The attached DRAFT document (provided here for historical purposes), originally posted on May 9, 2018, **has been superseded by the following publication**:

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

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

Publication Date: **October 2, 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/2018-05-09
- 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 ~~1~~2

~~Guide for Applying the~~ Risk Management Framework ~~to~~ ~~Federal~~for Information Systems and Organizations

A ~~Security~~System Life Cycle Approach for Security and Privacy

JOINT TASK FORCE

This publication contains comprehensive updates to the *Risk Management Framework*. These updates include an alignment with the NIST Cybersecurity Framework, the integration of privacy risk management principles and concepts, an alignment with the systems security engineering life cycle processes, and the incorporation of organization-wide risk management and supply chain risk management concepts. These frameworks, concepts, principles, and processes can be applied in a complementary manner to more effectively manage the security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. In addition, there are new RMF tasks that are designed to help better prepare information system owners to execute their system-level risk management activities—thus, increasing efficiency and effectiveness by establishing a closer connection to the missions and business functions of the organization and improving communications with senior leaders.

NOTE TO REVIEWERS

Markup Version of Special Publication (SP) 800-37, Revision 2, Initial Public Draft

This markup version of SP 800-37, Rev. 2 reflects only the significant changes to Risk Management Framework. Formatting, structural, minor editorial changes that do not impact the technical content of this publication are not reflected in this markup.

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

Draft NIST Special Publication 800-37
Revision 1~~2~~

~~Guide for Applying the~~ Risk Management Framework ~~to~~ ~~Federal~~for Information Systems and Organizations

A ~~Security~~System Life Cycle Approach for Security and Privacy

~~JOINT TASK FORCE~~
~~TRANSFORMATION INITIATIVE~~

~~*Computer Security Division*~~
~~*Information Technology Laboratory*~~
~~*National Institute of Standards and Technology*~~

http://dx.doi.org/10.6028/NIST.SP.800-37r1

~~February 2010~~

~~INCLUDES UPDATES AS OF 06-05-2014: PAGE IX~~

May 2018

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

National Institute of Standards and Technology
Walter Copan, 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 ~~1~~2
Natl. Inst. Stand. Technol. Spec. Publ. 800-37 ~~Revision 1, 102~~, Rev. 2, **149 pages** (~~February 2010~~May 2018)

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 publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: May 9 through June 22, 2018

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

Keywords

~~Risk management, risk assessment, security authorization, security control, system development life cycle, Risk Management Framework, security control assessment, continuous monitoring, ongoing authorization, security categorization, security control selection, security plan, security assessment report, plan of action and milestones, security authorization package, authorization to operate, common control, information system owner/steward, senior information security officer, common control provider, authorizing official.~~

~~Compliance with NIST Standards and Guidelines~~

~~In accordance with the provisions of FISMA,[1] the Secretary of Commerce shall, on the basis of standards and guidelines developed by NIST, prescribe standards and guidelines pertaining to federal information systems. The Secretary shall make standards compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of federal information systems. Standards prescribed shall include information security standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems.~~

- ~~Federal Information Processing Standards (FIPS) are approved by the Secretary of Commerce and issued by NIST in accordance with FISMA. FIPS are compulsory and binding for federal agencies.[2] FISMA requires that federal agencies comply with these standards, and therefore, agencies may not waive their use.~~
- ~~Special Publications (SPs) are developed and issued by NIST as recommendations and guidance documents. For other than national security programs and systems, federal agencies must follow those NIST Special Publications mandated in a Federal Information Processing Standard. FIPS 200 mandates the use of Special Publication 800-53, as amended. In addition, OMB policies (including OMB Reporting Instructions for FISMA and Agency Privacy Management) state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications.[3]~~
- ~~Other security-related publications, including interagency reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when specified by OMB.~~
- ~~Compliance schedules for NIST security standards and guidelines are established by OMB in policies, directives, or memoranda (e.g., annual FISMA Reporting Guidance).~~

~~[1] The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.~~

~~[2] The term *agency* is used in this publication in lieu of the more general term *organization* only in those circumstances where its usage is directly related to other source documents such as federal legislation or policy.~~

~~[3] While federal agencies are required to follow certain specific NIST Special Publications in accordance with OMB policy, there is flexibility in how agencies apply the guidance. Federal agencies apply the security concepts and principles articulated in the NIST Special Publications in accordance with and in the context of the agency's missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. Given the high priority of information sharing and transparency within the federal government, agencies also consider reciprocity in developing their information security solutions. When assessing federal agency compliance with NIST Special Publications, Inspectors General, evaluators, auditors, and assessors consider the intent of the security concepts and principles articulated within the specific guidance document and how the agency applied the guidance in the context of its mission/business responsibilities, operational environment, and unique organizational conditions.~~

assess; authorization to operate; common control authorization; authorization to use; authorizing official; categorize; common control; common control provider; continuous monitoring; control baseline; hybrid control; information owner or steward; monitor; ongoing authorization; plan of action and milestones; privacy assessment report; privacy control; privacy plan; privacy risk; profile; risk assessment; risk executive function; risk management; risk management framework; security assessment report; security control; security plan; security risk; senior agency official for privacy; senior agency information security officer; senior agency official for privacy; supply chain risk management; 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*	Kevin Herms *OMB*	Carol Bales *OMB*
Jeff Marron *NIST*	Kaitlin Boeckl *NIST*	Kirsten Moncada *OMB*	Jon Boyens *NIST*

The authors also wish to recognize Matt Barrett, Kathleen Coupe, Jeff Eisensmith, Chris Enloe, Ned Goren, Matthew Halstead, Jody Jacobs, Ralph Jones, Martin Kihiko, Raquel Leone, Celia Paulsen, and the scientists, engineers, and research staff from the Computer Security and Applied Cybersecurity Divisions for their exceptional contributions in helping to improve the content of the publication. A special note of thanks goes to Jim Foti and Elizabeth Lennon for their excellent technical editing and administrative support.

Commented [A1]: Changes not tracked.

In addition, the authors wish to acknowledge the United States Air Force and the "RMF Next" initiative, facilitated by Air Force CyberWorx, that provided the inspiration for some of the bold new ideas in the RMF 2.0. The working group, led by Lauren Knausenberger, Bill Bryant, and Venice Goodwine, included government and industry representatives Jake Ames, Chris Bailey, James Barnett, Steve Bogue, Wes Chiu, Shane Deichman; Joe Erskine, Terence Goodman, Jason Howe, Brandon Howell, Todd Jacobs, Peter Klabe, William Kramer, Bryon Kroger, Dihn Le, Noam Liran, Sam Miles, Michael Morrison, Raymond Tom Nagley, Wendy Nather, Jasmine Neal, Ryan Perry, Eugene Peterson, Lawrence Rampaul, Jessica Rheinschmidt, Greg Roman, Susanna Scarveles, Justin Schoenthal, Christian Sorenson, Stacy Studstill, Charles Wade, Shawn Whitney, David Wilcox, and Thomas Woodring.

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, John Gilligan, Pete Gouldmann, Richard Graubart, John Grimes, Gus Guissanie, Priscilla Guthrie, Jennifer Fabius, Cita Furlani, Richard Hale, Peggy Himes, William Hunteman, Arnold Johnson, Donald Jones, Stuart Katzke, Eustace King, Mark Morrison, Sherrill Nicely, Dorian Pappas, Esten Porter, Karen Quigg, George Rogers, Cheryl Roby, Gary Stoneburner, Marianne Swanson, Glenda Turner, and Peter Williams.

Foreword

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 2013 report, *Resilient Military Systems and the Advanced Cyber Threat*, provides a sobering assessment of the current vulnerabilities in the United States Government, 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 (SDLC) and can 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.

Executive Order (E.O.) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* recognizes the increasing interconnectedness of Federal information systems and requires agency heads to ensure appropriate risk management not only for the Federal agency's enterprise, but also for the Executive Branch as a whole. The E.O. states:

> *"…The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities…"*
>
> *"…Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents…"*

OMB Memorandum M-17-25 provides implementation guidance to Federal agencies for E.O. 13800. The memorandum states:

> *"… An effective enterprise risk management program promotes a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public. Such risks include, but are not limited to, strategic, market, cyber, legal, reputational, political, and a broad range of operational risks such as information security, human capital, business continuity, and related risks…"*
>
> *"… Effective management of cybersecurity risk requires that agencies align information security management processes with strategic, operational, and budgetary planning processes…"*

This update to NIST Special Publication 800-37 (Revision 2) responds to the call by the Defense Science Board, the Executive Order, and the OMB policy memorandum to develop the next-generation Risk Management Framework (RMF) for information systems, organizations, and individuals.

