; or a violation of the terms and conditions of the authorization. For example, failure to maintain an effective continuous monitoring program may be grounds for rescinding an authorization decision. Figure C-1 illustrates the types of authorization decisions that can be applied to organizational systems and common controls and the associated risk management roles in the authorization process.

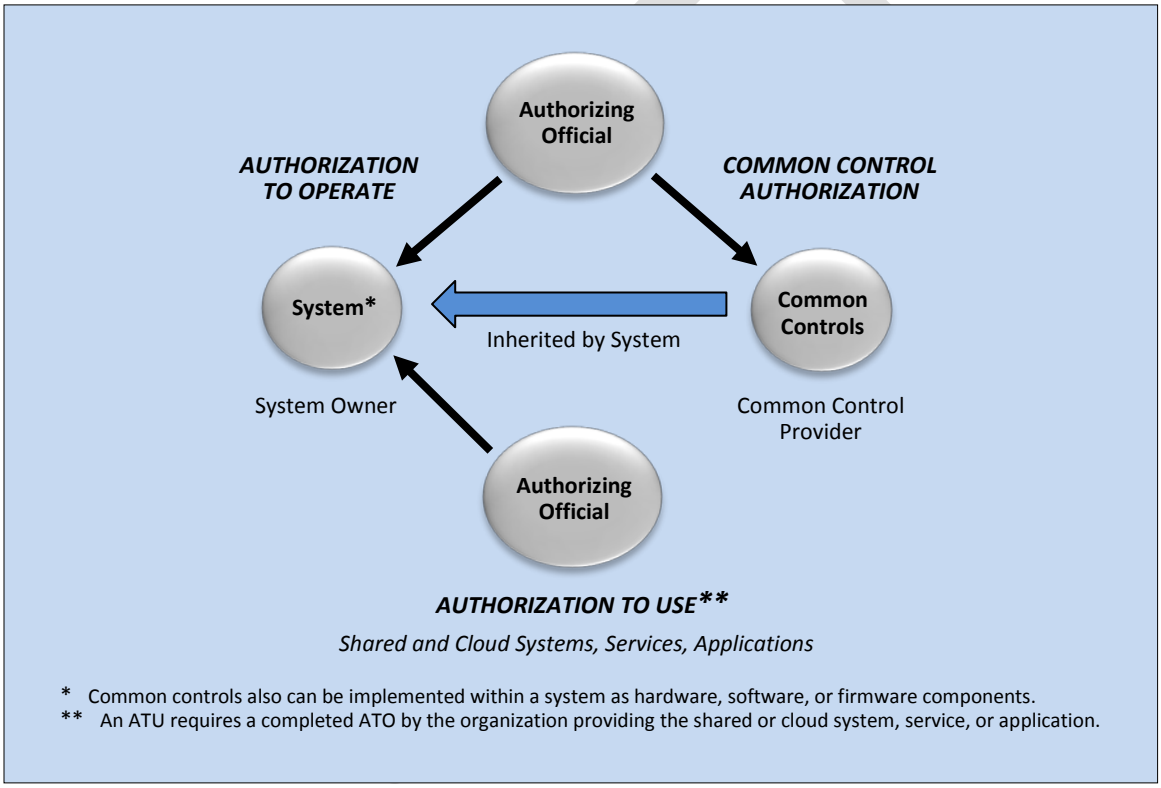

FIGURE C-1: TYPES OF AUTHORIZATION DECISIONS

AUTHORIZATION DECISION DOCUMENTS

The authorization decision document transmits the authorization decision from the authorizing official to system owners, common control providers, and other key organizational officials, as appropriate. The authorization decision document contains the following information:

- Authorization decision;
- Terms and conditions for the authorization;
- Time-driven authorization frequency or authorization termination date;

- Adverse events that may trigger a review of the authorization decision (if any);
- Input from senior accountable official for risk management/risk executive (function), if provided; and
- For common controls, the FIPS Publication 199 impact level supported by those controls.