There are seven major objectives for this update:

- To provide closer linkage and communication between the risk management processes and activities at the C-suite or governance level of the organization and the individuals, processes, and activities at the system and operational level of the organization;
- To institutionalize critical organization-wide risk management preparatory activities to facilitate a more effective, efficient, and cost-effective execution of the RMF;
- To demonstrate how the Cybersecurity Framework can be aligned with the RMF and implemented using established NIST risk management processes;
- To integrate privacy risk management concepts and principles into the RMF and support the use of the consolidated security and privacy control catalog in NIST Special Publication 800-53, Revision 5;
- To promote the development of trustworthy secure software and systems by aligning life cycle-based systems engineering processes in NIST Special Publication 800-160 with the steps in the RMF;
- To integrate supply chain risk management (SCRM) concepts into the RMF to protect against untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout the SDLC; and
- To provide an alternative organization-generated control selection approach to complement the traditional baseline control selection approach.

The addition of the *Prepare* step is one of the key changes to the RMF—incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes. The primary objectives for institutionalizing organization-level and system-level preparation are—

- To facilitate better communication between senior leaders and executives at the organization and mission/business process levels and system owners on the front lines of execution and operation.
- To facilitate organization-wide identification of common controls and the development of organization-wide tailored control baselines, to reduce the workload on individual system owners and the cost of system development and asset protection.
- To reduce the complexity of the information technology (IT) and operations technology (OT) infrastructure using Enterprise Architecture concepts and models to consolidate, optimize, and standardize organizational systems, applications, and services.
- To identify, prioritize, and focus resources on the organization's high-value assets and high-impact systems that require increased levels of protection—taking steps commensurate with the risk to such assets.

Recognizing that organizational preparation for RMF execution may vary from organization to organization, achieving the objectives outlined above can reduce the IT 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.

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

COMMON SECURITY AND PRIVACY FOUNDATIONS

In developing standards and guidelines, NIST consults with federal agencies, state, local, and tribal governments, and private sector organizations; avoids unnecessary and costly duplication of effort; and ensures 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 Management and Budget, as well as the Office of the Director of National Intelligence, Department of Defense, and Committee on National Security Systems, and has established a unified risk management framework for the federal government. This common foundation provides the Civil, Defense, and Intelligence Communities of the federal government and their contractors, more cost-effective, flexible, and consistent methods to manage security and privacy 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 public and private sector entities to establish mappings and relationships between its information security and privacy standards and guidelines and those developed by external organizations.

ACCEPTANCE OF SECURITY AND PRIVACY RISK

The Risk Management Framework (RMF) addresses security and privacy risk from two distinct perspectives—an *information system* perspective and a *common controls* perspective. For an information system, authorizing officials issue an authorization to operate or authorization to use for the system, accepting the security and privacy risks to the organization's operations and assets, individuals, other organizations, and the Nation. Alternatively, for common controls, authorizing officials issue a common control authorization for a specific set of controls that can be inherited by designated organizational systems, accepting the security and privacy risks to the organization's operations and assets, individuals, other organizations, and the Nation. Authorizing officials also consider the risk of inheriting common controls as part of their system authorizations. The different types of authorizations are described in Appendix F.

USE OF AUTOMATION IN THE EXECUTION OF THE RMF

Organizations should maximize the use of *automation*, wherever possible, to increase the speed, effectiveness, and efficiency of executing the steps in the Risk Management Framework (RMF). Automation is particularly useful in the assessment and continuous monitoring of security and privacy controls, the preparation of authorization packages, and the implementation of ongoing authorization approaches—together facilitating more real-time or near real-time risk-based decision making for senior leaders. Organizations have significant flexibility in deciding when, where, and how to use automation or automated support tools for their respective security and privacy programs. In some situations, and for certain security and privacy controls, automated assessments and monitoring may not be possible or feasible.

MANAGING 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). 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 organizations.

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 interoperate with the risk management processes and approaches 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 organization-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 the RMF includes references to applicable sections of the Cybersecurity Framework. For example, RMF Prepare—Organization Level step, Task 2, *Risk Management Strategy*, aligns with the Cybersecurity Framework Core [Identify Function]; RMF Prepare—Organization Level step, Task 4, *Organization-Wide Tailored Control Baselines and Profiles*, aligns with the construct of Cybersecurity Framework Profiles; and RMF Authorize step, Task 5, *Authorization Reporting*, and RMF Monitor step, Task 5, *Security and Privacy Posture Reporting*, support OMB reporting and security risk management requirements using the Functions, Categories, and Subcategories in the Cybersecurity Framework. The subcategory mappings to the security controls in NIST Special Publication 800-53 is available at: https://www.nist.gov/cyberframework/federal-resources.

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 controls to help protect federal information systems and organizations; and an effective and efficient 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 cybersecurity solutions.

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED FOR INFORMATION SECURITY, PRIVACY, AND RISK MANAGEMENT

Organizations depend on information systems[4] to successfully carry out their missions and business functions and those systems are constantly subject to serious threats. While the threats to information systems necessarily include environmental disruptions and human or machine errors, in today's environment the most significant threats to systems come from purposeful attacks that are often disciplined, well-organized, and well-funded. These attacks are generally, and in a growing number of cases, very sophisticated. When successful, attacks on information systems can result in serious or catastrophic damage to not just the organizational assets and operations,[5] but also to individuals, other organizations, and the Nation.[6] Given the significant and ever-increasing danger of those threats, it is imperative that organizations remain vigilant and that leaders and managers at all organizational levels understand their responsibilities and are accountable for protecting organizational assets and for managing security risks.[7]

In addition to the responsibility to protect organizational assets from the variety of threats that exist in today's environment, organizations also have a responsibility to consider and manage the risk to individuals when information systems process personally identifiable information (PII). Organizations' information security and privacy programs have complementary objectives with respect to managing the confidentiality, integrity, and availability of PII. While many privacy risks relate to the unauthorized access or disclosure of PII, some privacy risks may result from authorized uses and other related activities. For example, privacy risks may result from the creation, collection, use, and retention of PII; the inadequate quality or integrity of PII; and the lack of appropriate notice, transparency, or participation. While managing privacy risk requires close coordination between organizations' information security and privacy programs, privacy risks raise distinct concerns that require different expertise and different approaches. Therefore, it is critical that organizations establish and maintain robust privacy programs to ensure compliance with applicable privacy requirements and to manage the risk to individuals associated with the processing of PII.

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 ~~common information security framework for the federal government and its contractors. The intent of this common~~

[4] 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; paper-based systems; industrial/process control systems; cyber-physical systems; weapons systems; super computers; command, control, and communications systems; small form factor devices such as smart phones and tablets; environmental control systems; and embedded devices/sensors.

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

[6] 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.

[7] 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 is*Risk Management Framework* (RMF) to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies. This publication, developed by organizations. In July 2016, the Joint Task Force Transformation Initiative Working Group, transforms the traditional Certification and Accreditation (C&A) process into the six-step Risk Office of Management Framework (and Budget (OMB) revised Circular A-130 to include specific responsibilities for privacy programs under the RMF.[8] The RMF emphasizes risk management by building security and privacy capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls; (ii)throughout the SDLC; maintaining awareness of the security and privacy posture of information systems on an ongoing basis through continuous monitoring processes; and providing information to senior leaders and executives to facilitate decisions regarding the acceptance of risk to organizational operations and 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 controls; and the authorization of information systems and common controls;
- Promotes 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 seamless integration of security and privacy requirements and controls into enterprise architecture, SDLC, acquisition processes, and the authorization of information 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);[9] and
- Establishes responsibility and accountability for controls implemented within information systems and inherited by those systems.

The risk management process described in this publication changes the traditional focus of C&A as RMF provides a static, procedural activity to a more dynamic and flexible approach to effectively manage information system-related security and privacy risks in diverse environments with complex and sophisticated threats, 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:

[8] OMB Circular A-130, "Managing Federal Information as a Strategic Resource" (2016).
[9] OMB Memorandum M-17-25 defines a key organizational role of senior accountable official for risk management.