The authorization decision document indicates if the system is authorized to operate or common controls are authorized to be inherited by other organizational systems. The terms and conditions for the authorization provide any limitations or restrictions placed on the operation of the system that must be followed by the system owner or alternatively, limitations or restrictions placed on the implementation of common controls that must be followed by the common control provider. If the system or common controls are not under ongoing authorization, the termination date for the authorization established by the authorizing official indicates when the authorization expires and reauthorization is required. The authorization decision document is attached to the original authorization package and transmitted to the system owner or common control provider.[73]

Upon receipt of the authorization decision document and authorization package, the system owner and common control provider acknowledge, implement, and comply with the terms and conditions of the authorization and notify the authorizing official. The system owner and common control provider retain the original authorization decision document and authorization package.[74] The organization ensures that authorization documents are available to appropriate organizational officials. The contents of the authorization packages, including sensitive information regarding system vulnerabilities, privacy risks, and security and privacy control weaknesses or deficiencies, are marked and protected in accordance with federal and organizational policy. Such information is retained in accordance with the organization's record retention policy. The authorizing official verifies on an ongoing basis, that the terms and conditions established as part of the authorization are being followed by the system owner and common control provider.

Authorization to Use Decision Document

The authorization to use decision document is a brief statement signed by a senior management official of a customer organization indicating the explicit acceptance of the security and privacy risk incurred from the use of a shared system, service, or application with respect to the customer organization information processed, stored, or transmitted by or through the shared system, service, or application. The authorization to use decision document may include time- or even-driven triggers for review of the security and privacy posture of the provider organization system, service, or application being used by the customer organization.

ONGOING AUTHORIZATION

Information security and information privacy continuous monitoring strategies[75] that are part of the system development life cycle process, promote effective risk management on an ongoing basis. Risk management can become *near real-time* by using automation and state-of-the-practice tools, techniques, and procedures for the ongoing monitoring of security and privacy controls and changes to systems and the environments in which those systems operate. Continuous monitoring based on the needs of the authorizing official, produces the necessary information to determine

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

[74] Organizations may choose to employ automated tools to support the development, distribution, and archiving of risk management information to include artifacts associated with the authorization process.

[75] NIST Special Publication 800-137 provides additional guidance on information security continuous monitoring. Guidance on privacy continuous monitoring will be provided in future updates to this publication.

the current security and privacy state of the system (including the effectiveness of security and privacy controls employed within and inherited by the system). It also highlights the risks to organizational operations and assets, individuals, other organizations, and the Nation. Ultimately, continuous monitoring helps to guide and inform the authorizing official's decision whether to authorize the continued operation of the system or the continued use of common controls inherited by organizational systems.

Continuous monitoring helps to achieve a state of *ongoing authorization* where the authorizing official maintains sufficient knowledge of the current security state of the system to determine whether continued operation is acceptable based on ongoing risk determinations—and if not, which steps in the RMF need to be revisited to effectively respond to the additional risk. Formal reauthorizations are avoided in situations where continuous monitoring provides authorizing officials with the information necessary to manage the potential risk arising from any changes to the system or its environment of operation. If a formal reauthorization is required, organizations maximize the use of status reports and security and privacy state information that is produced during the continuous monitoring process to minimize the level of effort required.

When a system or common controls are under ongoing authorization, the system or controls may be authorized on a time-driven or event-driven basis, leveraging the security- and privacy-related information generated by the continuous monitoring program. The system and common controls are authorized on a time-driven basis in accordance with the authorization frequency determined as part of the continuous monitoring strategy. The system and common controls are authorized on an event-driven basis when predefined (trigger) events occur. This occurs at the discretion of the authorizing official. Whether the authorization is time-driven or event-driven, the authorizing official acknowledges ongoing acceptance of identified risks. The organization determines the level of formality required for such acknowledgement by the authorizing official.

System and Organizational Conditions for Implementation of Ongoing Authorization

When the RMF has been effectively applied across the organization and the organization has implemented a robust continuous monitoring program, organizational systems may transition from a static, point-in-time authorization process to a more dynamic, near real-time ongoing authorization process. To do so, the following conditions must be satisfied:

Condition 1 – The system or common controls being considered for ongoing authorization must have received an initial authorization based on a complete, zero-base review of the system or the common controls.[76]

Condition 2 – An organizational continuous monitoring program is in place that monitors all implemented security and privacy controls with the appropriate degree of rigor and at the required frequencies specified by the organization in accordance with the continuous monitoring strategy and NIST guidance.[77]

The organization defines and implements a process to designate that the system and the common controls have satisfied the two conditions and are transitioning to ongoing authorization. This includes the authorizing official formally acknowledging that the system is now being managed by an ongoing authorization process and accepting the responsibility for performing all necessary

[76] System owners and authorizing officials leverage security- and privacy-related information about inherited common controls from assessments conducted by common control providers.

[77] NIST Special Publication 800-53 and NIST Special Publication 800-53A provide guidance regarding the appropriate degree of rigor for security assessments and monitoring. Future updates to NIST Special Publication 800-53A will address privacy assessments.

activities associated with that process. The transition to ongoing authorization is documented by the authorizing official by issuing a new authorization decision document.[78] The security- and privacy-related information generated through the continuous monitoring process is provided to the authorizing officials and other organizational officials in a timely manner through security management and reporting tools. Such tools facilitate risk-based decision making for the ongoing authorization for systems and common controls.

Information Generation, Collection, and Independence Requirements

To support ongoing authorization, security- and privacy-related information for security and privacy controls is generated and collected at the frequency specified in the organizational continuous monitoring strategy. Such information may be collected using automated tools or other methods of assessment depending on the type and purpose of the control and the desired rigor of the assessment. Automated tools may not generate security- and privacy-related information sufficient to support the authorizing official in making risk determinations. This occurs because the tools do not generate information for every security and privacy control or every part of an implemented control; additional assurance is needed; or the tools do not generate information on specific technologies or platforms. In such cases, manual or procedural security and privacy control assessments are conducted at organizationally-defined frequencies to cover any gaps in automated security- and privacy-related information generation. The manually or procedurally-generated assessment results are provided to the authorizing official in the manner deemed appropriate by the organization.

To support ongoing authorizations for moderate-impact and high-impact systems, the security- and privacy-related information provided to the authorizing official, whether generated manually or procedurally or in an automated fashion, is produced and analyzed by an entity that meets the independence requirements defined by the organization. The independent entity is impartial and free from any perceived or actual conflicts of interest regarding the development, implementation, assessment, operation, or ongoing management of the organizational systems and common controls being monitored.

Ongoing Authorization Frequency

NIST Special Publication 800-53, security control CA-6, Part c. specifies that the authorization for a system and any common controls inherited by the system be updated at an organization-defined frequency. This reinforces the concept of ongoing authorization. Thus, in accordance with CA-6 (along with the security and privacy control assessment and monitoring frequency determinations defined as part of the continuous monitoring strategy), organizations determine a frequency with which authorizing officials review security- and privacy-related information via the security/privacy management and reporting tool.[79] This near real-time information is used to determine whether the mission/business risk of operating the system or inheriting the common controls continues to be acceptable. NIST Special Publication 800-137 provides criteria for determining assessment/monitoring frequencies.

[78] Prior to transitioning to ongoing authorization, organizations have authorization decision documents that include an authorization termination date. By requiring a new authorization decision document, it is made clear that the system or the common controls are no longer bound to the termination date specified in the initial authorization document because the system and the common controls are now under ongoing authorization.

[79] *Ongoing authorization* and *ongoing assessment* are different concepts but closely related. To employ an ongoing authorization approach (which implies an ongoing understanding and acceptance of security risk), organizations must have in place, an organization-level and system-level continuous monitoring process to assess implemented security controls on an ongoing basis. The findings/results from ongoing control assessments provides critical information to authorization officials to support near-real time risk-based decision making.

Under ongoing authorization, *time-driven* authorization triggers refer to the frequency with which the organization determines that authorizing officials are to review security- and privacy-related information and authorize the system (or common controls) for continued operation as described above. Time-driven authorization triggers can be based on a variety of organization-defined factors including, for example, the impact level of the system. When a time-driven trigger occurs, authorizing officials review security- and privacy-related information on the systems for which they are responsible and accountable to determine the ongoing organizational mission/business risk, the acceptability of such risk in accordance with organizational risk tolerance, and whether the approval for continued operation is justified and in the best interest of the organization. The organizational continuous monitoring process, supported by the organization's security/privacy management and reporting tools, provides the appropriate functionality to notify the responsible and accountable authorizing official that it is time to review the security- and privacy-related information to support ongoing authorization.