- 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 security and privacy protections for organizational information and information systems through the implementation of appropriate risk response strategies;
- To facilitate the implementation of the Framework for Improving Critical Infrastructure Cybersecurity.[10]
- To ensure that security and privacy requirements and controls are effectively integrated into the enterprise architecture, SDLC processes, acquisition processes, and systems engineering processes;[11] and
- To support consistent, informed, and ongoing ~~security~~ authorization decisions (through continuous monitoring),[12] transparency and traceability of security~~-~~ and ~~risk management~~privacy-related information, and reciprocity.[13]

This publication is intended to help organizations manage risk and to satisfy the security and privacy requirements in FISMA, the Privacy Act ~~(FISMA) and meets or exceeds the information security requirements established for executive agencies[14] by the Office of Management and Budget (~~of 1974, OMB policies (e.g., OMB Circular A-130~~, Appendix III, *Security of Federal Automated Information Resources*. The guidelines in this publication are applicable to all federal information systems other than those systems.)~~, and designated ~~as national security systems as defined in 44 U.S.C., Section 3542.~~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.[15]

1.3 TARGET AUDIENCE

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

- Individuals with mission or business ownership responsibilities or fiduciary responsibilities including, for example, and heads of federal agencies;

[10] Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.
[11] NIST Special Publication 800-160, Volume 1, provides guidance and considerations for a multidisciplinary approach in the engineering of trustworthy secure systems as part of the SDLC process.
[12] NIST Special Publication 800-137 provides guidance on information security continuous monitoring programs. Future updates to this publication will also address privacy continuous monitoring.
[13] *Reciprocity* is ~~the mutual~~an agreement among participating organizations to accept each other's security ~~assessments in order~~and privacy assessment results to reuse system resources ~~and/~~or to accept each other's assessed security and privacy posture ~~in order~~ to share information. Reciprocity ~~is best achieved by promoting the concept of transparency (i.e., making sufficient evidence regarding the security state of an information system available, so that an authorizing official from another organization can use that evidence~~does not apply to ~~make credible,~~ accepting the risk-based decisions ~~regarding the operation and use of that system or the information it processes, stores, or transmits).~~of other organizations.

- Individuals with information system development and ~~integration~~acquisition responsibilities, including, for example, program managers, ~~information technology~~procurement officials, component product and system developers, systems integrators, and enterprise architects~~, information security architects);~~;
- Individuals with information system, security, or privacy management and/or oversight responsibilities including, for example, senior leaders, risk executives, authorizing officials, chief information officers, senior agency information security officers, and senior agency officials for privacy;
- Individuals responsible for conducting security or privacy assessments and for monitoring information systems, for example, 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.

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 information system-related security and privacy risk. This includes an organization-wide view of risk management and the application of the RMF steps; the relationship between security and privacy and the integration of ~~information security requirements~~privacy into the ~~system development life cycle; (iii)~~RMF; the establishment of a system-of-interest and system ~~boundaries; and (iv)~~elements; the allocation of controls to ~~organizational information~~ organizations and systems as system-specific, hybrid, and common controls; the security and privacy posture of systems and organizations; and consideration related to supply chain risk management.
- Chapter Three describes the tasks required to implement the steps in the RMF including: organization-level and information system-level preparation; categorization of information and information systems; control selection, tailoring, and implementation; assessment of control effectiveness; information system and common control authorization; the ongoing monitoring of controls; and maintaining awareness of the security ~~controls~~and privacy posture of information systems and the organization.
- Supporting Appendices provide information and guidance for the application of the RMF including: references; glossary of terms; acronyms; roles and responsibilities; summary of tasks; ~~(vi) security authorization of information systems; (vii) monitoring the security state of information systems; (viii) operational scenarios; and (ix) security controls in external environments~~information system and common control authorizations; and SDLC considerations affecting RMF implementation.

CHAPTER TWO

THE FUNDAMENTALS

MANAGING ~~INFORMATION~~ SYSTEM-RELATED SECURITY AND PRIVACY RISKS IN ORGANIZATIONS

This chapter describes the basic concepts associated with managing information 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~~, core missions and business~~ in SDLC processes~~, and supporting organizational information systems; (ii) integrating information security requirements into system development life cycle processes; (iii) establishing practical and meaningful boundaries for organizational information systems~~; and security ~~controls to organizational information systems as system-specific, hybrid, or common controls~~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.

2.1 ~~INTEGRATED~~ ORGANIZATION-WIDE RISK MANAGEMENT

Managing information 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 is a holistic activity that is fully integrated into every aspect of the organization including the mission and business planning activities, the enterprise architecture, the SDLC processes, and the systems engineering activities that are integral to those system life cycle processes. Security and privacy requirements, key elements of risk management, are clearly articulated and communicated to each organizational entity to help ensure mission and business success. Figure 1 illustrates a three-level (tiered) approach to risk management that addresses risk-related concerns at the *organization* level, the *mission/business process* level, and the *information system* or *system component* level.[16]

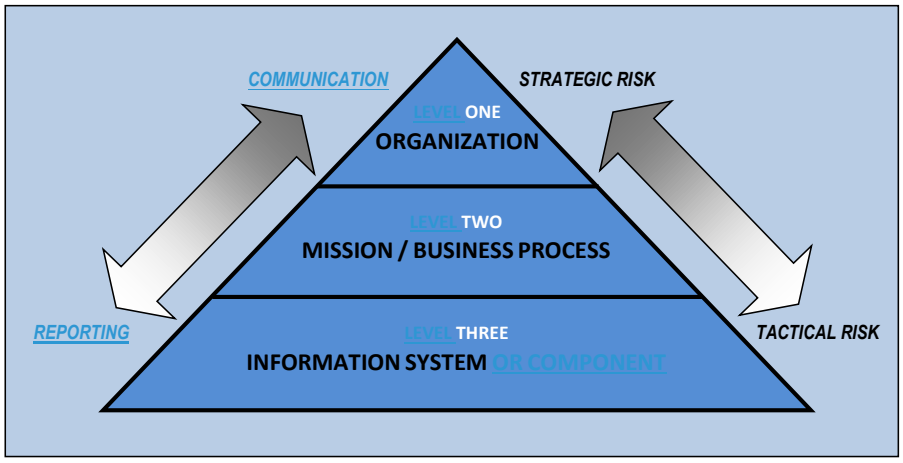


FIGURE 1: ~~TIERED~~ORGANIZATION-WIDE RISK MANAGEMENT APPROACH

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 beyond managing the security and privacy risks associated with operating or using specific systems and includes activities that are essential to managing security and privacy risks appropriately throughout the organization. Decisions about how to manage security and privacy risks at the system level cannot be made in isolation. Such decisions are closely linked to decisions regarding the mission/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);[17] 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 can include assigning key roles and responsibilities for risk management processes; establishing a risk management strategy and organizational risk tolerance; identifying the missions, business functions, and mission/business processes the information system is intended to support; identifying key stakeholders (internal and external to the organization) that have an interest in the information system; identifying and prioritizing assets (including information assets); understanding threats to information systems organizations, and individuals; conducting risk assessments; identifying and prioritizing key stakeholder protection needs and security and privacy requirements;[18] determining systems-of-interest (i.e., authorization boundaries); defining information systems in terms of the enterprise architecture; developing the security and privacy architectures that include controls suitable for inheritance by organizational systems; identifying, aligning, and deconflicting requirements; and allocating both security and privacy requirements to information systems and environments in which those systems operate.

In contrast to the Level 1 and 2 activities that prepare the organization for the execution of the RMF, Level 3 addresses risk from an *information system* perspective and is guided and informed by the risk decisions at the organization and mission/business process levels. The risk decisions at Levels 1 and 2 impact the selection and implementation of controls at the system level. System security and privacy requirements are satisfied by the selection and implementation of controls from NIST Special Publication 800-53. These controls are allocated to the system as system-specific, hybrid, or common controls in accordance with the enterprise architecture, security or privacy architecture, and any tailored control baselines or overlays that have been developed by the organization.[19] In certain cases, when appropriate, controls are allocated to individual system

[17] *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. The Common Approach to Federal Enterprise Architecture and Federal Enterprise Architecture Framework provide guidance for implementing enterprise architectures.

[18] 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.

[19] Controls can be allocated at all three ~~tiers~~levels in the risk management hierarchy. For example, common controls may be allocated at the organization, mission/business process, or information system level. ~~See Section 2.4 for~~

elements. Controls are *traceable* 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 that the requirements are fully addressed during system design, development, ~~Security controls can be provided by the organization or by an external provider. Relationships with external providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain arrangements.[20]~~

~~Risk management tasks begin early in the system development life cycle and are important in shaping the security capabilities of the information system. If these tasks are not adequately performed during the initiation, development, and acquisition phases of the system development life cycle, the tasks will, by necessity, be undertaken later in the life cycle and be more costly to implement. In either situation, all tasks are completed prior to placing the information system into operation or continuing its operation to ensure that: (i) information system-related security risks are being adequately addressed on an ongoing basis; and (ii) the authorizing official explicitly understands and accepts the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of a defined set of security controls and the current security state of the information system.~~

~~The Risk Management Framework (RMF), illustrated in Figure 2-2, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The RMF operates primarily at Tier 3 in the~~ implementation, and maintenance. Each level of the risk management hierarchy ~~but can also have interactions at Tiers 1 and 2 (e.g., providing feedback from ongoing authorization decisions to the risk executive [function], dissemination of updated threat and risk information to authorizing officials and information system owners). The RMF steps include:~~is a beneficiary of a successful RMF execution—reinforcing the iterative nature of the risk management process where risk is framed, assessed, responded to, and monitored at various levels of an organization.

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.

HOLISTIC APPLICATION OF RISK MANAGEMENT CONCEPTS

Successful security, privacy, and risk management programs depend on a holistic application of the concepts to help 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 assets, individuals, other organizations, and the Nation.