In contrast to time-driven authorization triggers, *event-driven* triggers necessitate an immediate review of security- and privacy-related information by the authorizing official. Organizations may define event-driven *triggers* (i.e., indicators or prompts that cause an organization to react in a predefined manner) for ongoing authorization and reauthorization. When an event-driven trigger occurs under ongoing authorization, the authorizing official is either notified by organizational personnel (e.g., senior agency information security officer, senior agency official for privacy, system owner, common control provider, or system security or privacy officer) or via automated tools that defined trigger events have occurred requiring an immediate review of the system or common controls; or the authorizing official determines independently that an immediate review is required. The authorizing official reviews available security- or privacy-related information via the security/privacy management and reporting tools or may request procedurally- or manually-generated information to make effective ongoing risk determinations. This immediate review is conducted in addition to the time-driven frequency for review defined in the organizational continuous monitoring strategy (i.e., CA-6c./time-driven authorization) and occurs within ongoing authorization when the residual risk remains within the acceptable limits of organizational risk tolerance.[80]

Transitioning from Static Authorization to Ongoing Authorization

The intent of continuous monitoring is to monitor security and privacy controls at a frequency to provide authorizing officials with the necessary and sufficient information to make effective, risk-based decisions, whether by automated or procedural/manual means. However, if a substantial portion of monitoring is not accomplished via automation, it will not be feasible or practical for organizations to move from the current static authorization approach to an effective and efficient ongoing authorization approach. A phased approach for the generation of security- and privacy-related information may be necessary during the transition as automated tools become available and a greater number of security and privacy controls are monitored by automated techniques. Organizations may begin by generating security- and privacy-related information from automated tools that are in place and fill in gaps by generating additional information from procedural or manual assessments. As additional automated monitoring functionality is added, processes can be adjusted.

[80] The immediate reviews initiated by specific trigger events may occur simultaneously (i.e., in conjunction) with time-driven monitoring activities based on the monitoring frequencies established by the organization and how the reviews are structured within the organization. The same reporting structure may be used for event- and time-driven reviews to achieve efficiencies.

Transitioning from a static authorization process to a dynamic, ongoing authorization process requires considerable thought and preparation. One methodology that organizations may consider is to take a phased approach to the migration based on the security categorization of the system. Because risk tolerance levels for low-impact systems are likely to be greater than for moderate-impact or high-impact systems, implementing continuous monitoring and ongoing authorization for low-impact systems first may help ease the transition—allowing organizations to incorporate lessons learned as continuous monitoring and ongoing authorization are implemented for the moderate-impact and high-impact systems. This will facilitate the continued steady and consistent progression of the continuous monitoring and ongoing authorization implementation from the lowest to the highest impact levels for the systems within the organization. Organizations may also consider employing the phased implementation approach by partitioning their systems into well-defined subsystems or system components and subsequently transitioning those subsystems or system components to ongoing authorization one segment at a time until the entire system is ready for the full transition (at which time the authorizing official acknowledges that the system is now being managed by an ongoing authorization process).

REAUTHORIZATION

Reauthorization actions occur at the discretion of the authorizing official in accordance with federal or organizational policy. If a reauthorization action is required, organizations maximize the use of security, privacy, and risk-related information produced as part of the continuous monitoring processes currently in effect. Reauthorization actions, if initiated, can be either time-driven or event-driven. Time-driven reauthorizations occur when the authorization termination date is reached (if one is specified). If the system is under ongoing authorization,[81] a time-driven reauthorization may not be necessary. However, if the continuous monitoring program is not yet sufficiently comprehensive to fully support ongoing authorization, a maximum authorization period can be specified by the authorizing official. Authorization termination dates are influenced by federal and organizational policies and by the requirements of authorizing officials. Under ongoing authorization, a full reauthorization may be necessary if an event occurs that produces risk above the acceptable organizational risk tolerance. This situation may occur, for example, if there was a catastrophic breach/incident or failure of or significant problems with the continuous monitoring program. Reauthorization actions may necessitate a review of and changes to the continuous monitoring strategy which may in turn, affect ongoing authorization.

For security and privacy control assessments associated with reauthorization, organizations leverage security- and privacy-related information generated by the continuous monitoring program and fill in any gaps with manual or procedural assessments. Organizations may supplement automatically-generated assessment information with manually/procedurally-generated information in situations where greater assurance is needed. If security and privacy control assessments are conducted by qualified assessors with the necessary independence, use appropriate security and privacy standards and guidelines, and are based on the needs of the authorizing official, the assessment results can be cumulatively applied to the reauthorization.[82] The reauthorization action may be as simple as updating security and privacy status information in the authorization package (i.e., the security and privacy plans, security and privacy assessment reports, and plans of action and milestones), focused only on specific problems or ongoing issues, or as comprehensive as the initial authorization. The authorizing official signs an updated

[81] An ongoing authorization approach requires that a continuous monitoring program is in place to monitor all implemented security controls with a frequency specified in the continuous monitoring strategy.