~~additional information on security control allocation.~~

~~[20] Appendix I provides additional guidance regarding external service providers and the provision of security controls in external environments.~~

The RMF provides a structured and flexible process that integrates security and privacy activities into the SDLC. The RMF operates at all levels in the risk management hierarchy illustrated in Figure 1. 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** to execute the RMF from an organization-level and a system-level perspective by considering a variety of inputs and carrying out specific activities 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 a security impact analysis.
- **Select** an initial set of controls for the system and tailor the controls as needed based on an organizational assessment of risk and local conditions.
- **Implement** the controls and describe how the controls are employed within the system and its environment of operation.
- **Assess** the 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 satisfying security and privacy policy.
- **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation ~~resulting from the operation of the information system and the decision that this risk~~ is acceptable.
- **Monitor** the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

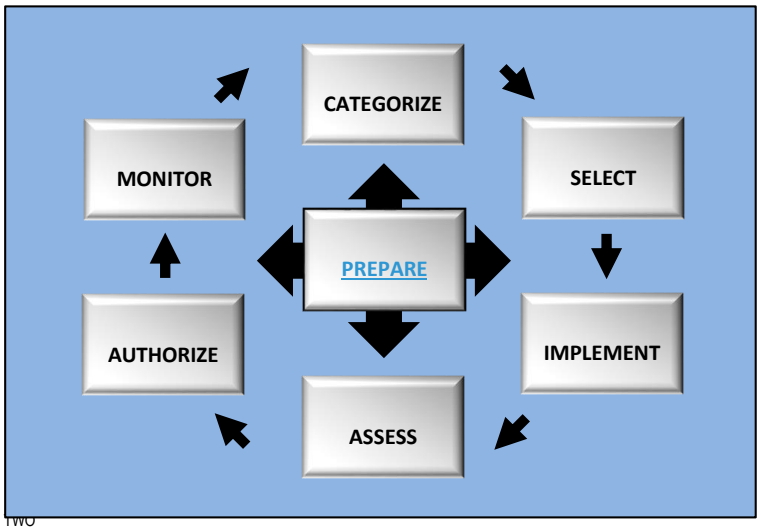


FIGURE 2: RISK MANAGEMENT FRAMEWORK

Figure 2 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, Vol. 1.

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 SDLC as part of the continuous monitoring step, events may dictate nonsequential execution.

FLEXIBILITY IN RMF IMPLEMENTATION

Organizations have significant flexibility in developing their security and privacy programs—including the *selection* of baseline 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 missions, business functions, and operating environments of the organization.

Although the risk management approach in Figure 1 is conveyed as hierarchical, project and organization dynamics are typically more complex. The ~~organizational~~risk management approach selected by an organization may ~~be at one or more points~~vary on a continuum from top-down command to decentralized consensus among peers. ~~For risk management to succeed at~~However, in all ~~levels of the organization, the organization must have~~cases, organizations use a consistent approach that is applied to risk management processes ~~and procedures. Organizational~~across the enterprise from the *organization* level to the *information 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 that will be needed to accomplish the tasks.

~~his chapter describes the process of applying the Risk Management Framework (RMF) to federal information systems.[21] The process includes a set of well-defined risk-related tasks that are to be carried out by selected individuals or groups within well-defined organizational roles (e.g., risk executive [function], authorizing official, authorizing official designated representative, chief information officer, senior information security officer, , information security architect,~~

~~[21] The process for managing risk described in this publication can be tailored to meet the needs of many communities of interest within the federal government including, for example, the Civil, Defense, and Intelligence Communities. Tailoring provides flexibility in applying the risk management concepts associated with the RMF in a manner that is most suitable for the organizations and the information systems involved.~~

information owner/steward, information system owner, common control provider, information system security officer, and security control assessor).[22] 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 and consistent with core missions/business processes, 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 system development life cycle processes, taking into account appropriate dependencies. This helps to ensure that organizations are effectively integrating the process of managing information system-related security risks with system development life cycle processes.

Each RMF task description includes the individual or group with the primary responsibility for carrying out the task, the supporting roles that may be called upon to assist in completing the task, the system development life cycle phase most closely associated with the task, supplemental guidance to help explain how the task is executed, and appropriate references for publications or Web sites with information related to the task.[23] To summarize the key risk management-related activities to be carried out by the organization, a milestone checkpoint is provided for each step in the RMF. The milestone checkpoints contain a series of questions for the organization to help ensure that important activities described in a particular step in the RMF have been completed prior to proceeding to the next step.

The process of implementing the RMF tasks (i.e., the order and manner in which the tasks occur and are executed, the names of primary/supporting roles, the names and format of artifacts) may vary from organization to organization. The RMF tasks can be 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 tasks and revisiting tasks. For example, the results from security control assessments can trigger remediation actions on the part of an information system owner, which can in turn require the reassessment of selected controls. Monitoring the security controls in an information system can also generate a potential cycle of tracking changes to the system and its environment of operation, conducting security impact analyses, taking remediation actions, reassessing security controls, and reporting the security status of the system. There may also be other opportunities to diverge from the sequential nature of the tasks when it is more efficient or cost-effective to do so. For example, while the security control assessment tasks are listed after the security control implementation tasks, some organizations may choose to begin the assessment of certain controls as soon as they are implemented but prior to the complete implementation of all controls described in the security plan. This may result in the organization assessing the physical and environmental protection controls within a facility prior to assessing the security controls employed in the hardware and software components of the information system (which may be implemented at a later time). Regardless of the task ordering, the last step before an information system is placed into operation is the explicit acceptance of risk by the authorizing official.

[22] Appendix D describes the roles and responsibilities of key participants involved in an organization's risk management process.

[23] A reference is included in the RMF task list if: (i) the reference is generally applicable to both national security systems and nonnational security systems; (ii) the reference for nonnational security systems has an equivalent or supporting reference for national security systems; or (iii) the reference relates to specific national security community guidance regarding the implementation of certain NIST standards or guidelines.

RMF steps and associated tasks can be applied to both new development and legacy information systems. For legacy systems, organizations can use RMF Steps 1 through 3 to confirm that the security categorization has been completed and is appropriate and that the requisite security controls have been selected and allocated. Applying the first three steps in the RMF to legacy systems can be viewed as a *gap analysis* to determine if the necessary and sufficient security controls (i.e., system-specific, hybrid, and common controls) have been appropriately selected and allocated. Security control weaknesses and deficiencies, if discovered, can be subsequently addressed in RMF Steps 3 through 6 similar to new development systems. If no weaknesses or deficiencies are discovered in the security controls during the gap analysis and there is a current security authorization in effect, the organization can move directly to the last step in the RMF, continuous monitoring. If a current security authorization is not in place, the organization continues with RMF Steps 4 through 6.

The security categorization process influences the level of effort expended when implementing the RMF tasks. Information systems supporting the most critical and/or sensitive operations and assets within the organization as indicated by the security categorization, demand the greatest level of attention and effort to ensure that appropriate information security and risk mitigation are achieved. Most RMF tasks can be carried out by external providers with appropriate contractual agreements or other arrangements in place (see Appendix I). A summary table of the RMF tasks is provided in Appendix E.

APPLICATION OF THE RISK MANAGEMENT FRAMEWORK

The Risk Management Framework and associated RMF tasks apply to both ***information system owners*** and ***common control providers***. In addition to supporting the authorization of information systems, the RMF tasks support the selection, development, implementation, assessment, authorization, and ongoing monitoring of common controls inherited by organizational information systems. Execution of the RMF tasks by common control providers, both internal and external to the organization, helps to ensure that the security capabilities provided by the common controls can be inherited by information system owners with a degree of assurance appropriate for their information protection needs. This approach recognizes the importance of security control effectiveness within information systems and the infrastructure supporting those systems.

Since the tasks in the RMF are described in a ***sequential*** manner, organizations may choose to deviate from that sequential structure in order to be consistent with their established management and system development life cycle processes or to achieve more cost-effective and efficient solutions with regard to the execution of the tasks. Regardless of the task ordering, the last step before an information system is placed into operation is the explicit acceptance of risk by the authorizing official. Organizations may also execute certain RMF tasks in an iterative manner or in different phases of the system development life cycle. For example, security control assessments may be carried out during system development, system implementation, and system operation/maintenance (as part of continuous monitoring).

Organizations may also choose to expend a greater ***level of effort*** on certain RMF tasks and commit fewer resources to other tasks based on the level of maturity of selected processes and activities within the organization. Since the RMF is life cycle-based, there will be a need to revisit various tasks over time depending on how the organization manages changes to the information systems and the environments in which those systems operate. Managing information security-related risks for an information system is viewed as part of a larger organization-wide risk management activity carried out by senior leaders. The RMF must simultaneously provide a disciplined and structured approach to mitigating risks from the operation and use of organizational information systems and the flexibility and agility to support the core missions and business operations of the organization in highly dynamic environments of operation.

Successful security, privacy, and risk management programs depend on a holistic application of the concepts to help ensure that there is a high degree of transparency and traceability of every programmatic element. 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 assets, individuals, other organizations, and the Nation.

2.2 INFORMATION SECURITY AND PRIVACY UNDER THE RMF

Commented [A2]: In SP 800-37, Rev. 1, Section 2.2 covered the System Development Life Cycle. This has been moved in the IPD of Rev. 2 to Appendix G.

OMB CIRCULAR A-130: INTEGRATION OF INFORMATION SECURITY AND PRIVACY

In 2016, OMB revised Circular A-130, the circular establishing general policy for the planning, budgeting, governance, acquisition, and management of federal information, personnel, equipment, funds, information technology resources, and supporting infrastructure and services. The circular addresses responsibilities for protecting federal information resources and managing personally identifiable information (PII). In establishing requirements for information security programs and privacy programs, the circular emphasizes the need for both programs to collaborate on shared objectives:

> *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.*

Circular A-130 requires organizations to implement the RMF that is described in this guideline. With the 2016 revision to the circular, OMB also requires organizations to integrate privacy into the RMF process:

> *The RMF provides a disciplined and structured process that integrates information security, privacy, and risk management activities into the SDLC. This Circular requires organizations to use the RMF to manage privacy risks beyond those that are typically included under the "confidentiality" objective of the term "information security." While many privacy risks relate to the unauthorized access or disclosure of PII, privacy risks may also result from other activities, including the creation, collection, use, and retention of PII; the inadequate quality or integrity of PII; and the lack of appropriate notice, transparency, or participation.*

This section of the guideline describes the *relationship* between information security programs and privacy programs under the RMF. However, subject to OMB policy, organizations retain the flexibility to undertake the integration of privacy into the RMF in the most effective manner, considering the organization's mission and circumstances.

Executing the RMF requires close collaboration between information security programs and privacy programs. While information security programs and privacy programs have different objectives, those objectives are overlapping and complementary. Information security programs are responsible for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized system activity or behavior) in order to provide confidentiality, integrity, and availability. Privacy programs are responsible for ensuring compliance with applicable privacy requirements and for managing the risks to individuals associated with the creation, collection, use, processing, storage, maintenance,

dissemination, disclosure, or disposal (collectively referred to as "processing") of PII.[24] When preparing to execute the steps of the RMF, organizations consider how to best promote and institutionalize collaboration between the two programs to ensure that the objectives of both disciplines are met at every step of the process.

When an information system processes PII, the organizations' information security program and privacy program have a shared responsibility for managing the risks to individuals that may arise from unauthorized system activity or behavior. This requires the two programs to collaborate when selecting, implementing, assessing, and monitoring security controls. However, while information security programs and privacy programs have complementary objectives with respect to managing the confidentiality, integrity, and availability of PII, protecting individuals' privacy cannot be achieved solely by securing PII. Not all privacy risks arise from unauthorized system activity or behavior, such as unauthorized access or disclosure of PII; some privacy risks may result from authorized activity that is beyond the scope of information security. For example, privacy programs are responsible for managing the risks to individuals that may result from the creation, collection, use, and retention of PII; the inadequate quality or integrity of PII; and the lack of appropriate notice, transparency, or participation. Therefore, to ensure compliance with applicable privacy requirements and to manage privacy risks from authorized and unauthorized processing of PII, organizations' privacy programs also select, implement, assess, and monitor privacy controls.

OMB Circular A-130 defines a *privacy control* as an administrative, technical, or physical safeguard employed within an agency to ensure compliance with applicable privacy requirements and to manage privacy risks. A privacy control is different from a *security control*, which the Circular defines as a safeguard or countermeasure prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. Due to the shared responsibility that organizations' information security programs and privacy programs have to manage the risks to individuals arising from unauthorized system activity or behavior, controls that achieve both security and privacy objectives are both privacy and security controls. This guideline refers to controls that achieve both sets of objectives as "controls." Organizations' information security programs and privacy programs are responsible for control selection, implementation, and assessment. When this guideline uses the descriptors "privacy" and "security" with the term *control*, it is referring to those controls in circumstances where they are selected, implemented, and assessed for particular objectives.

Figure 3 illustrates how organizations manage privacy risks under the RMF, including both the risks that arise from authorized processing of PII and the risks that arise from unauthorized system activity or behavior. The only step that does not consider the risks that arise from the authorized processing of PII is the *Categorize* step (with the exception of the system description task). Information and information systems are categorized based on a security risk assessment, which informs whether the impact on organizational operations and assets, individuals, other organizations, and the Nation from a loss of confidentiality, integrity, and availability is low, moderate, or high. While the *Categorize* step only considers the risks that arise from unauthorized system activity and behavior, when an information system processes PII, this necessarily includes

[24] Privacy programs may also choose to consider the risks to individuals that may arise from their interactions with information systems, where the processing of PII may be less impactful than the effect the system has on individuals' behavior or activities. Such effects would constitute risks to individual autonomy and organizations may need to take steps to manage those risks in addition to information security and privacy risks.

risks to individuals. As such, categorizing information and information systems is a collaborative effort between the organizations' information security program and privacy program.

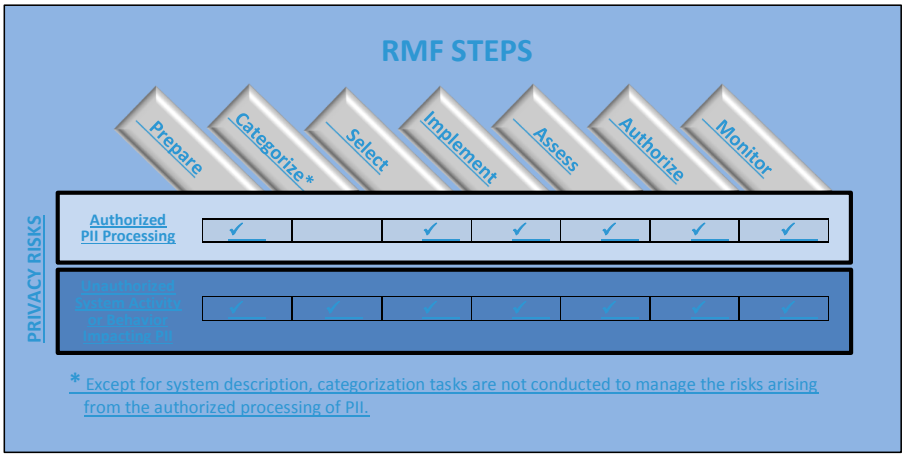


FIGURE 3: PRIVACY INTEGRATION INTO THE RISK MANAGEMENT FRAMEWORK

2.3 SYSTEM AND SYSTEM ELEMENTS

This publication uses the statutory definition of information system for RMF execution. However, it is important to describe information systems in the context of the SDLC and how security and privacy capabilities are implemented within the basic components of those systems. Therefore, organizations executing the RMF take a broad view of the entire life cycle of information system development to provide a contextual relationship and linkage to architectural and engineering concepts that allow security and privacy issues to be addressed throughout the life cycle and at the appropriate level of detail to help ensure that such capabilities are achieved. ISO/IEC/IEEE 15288 provides an architectural and engineering view of an information system and the entities that the system interacts with in its environment of operation.

Similar to how federal law defines information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, ISO/IEC/IEEE 15288 defines a *system* as a set of interacting elements organized to achieve one or more stated purposes. And, just as the information resources that comprise an information system include resources such as personnel, equipment, funds, and information technology, system elements include technology or machine elements, human elements, and physical or environmental elements. Each of the *system elements*[25] within the system fulfills specified requirements and may be implemented via hardware, software, or firmware;[26] physical structures or devices; or people, processes, policies, and procedures. Individual system elements or a combination of system elements may satisfy stated system requirements. Interconnections between system elements allow those elements to interact as necessary to produce a capability as

Commented [A3]: In SP 800-37, Rev. 1, Section 2.2 covered Information System Boundaries. Note that NIST is no longer using the terms system boundary and authorization boundary interchangeably; only the term authorization boundary is now used.

A new RMF Task, Authorization Boundary (Prepare Step, System-Level Task 4), has been added to the IPD of Rev. 2. Additional information on authorization boundaries will also be available in a pending version of NIST SP 800-18, Rev. 2.

[25] *System elements* are included in the set of information resources defined in 44 U.S.C. Sec. 3502 as information and related resources, such as personnel, equipment, funds, and information technology.
[26] The term *system component* refers to a *system element* that is implemented via hardware, software, or firmware.

specified by the system requirements. Finally, every system operates within an environment that influences the system and its operation.