[82] NIST Special Publication 800-53A describes the specific conditions when security-related information can be reused to support authorization actions.

authorization decision document based on the current risk determination and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation.[83] In all situations where there is a decision to reauthorize a system or the common controls inherited by organizational systems, the maximum reuse of authorization information is encouraged to minimize the time and expense associated with the reauthorization effort.

EVENT-DRIVEN TRIGGERS AND SIGNIFICANT CHANGES

Organizations define event-driven *triggers* (i.e., indicators or prompts that cause a predefined organizational reaction) for both ongoing authorization and reauthorization. Event-driven triggers may include, but are not limited to:

- New threat, vulnerability, privacy risk, or impact information;
- An increased number of findings, weaknesses, or deficiencies from the continuous monitoring program;
- New missions/business requirements;
- Change in the authorizing official;
- Significant change in risk assessment findings;
- Significant changes to the system, common controls, or the environments of operation; or
- Exceeding organizational thresholds.

When there is a change in authorizing officials, the new authorizing official reviews the current authorization decision document, authorization package, any updated documents from ongoing monitoring activities, or a report from automated security/privacy management and reporting tools. If the new authorizing official finds the current risk to be acceptable, the official signs a new or updated authorization decision document, formally transferring responsibility and accountability for the system or the common controls. In doing so, the new authorizing official explicitly accepts the risk to organizational operations and assets, individuals, other organizations, and the Nation. If the new authorizing official finds the current risk to be unacceptable, an authorization action (i.e., ongoing authorization or reauthorization) can be initiated. Alternatively, the new authorizing official may instead establish new terms and conditions for continuing the original authorization, but not extend the original authorization termination date (if not under ongoing authorization).

A significant change is defined as a change that is likely to affect the security or privacy state of a system. Significant changes to a system that may trigger an event-driven authorization action may include, but are not limited to:

- Installation of a new or upgraded operating system, middleware component, or application;
- Modifications to system ports, protocols, or services;
- Installation of a new or upgraded hardware platform;
- Modifications to cryptographic modules or services; or
- Modifications to security and privacy controls.

[83] Decisions to initiate a formal reauthorization action include inputs from the senior accountable official for risk management/risk executive (function), senior agency information security officer, and senior agency official for privacy.

Significant changes to the environment of operation that may trigger an event-driven authorization action may include, but are not limited to:

- Moving to a new facility;
- Adding new core missions or business functions;
- Acquiring specific and credible threat information that the organization is being targeted by a threat source; or
- Establishing new/modified laws, directives, policies, or regulations.

The examples of changes listed above are only significant when they meet the organizational threshold established in the definition of significant change (i.e., a change that is likely to affect the security and privacy state of the system). Organizations establish definitions of significant change based on a variety of factors including, for example, mission and business needs; threat and vulnerability information; environments of operation for systems; privacy risks; and security categorization.

Risk assessment results or the results from a security or privacy impact analysis may be used to determine if changes to systems or common controls are sufficiently significant to trigger an authorization action. If an authorization action is initiated, the organization targets only the specific security and privacy controls affected by the changes and reuses previous assessment results wherever possible. An effective monitoring program can significantly reduce the overall cost and level of effort of authorization actions. Most changes to a system or its environment of operation can be handled through the continuous monitoring program and ongoing authorization.

TYPE AND FACILITY AUTHORIZATIONS

A *type authorization*[84] is an official authorization decision to employ identical copies of a system or subsystem (including hardware, software, firmware, or applications) in specified environments of operation. This form of authorization allows a single authorization package (i.e., security and privacy plans, security and privacy assessment reports, and plans of action and milestones) to be developed for an archetype (i.e., common) version of a system that is deployed to multiple locations, along with installation and configuration requirements or operational security and privacy needs, that will be assumed by the hosting organization at a specific location. The type authorization is used in conjunction with authorized site-specific controls[85] or with a facility authorization as described below.

A *facility authorization* is an official authorization decision that is focused on specific security and privacy controls implemented in a defined environment of operation to support one or more systems residing within that environment. This form of authorization addresses common controls within a facility and allows systems residing in the defined environment to inherit the common controls and the affected system security and privacy plans to reference the authorization package for the facility. The common controls are provided at a specified impact level to facilitate risk decisions on whether it is appropriate to locate a given system in the facility.[86] Physical and

[84] Examples of type authorizations include: an authorization of the hardware and software applications for a standard financial system deployed in multiple locations; or an authorization of a common workstation or operating environment (i.e., hardware, operating system, and applications) deployed to all operating units within an organization.

[85] Site-specific controls are typically implemented by an organization as *common controls*. Examples include physical and environmental protection controls and personnel security controls.

[86] For example, if the facility is categorized as moderate impact, it would not be appropriate to locate high-impact systems or system components in that environment of operation.

environmental controls are addressed in a facility authorization but other controls may also be included, for example, boundary protections; contingency plan and incident response plan for the facility; training and awareness and personnel screening for facility staff.

Type authorizations and facility authorizations can be described in the context of the three types of authorizations: authorization to use, authorizations to operate, and authorizations to provide. The facility authorization official issues a common control authorization to describe the common controls available for inheritance by systems residing within the facility. A type authorization is issued by the authorizing official responsible for the development of the archetype (i.e., common) version of a system.[87] This authorization represents an authorization to operate. The authorizing official who will be using and possibly taking ownership of the system at the site or facility is responsible and accountable for the risk in doing so—and accordingly, issues an authorization to use. This authorization leverages the information available in the authorization package for the system based on the authorization to operate and the information from the authorization package for the facility common controls based on the common control authorization.

AUTHORIZATION APPROACHES

Organizations can choose from two approaches when planning for and conducting authorizations. These include an authorization with a *single* authorizing official or an authorization with *multiple* authorizing officials.[88]

The first approach is the traditional authorization process defined in this appendix where a single organizational official in a senior leadership position is responsible and accountable for a system or for common controls. The organizational official accepts the security- and privacy-related risks that may adversely impact organizational operations and assets, individuals, other organizations, or the Nation.

The second approach, *joint authorization*, is employed when multiple organizational officials either from the same organization or different organizations, have a shared interest in authorizing a system. The organizational officials collectively are responsible and accountable for the system and jointly accept the security- and privacy-related risks that may adversely impact organizational operations and assets, individuals, other organizations, and the Nation. A similar authorization process is followed as in the single authorization official approach with the essential difference being the addition of multiple authorizing officials. Organizations choosing a joint authorization approach are expected to work together on the planning and the execution of RMF tasks and to document their agreement and progress in implementing the tasks. Collaborating on security categorization, security and privacy control selection and tailoring, plan for assessing the controls to determine effectiveness, plan of action and milestones, and continuous monitoring strategy is necessary for a successful joint authorization.[89] The specific terms and conditions of the joint authorization are established by the participating parties in the joint authorization including, for example, the process for ongoing determination and acceptance of risk. The joint authorization remains in effect only while there is agreement among authorizing officials and the authorization

[87] Typically, type authorizations are issued by organizations that are responsible for developing standardized hardware and software capabilities for customers and delivered to the recipient organizations as "turn key" solutions. The senior leaders issuing such authorizations may be referred to as developmental authorizing officials.

[88] Authorization approaches can be applied to systems and to common controls inherited by organizational systems.

[89] Risk-based decisions related to control selection and baseline tailoring actions by organizations providing cloud or shared systems, services, or applications should consider the protection needs of the customer organizations that may be using those cloud or shared systems, services, or applications. Thus, organizations hosting cloud or shared systems, services, or applications should consider the shared risk of operating in those types of environments.

meets the specific requirements established by federal and organizational policies. NIST Special Publication 800-53 controls CA-6 (1), *Joint Authorization – Same Organization* and CA-6 (2) *Joint Authorization – Different Organizations*, describe the requirements for joint authorizations.