The term *system-of-interest* defines the set of system elements, system element interconnections, and the environment in which the system operates. The system-of-interest also determines the authorization boundary[27] for the execution of the RMF. The system-of-interest may be supported by one or more *enabling systems* that provide support during the system life cycle. The enabling systems are not within the authorization boundary of 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 are also outside of the authorization boundary and may be the beneficiaries of services provided by the system-of-interest or simply have some general interaction. Figure 4 illustrates the conceptual view of the system-of-interest and the relationships among systems, systems elements, and the environment of operation.

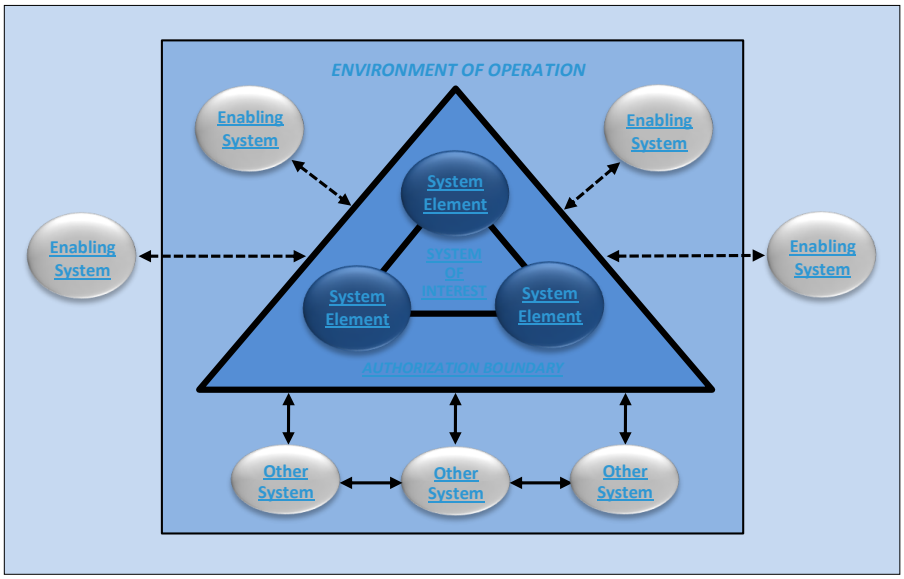


FIGURE 4: CONCEPTUAL VIEW OF THE SYSTEM-OF-INTEREST

The RMF, including the authorization process, is applied to an authorization boundary that can be conceptualized as a system-of-interest, not individual system elements. Organizations can employ "component-level" assessments for system elements[28] and can take advantage of the assessment results generated during that process to support risk-based decision making for the system.

[27] NIST Special Publication 800-18 provides guidance on *system boundary* determination. In this publication, system boundary is synonymous with *authorization boundary* (as determined by the system-of-interest) which includes all components of an information system to be authorized for operation or authorized for use by an authorizing official.
[28] For example, the evaluation program established under ISO/IEC 15408 (Common Criteria) provides independent component-level assessments for IT products.

RISK MANAGEMENT IN THE SYSTEM DEVELOPMENT LIFE CYCLE

Risk management activities begin early in the SDLC and continue throughout the life cycle. These activities are important in helping to shape the security and privacy capabilities of the system; ensuring that the necessary controls are implemented and that the security and privacy risks are being adequately addressed on an ongoing basis; and ensuring that the authorizing officials understand the current security and privacy posture of the system in order to accept the risk to organizational operations and assets, individuals, other organizations, and the Nation.

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 or privacy capability for an information 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 and common characteristics). Controls are *allocated* to a system or an organization consistent with the organization's enterprise architecture and security or privacy architecture.[29] This activity is carried out as an organization-wide activity that involves authorizing officials, system owners, common control providers, the chief information officer, the senior accountable official for risk management or risk executive (function); the senior agency information security officer, the senior agency official for privacy, system security or privacy officers, the enterprise architect, and security and privacy architects.[30]

Organizations are encouraged to identify and implement common controls that can support multiple information 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 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 controls from NIST Special Publication 800-53 are appropriate for specific types of allocations. ~~The organization has significant flexibility in deciding which families of security controls or specific controls from selected families in NIST Special Publication 800-53 are appropriate for the different types of allocations. Since the security control allocation process involves the assignment and provision of security capabilities derived from security controls, the organization ensures that there is effective communication among all entities either receiving or providing such capabilities. This communication includes, for example, ensuring that common control authorization results and continuous monitoring information are readily available to those organizational entities inheriting common controls, and that any changes to common controls are effectively communicated to those affected by such~~

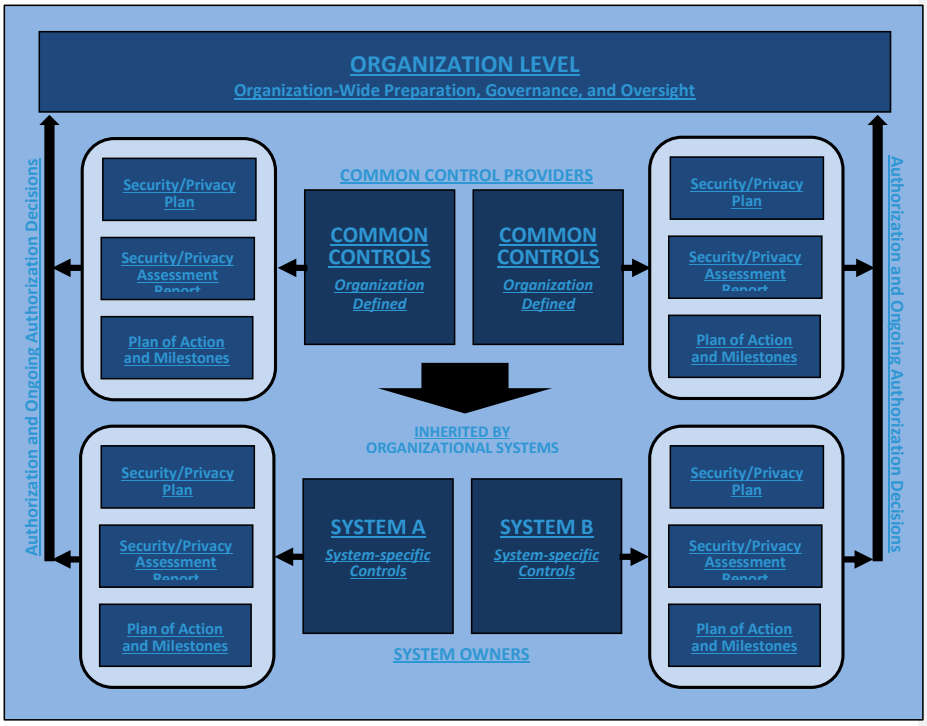
[29] *Allocation* is the process an organization employs to determine whether controls are system-specific, hybrid, or common and to assign the controls to the specific system elements (i.e., machine, physical, or human components) responsible for providing a security or privacy capability.

[30] Security control allocation also occurs during the SDLC process as part of *requirements engineering*. NIST Special Publication 800-160, Volume 1, describes the systems security engineering activities associated with system life cycle processes to achieve trustworthy, secure components, systems, and services.

~~changes.~~[31]

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 always be necessary to allocate every control in the tailored baseline to each system element. Organizations can save resources by allocating controls to only those system elements that require such protection.

Figure 5 illustrates control allocation using the RMF to produce risk-related information for the senior leaders and executives (including authorizing officials) in the organization on the security and privacy posture of organizational systems and the mission/business processes supported by those systems.[32]



~~[31] Communication regarding the security status of common (inherited) controls is essential irrespective of whether the common control provider is internal or external to the organization. Appendix I provides guidance for organizations relying on security controls in external environments including the types of contractual agreements and arrangements that are necessary to ensure appropriate security-relevant information is conveyed to the organization from external providers.~~

[32] When authorizing officials issue a *common control authorization* (see Appendix F), they are addressing the security and privacy risks related to organizational systems that can potentially inherit those controls. Authorizing officials that issue an *authorization to operate* or *authorization to use* also consider the security and privacy risks associated with the actual inheritance of the common controls identified by the organization for the system they are authorizing. Thus, the common control authorization addresses the risk in providing (i.e., provisioning) common controls to system owners and the system authorization addresses the risk in receiving or using the inherited controls.

FIGURE 5: ORGANIZATION-WIDE CONTROL ALLOCATION

2.5 SECURITY AND PRIVACY POSTURE

The purpose of the RMF is to ensure that information systems, organizations, and individuals are adequately protected; and that authorizing officials have the information needed to make credible, risk-based decisions regarding the operation or use of those systems or the inheritance of common controls. A key aspect of risk-based decision making for authorizing officials is understanding the security and privacy posture of organizational information systems and the common controls that are designated for inheritance by those systems. The security and privacy posture represents the status of the information systems and information resources (i.e., personnel, equipment, funds, and information technology) within an organization based on information assurance resources (e.g., people, hardware, software, policies, procedures) and the capabilities in place to manage the defense of the organization; comply with applicable privacy requirements and manage privacy risks; and react as the situation changes.