LEVERAGING EXTERNAL PROVIDER CONTROLS AND ASSESSMENTS

Organizations should exercise caution when attempting to leverage external provider security and privacy controls and assessment results. Security and privacy controls implemented by external providers may be different than the controls in NIST Special Publication 800-53 in the scope, coverage, and capability provided. NIST provides a mapping of the security and privacy controls in its catalog to the ISO/IEC 27001 security controls and to the ISO/IEC 15408 security requirements. However, such mappings are inherently subjective and should be reviewed carefully by organizations to determine if the security and privacy controls and requirements addressed by external providers meet the protection needs of the organization.

Similar caution should be exercised when attempting to use or leverage security and privacy assessment results from external providers. The type, rigor, and scope of the assessments may vary widely from provider to provider. In addition, the assessment procedures employed by the provider and the independence of the assessors conducting the assessments are critical issues that should be reviewed and considered by organizations prior to leveraging assessment results.

Effective risk decisions by authorizing officials depend on the transparency of the security and privacy controls selected and implemented by external providers and the quality and efficacy of the assessment evidence produced by those providers. Transparency is essential to achieve the assurance and trustworthiness necessary to ensure adequate protection for organizational assets.

APPENDIX D

OTHER CONSIDERATIONS

SYSTEM DEVELOPMENT LIFE CYCLE AND SUPPLY CHAIN EFFECTS ON THE RMF

SYSTEM DEVELOPMENT LIFE CYCLE

All systems, including operational systems, systems under development, and systems undergoing modification or upgrade, are in some phase of a system development life cycle.[90] Requirements definition is a critical part of any system development process and begins early in the life cycle, typically in the *initiation* phase.[91] Security and privacy requirements are a subset of the overall functional and nonfunctional[92] requirements allocated to a system. The security and privacy requirements are incorporated into the system development life cycle simultaneously with the functional requirements and the nonfunctional requirements. Without the early integration of security and privacy requirements, significant expense may be incurred by the organization later in the life cycle to address security and privacy concerns that could have been included in the initial design. When security and privacy requirements are considered as an integral subset of other system requirements, the resulting system has fewer weaknesses and deficiencies, and therefore, fewer privacy risks or vulnerabilities that can be exploited in the future.

Integration of security and privacy requirements into the system development life cycle is the most cost-effective and efficient method to ensure that an organizational protection strategy is implemented. It also ensures that security- and privacy-related processes are not isolated from other processes employed by the organization to develop, implement, operate, and maintain the systems supporting ongoing missions and business functions. In addition to incorporating security and privacy requirements into the system life cycle, the requirements are also integrated into the program, planning, and budgeting activities within the organization to ensure that resources are available when needed and program/project milestones are completed. The enterprise architecture provides a central record of this integration within an organization.

Ensuring that security and privacy requirements are integrated into the system development life cycle helps facilitate the development and implementation of more resilient systems to reduce the security and privacy risk to organizational operations and assets, individuals, other organizations, and the Nation. This can be accomplished by using the concept of integrated project teams.[93] Organizational officials ensure that security and privacy professionals are part of the system development life cycle activities. Such consideration fosters an increased level of cooperation among personnel responsible for the development, implementation, assessment, operation, maintenance, and disposition of systems and the security and privacy professionals advising the senior leadership on the security and privacy controls needed to adequately mitigate risk and protect critical missions and business functions.

Finally, organizations maximize the use of security- and privacy-relevant information generated during the system development life cycle process to satisfy requirements for similar information

[90] There are typically five phases in the system development life cycle including initiation; development/acquisition; implementation; operation/maintenance; and disposal.

[91] Organizations may employ a variety of system development life cycle processes including, for example, waterfall, spiral, or agile development.

[92] Nonfunctional requirements include, for example, quality and assurance requirements.

[93] Integrated project teams are multidisciplinary entities consisting of individuals with a range of skills and roles to help facilitate the development of systems that meet the requirements of the organization.

needed for security- and privacy-related purposes. The judicious reuse of such information is an effective method to eliminate duplication of effort, reduce documentation, promote reciprocity, and avoid unnecessary costs that may result when security and privacy activities are conducted independently of system development life cycle processes. In addition, reuse promotes greater consistency of information used in the development, implementation, assessment, operation, maintenance, and disposition of systems including security- and privacy-related considerations.