The security and privacy posture of the information systems and the organization is determined on an ongoing basis by assessing and continuously monitoring system-specific, hybrid, and common controls.[33] The control assessments and monitoring activities provide evidence that the controls selected by the organization are implemented correctly, operating as intended, and satisfying the security and privacy requirements in response to mission or business requirements, laws, executive orders, regulations, directives, policies, or standards. Authorizing officials use the security and privacy posture to determine if the risk to organizational operations and assets, individuals, other organizations, or the Nation are acceptable based on the organization's risk management strategy and organizational risk tolerance.[34]

2.6 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.[35] Relationships providers can be established in a variety of ways, for example, through joint ventures, business partnerships, various types of formal agreements (e.g., contracts, interagency agreements, lines of business arrangements, licensing agreements), or outsourcing arrangements. the growing dependence on component products, systems, and services from external providers and the relationships with the providers, present an increasing amount of risk to an 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—and the processes, procedures, and practices

[33] The assessment and continuous monitoring of controls is part of the organization-wide risk management approach defined in NIST Special Publication 800-39. This holistic and iterative approach to risk management includes *framing* risk, *assessing* risk, *responding* to risk, and *monitoring* risk on an ongoing basis.

[34] See RMF *Prepare-Organization Level* step, Task 2.

[35] OMB Circular A-130 requires federal agencies to consider supply chain security issues for all resource planning and management activities throughout the SDLC so that risks are appropriately managed.

used to assure the integrity, security, resilience, and quality of the products, systems, 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 and privacy 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 avoided, mitigated, or accepted.

Organizations develop a supply chain risk management (SCRM) policy, which is a critical vehicle for guiding and informing SCRM activities. Driven by applicable laws, executive orders, directives, policies, and regulations, the SCRM policy supports applicable organizational policies including acquisition and procurement, information security and privacy, quality, supply chain, and logistics. The policy addresses the goals and objectives established in the organization's strategic plan, specific missions and business functions, and the internal and external customer requirements. It also defines the integration points for SCRM with the risk management and the SDLC processes for the organization.

SCRM policy defines SCRM-related roles and responsibilities within the organization, any dependencies among those roles, and the interaction among the roles. SCRM-related roles specify the responsibilities for procurement, collecting supply chain threat intelligence, conducting risk assessments, identifying and implementing risk-based mitigations, and performing monitoring functions. In order to implement SCRM, organizations establish a coordinated team-based approach (either ad hoc or formal) to assess supply chain risk and manage this risk by using programmatic and technical mitigation techniques. The coordinated team approach enables organizations to conduct a comprehensive analysis of their supply chain, communicate with external partners or stakeholders, and gain broad consensus regarding appropriate resources for SCRM. The SCRM team consists of members with diverse roles and responsibilities for leading and supporting SCRM activities including information technology, risk executive, contracting, information security, mission/business, legal, acquisition and procurement, supply chain and logistics, and other relevant functions. Members of the SCRM team are involved in the various aspects of the SDLC. Collectively, these individuals have an awareness of, and provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems. The SCRM team can be an extension of an organization's existing security and privacy risk management processes or can be included as part of a general organizational risk management team.

FISMA and OMB Circular A-130 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 controls for systems processing, storing, or transmitting federal information are expressed in contracts or other formal agreements. ~~Organizations can require external providers to implement all steps in the~~ The RMF ~~with the exception of the security authorization step, which remains~~ can be effectively used to manage supply chain security risk. The conceptual view of the system-of-interest in Figure 4 can guide and inform security and risk management activities for all elements of the supply chain. Every step in the RMF can be executed by nonfederal entities except for the *Authorize* step—that is, the acceptance of risk is an inherent federal responsibility

for which senior leaders and executives are held accountable.[36] The authorization decision is directly linked to the management of risk related to the acquisition and use of ~~external information system~~component products, systems, and services.~~[37]~~

~~The assurance or confidence that the risk~~ from ~~using~~ external providers.
OMB Circular A-130 also requires organizations 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 both internal and external stakeholders. This includes engaging multiple disciplines in identifying priorities and developing solutions; ensuring that SCRM activities are performed throughout the SDLC; and incorporating SCRM into organizational risk management decisions. SCRM activities 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 are tailored to individual organizational, program, and operational contexts. Tailored plans provide the basis for determining whether a system is "fit for purpose" and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations to focus their resources on the most critical missions and business functions based on mission and business requirements and their risk environment.

The determination that the risk from acquiring component products, systems, or services from external providers is acceptable depends on the ~~trust~~level of assurance[38] that the organization ~~places in the external service provider. In some cases, the~~can gain from the providers. The level of ~~trust~~assurance is based on the ~~amount~~degree of ~~direct~~ control the organization can exert on the external provider regarding the controls needed for the protection of the component product, system, or service and the evidence brought forth by the provider as to the effectiveness of those controls. The degree of control is established by the specific terms and conditions of the contract or service-level agreement ~~with the external service provider and can range from~~. Some organizations have extensive ~~(e.g., negotiating a~~ control through contract vehicles or ~~agreement~~other agreements that specify the security ~~control~~and privacy requirements for the external provider~~) to very~~. Other organizations, in contrast, have rather limited ~~(e.g., using a contract or service-level agreement to obtain~~control because they are purchasing commodity services or commercial ~~telecommunications services). In other cases, the~~off-the-shelf products. The level of ~~trust is~~assurance can also be based on many other factors that convince the organization that the requisite controls have been implemented and that a credible determination of control effectiveness exists. For example, an authorized external ~~information system~~cloud service provided to an organization through a well-established line of business relationship may provide a level of trust in the ~~external~~ service that is within the risk tolerance of thethe organization.

Ultimately, the responsibility for ~~adequately mitigating unacceptable~~ responding to risks arising from the use of ~~external information system~~component products, systems, and services from external providers remains with the organization and the authorizing official. Organizations

[36] While *authorization* (i.e., the acceptance of risk) is an inherent federal responsibility, it is a foundational concept that can be used by senior executives in nonfederal organizations at all levels in the supply chain to manage risk.
[37] ~~If the external provider is a federal agency, the provider can conduct all RMF tasks to include the information system authorization (see Appendix H).~~

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

require that an appropriate *chain of trust* be established with external ~~service~~ 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 certain level of ~~confidence~~trust such that each participant in the consumer-provider relationship in the supply chain provides adequate protection for component products, systems, and services provided to the organization. The chain of trust can be complicated due to the number of entities participating 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 ~~even more complicated and~~ difficult to manage. Depending on the ~~nature~~type of ~~the~~component product, system, or service, it may not be prudent for the organization to place significant trust in the external provider. This is not necessarily due to any inherent untrustworthiness on the provider's part, but due to the intrinsic level of risk in the component product, system, or service. Where sufficient degree of trust cannot be established, the organization can implement mitigating controls, accept additional risk, or forgo using the product, system, or service.[39]

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

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

A USE CASE FOR THE RMF

Organizations can use the RMF to help protect Controlled Unclassified Information (CUI) when such information resides in nonfederal information systems. The CUI security requirements in NIST Special Publication 800-171 are an output from the RMF *Prepare-System Level* step, Task 8. The CUI requirements can be referenced by federal agencies in contracts or other formal agreements with nonfederal organizations. The requirements can be satisfied by the selection (see RMF *Select* step, Task 1 and Task 2) and implementation (see RMF *Implement* step, Task 1) of organization-defined security controls. Following implementation, the requirements (and the associated controls) can be assessed* for effectiveness (see RMF *Assess* step, Task 3) with the findings from the assessments providing evidence for risk-based decisions by senior leaders and executives (see RMF *Authorize* step, Task 4). The security posture of the nonfederal system can be monitored on an ongoing basis to ensure that the CUI requirements continue to be satisfied (see RMF *Monitor* step, Task 2). Security plans are reflected in the RMF *Select* step, Task 4. Plans of Action are reflected in RMF *Assess* step, Task 6.

The RMF provides a structured, yet flexible process that can be used by both consumer and producer entities to any degree of rigor or formality in ensuring that CUI is adequately protected when outside of federal control.

* NIST Special Publication 800-171A provides guidance on assessing CUI requirements in nonfederal systems.

CHAPTER THREE

THE PROCESS

EXECUTING THE RISK MANAGEMENT FRAMEWORK TASKS

This chapter describes the process of applying the RMF to organizations and information systems. The process includes a set of risk-based tasks that are to be carried out by selected individuals or groups within defined organizational roles.[40] Many risk management roles defined in this publication have counterpart roles defined in the SDLC process. Organizations align their risk management roles with similar or complementary roles defined for the SDLC whenever possible, and consistent with missions and business functions. RMF tasks are executed concurrently with or as part of the SDLC 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.[41] Each task contains a set of potential inputs needed to execute the task and a set of potential outputs generated from task execution.[42] In addition, each task describes the phase of the SDLC where task execution takes place and the risk management roles and responsibilities associated with the task. Finally, there is a discussion section and references to provide organizations with information on how to effectively execute each task.