SUPPLY CHAIN RISK MANAGEMENT

Organizations are becoming increasingly reliant on component products, systems, and services provided by external providers to carry out their important missions and business functions. Organizations are responsible and accountable for the risk incurred when using such component products, systems, and services. Relationships with external providers can be established in a variety of ways, for example, through joint ventures, business partnerships, various types of formal agreements (i.e., contracts, interagency agreements, lines of business arrangements, licensing agreements), or outsourcing arrangements. The growing dependence on products, systems, and services from external providers and the relationships with those providers, present an increasing amount of risk to the organization. Some of the risks associated with the global and distributed nature of product and service supply chains include the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the supply chain. These risks are associated with an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. Challenges to managing these risks include:

- Defining the types of component products, systems, and services provided to the organization by external providers;
- Describing how component products, systems, and services provided by external providers are protected in accordance with the security requirements of the organization; and
- Obtaining the necessary assurances that the risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of component products, systems, and services provided by external providers is either avoided, mitigated, or acceptable.

FISMA and OMB policy require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies. Security and privacy requirements for external providers including the security and privacy controls for systems processing, storing, or transmitting federal information are expressed in contracts or other formal agreements. Organizations require external providers to implement all steps in the RMF except for the authorization step, which remains an inherent federal responsibility that is directly linked to the management of risk related to the use of external system services.

OMB policy also requires departments and agencies to develop and implement supply chain risk management plans. Managing supply chain risks is a complex, multifaceted undertaking requiring a coordinated effort across an organization—building trust relationships and communicating with internal and external stakeholders. This includes engaging multiple disciplines in identifying priorities and developing solutions; ensuring that robust supply chain risk management (SCRM) activities are performed throughout the system development life cycle; and incorporating SCRM into overall risk management decisions. SCRM activities should involve identifying and assessing

applicable risks, determining appropriate mitigating actions, developing appropriate SCRM plans to document selected mitigating actions, and monitoring performance against SCRM plans. Because supply chains differ across and within organizations, SCRM plans should be tailored to individual organizational, program, and operational contexts. Tailored SCRM plans provide the basis for determining whether a system is "fit for purpose" and as such, the security and privacy controls need to be tailored accordingly. Tailored SCRM plans will help organizations to focus appropriate resources on the most critical functions and components based on organizational mission/business requirements and their risk environment.

The assurance or confidence that the risk from using products, systems, or services from external providers is at an acceptable level depends on the level of assurance[94] that the organization can gain from the providers. The level of assurance is based on the degree of control the organization can exert on the external provider regarding the security and privacy controls necessary for the protection of the product, system, or service and the evidence brought forth as to the effectiveness of those controls. The degree of control can be established by the terms and conditions of the contract or service-level agreement. Some organizations have extensive control of the required security and privacy controls through contract vehicles or agreements that specify the security and privacy requirements for the external provider. Other organizations have rather limited control because of purchasing commodity services or commercial off-the-shelf products. The level of assurance can also be based on many other factors that convince the organization that the requisite security and privacy controls have been implemented and that a credible determination of control effectiveness exists. For example, an authorized external cloud service provided to an organization through a well-established line of business relationship may provide a level of trust in the service that is within the risk tolerance of the organization.

Ultimately, the responsibility for responding to risks arising from the use of products, systems, and services from external providers remains with the organization and the authorizing official. Organizations require that an appropriate *chain of trust* be established with external providers when dealing with the many issues associated with system security or privacy risks. A chain of trust requires that organizations establish and retain a level of trust such that each participant in the consumer-provider relationship provides adequate protection for component products, systems, and services provided to the organization. The trust chain can be complicated due to the number of entities participating in the consumer-provider relationships and the types of relationships between the parties. In certain situations, external providers may outsource the development of component products, systems, and services to other external entities, making the chain of trust complicated and difficult to manage. Depending on the type of component product, system, or service, it may be unwise for the organization to place significant trust in the external provider. This is not due to any inherent untrustworthiness on the provider's part, but due to the intrinsic level of risk in the product, system, or service. Where sufficient trust cannot be established in the product, system or service, the organization can employ mitigating controls; accept more risk; or choose to not obtain the product, system, or service from the external provider.[95]

[94] The level of assurance provided by an external provider can vary widely, ranging from those who provide high assurance (e.g., business partners in a joint venture that share a common business model and goals) to those who provide less assurance and represent greater sources of risk (e.g., business partners in one endeavor who are also competitors in another market sector).

[95] NIST Special Publication 800-161 provides guidance on supply chain risk management practices.