The process of implementing RMF tasks may vary from organization to organization. The tasks are applied at appropriate phases in the SDLC. 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, 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 controls can generate a cycle of tracking changes to the system and its environment of operation; assessing the security or privacy impact; taking remediation actions, reassessing controls, and reporting the security and privacy posture of the system.

There may 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 control assessment tasks are listed after the 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 implemented 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 associated tasks can be applied to new development systems and existing systems. For new and existing systems, organizations ensure that the designated tasks have been

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

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

[42] 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.

completed to prepare for the execution of the RMF. For existing systems, organizations confirm that the security categorization and (for systems processing PII) a privacy risk assessment have been completed and are appropriate; and that the needed controls have been selected, tailored, and implemented.

Applying these steps to existing systems can serve as a gap analysis to determine if security and privacy risks have been managed. Any 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 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.

THE IMPORTANCE OF WELL-DEFINED SECURITY AND PRIVACY REQUIREMENTS

The RMF is a system life cycle-based process that can be effectively used to ensure that security and privacy requirements are satisfied for information systems or organizations. Defining clear, consistent, and unambiguous security and privacy requirements is a critically important element in the successful execution of the RMF. The requirements should be defined early in the system development life cycle in collaboration with senior leaders and executives and be integrated in the organization's acquisition and procurement processes. For example, organizations can use a life cycle-based systems engineering process (i.e., NIST Special Publication 800-160, Volume 1) to define an initial set of security and privacy requirements, which in turn, can be used to select a set of controls* to satisfy the requirements. The requirements or the controls can be stated in the Request for Proposal or other contractual agreement when organizations acquire systems, system components, or services.

The NIST Cybersecurity Framework (i.e., Core, Profiles) can also be used to identify, align, and deconflict security requirements and to subsequently drive the selection of security controls for an organization. Some organizations may choose to use the Cybersecurity Framework in concert with the NIST Systems Security Engineering publications—identifying, aligning, and deconflicting requirements across a sector, an industry, or an organization, and subsequently employing a life cycle-based systems engineering approach to further refine the requirements and to obtain trustworthy secure solutions to help protect the organization's operations, assets, individuals.

* See Section 2.2 for specific guidance on privacy control selection and managing privacy risk.

ORGANIZATION AND SYSTEM PREPARATION

Preparation can achieve effective, efficient, and cost-effective execution of risk management processes. The primary objectives of *organization level* and *system level* preparation are to:

- Facilitate better communication between senior leaders and executives in the C-suite and system owners and operators—
  - aligning organizational priorities with resource allocation and prioritization at the system level; and
  - conveying acceptable limits regarding the selection and implementation of controls within the established organizational risk tolerance.
- Promote organization-wide identification of common controls and the development of organization-wide tailored control baselines, to reduce the workload on individual system owners and the cost of system development and protection.
- 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.
- Identify, prioritize, and focus resources on high-value assets and high-impact systems that require increased levels of protection.
- Facilitate system readiness for system-specific tasks.

These objectives, if achieved, significantly reduce the information technology footprint and the 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.

3.1 PREPARE[43]

Purpose

The purpose of the ***Prepare*** step is to carry out essential activities at the organization, mission and business process, and information system levels of the enterprise to help prepare the organization to manage its security and privacy risks using the *Risk Management Framework*.

PREPARE TASKS—ORGANIZATION LEVEL[44]

Table 1 provides a summary of tasks and expected outcomes for the RMF *Prepare* step at the *organization* level. A mapping of Cybersecurity Framework categories, subcategories, and constructs is also provided.

TABLE 1: PREPARE TASKS AND OUTCOMES—ORGANIZATION LEVEL

Tasks	Outcomes
TASK 1 RISK MANAGEMENT ROLES	• Individuals are identified and assigned key roles for executing the Risk Management Framework. [Cybersecurity Framework: **ID.AM-6**; **ID.GV-2**]
TASK 2 RISK MANAGEMENT STRATEGY	• A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [Cybersecurity Framework: **ID.RM**]
TASK 3 RISK ASSESSMENT—ORGANIZATION	• An organization-wide risk assessment is completed or an existing risk assessment is updated. [Cybersecurity Framework: **ID.RA**]
TASK 4 ORGANIZATION-WIDE TAILORED CONTROL BASELINES AND PROFILES (OPTIONAL)	• Tailored control baselines for organization-wide use are established and made available. [Cybersecurity Framework: **Profile**]
TASK 5 COMMON CONTROL IDENTIFICATION	• Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK 6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	• A prioritization of organizational systems with the same impact level is conducted. [Cybersecurity Framework: **ID.AM-5**]
TASK 7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	• An organization-wide strategy for monitoring control effectiveness is developed and implemented. [Cybersecurity Framework: **DE.CM**]

Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.

[43] The *Prepare* step is not intended to require new or additional activities for security and privacy programs. Rather, it emphasizes the importance of having comprehensive, enterprise-wide governance and the appropriate resources in place to enable the execution of cost-effective and consistent risk management processes across the organization.

[44] For ease of use, the preparatory activities are grouped into organization-level preparation and information system-level preparation.

RISK MANAGEMENT ROLES

Task 1 Identify and assign individuals to specific roles associated with security and privacy risk management.

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

Potential Outputs: Documented Risk Management Framework role assignments.

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

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

Discussion: The roles and responsibilities of key participants in risk management processes are described in Appendix D. The roles and responsibilities may include personnel that are internal or external to the organization, as appropriate. 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 one individual filling multiple roles. In either situation, the basic risk management functions remain the same. 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 the two disciplines may require different expertise, and in some circumstances, the priorities may be competing.

References: NIST Special Publication 800-160, Volume 1 (Human Resource Management Process); NIST Special Publication 800-181; NIST Cybersecurity Framework (Core [Identify Function]).

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: Risk management strategy and statement of risk tolerance.

Primary Responsibility: Head of Agency.

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

Discussion: 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 for 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 expression of organizational risk tolerance; acceptable risk assessment methodologies and risk response strategies; a process for consistently evaluating the security, privacy, and supply chain risks across the organization with respect to risk tolerance; and approaches for monitoring risk over time. As organizations define and implement risk management strategies, policies, procedures, and processes, it is important that they include SCRM considerations. The risk management

strategy for security and privacy links security and privacy programs with the management control systems established in the organization's Enterprise Risk Management strategy.[45]

References: NIST Special Publication 800-30; NIST Special Publication 800-39 (Organization Level); NIST Special Publication 800-160, Volume 1 (Risk Management, Decision Management, Quality Assurance, Quality Management, Project Assessment and Control Processes); NIST Special Publication 800-161; NIST Interagency Report 8062; NIST Cybersecurity Framework (Core [Identify Function]).

RISK ASSESSMENT—ORGANIZATION

Task 3 Assess organization-wide security and privacy risk and update the results on an ongoing basis.

Potential Inputs: Risk management strategy; current threat information; system-level risk assessment results; information sharing agreements/memoranda of understanding.

Potential Outputs: Organization-level risk assessment results.

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

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative.

Discussion: Risk assessment at the organizational level is based primarily on aggregated information from system-level risk assessment results, continuous monitoring, and any strategic risk considerations relevant to the organization. The organization considers the totality of risk derived from the operation and use of its information systems and from information exchange and connections with other internally and externally owned systems. For example, the organization may review risk related to its enterprise architecture and information systems of varying impact levels residing on the same network and whether higher impact systems are sufficiently segregated from lower impact systems.

References: NIST Special Publication 800-30; NIST Special Publication 800-39 (Organization Level, Mission/Business Process Level); NIST Special Publication 800-161; NIST Interagency Report 8062.

ORGANIZATION-WIDE TAILORED CONTROL BASELINES AND PROFILES (OPTIONAL)

Task 4 Establish, document, and publish organization-wide tailored control baselines and/or 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 control baselines; organization- and system-level risk assessment results; NIST Special Publication 800-53 control baselines.

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

Primary Responsibility: Mission or Business Owner; Senior Accountable Official for Risk Management or Risk Executive (Function).

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Discussion: To address the organizational need for specialized sets of controls, tailored control baselines may be developed for organization-wide use.[46] An organization-wide tailored baseline provides a fully specified set of controls, control enhancements, and supplemental guidance derived from established

[45] OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," (2016).

[46] Tailored control baselines may also be referred to as *overlays*. Thus, an organization-wide tailored control 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.

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, Volume 1. 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, for example, situations when the organization has specific security and privacy risks, has specific mission or business needs, or plans to operate in environments that are not addressed in the initial baselines.

Tailored baselines complement the initial NIST Special Publication 800-53 control baselines by providing an opportunity to add or eliminate controls to accommodate organizational requirements while continuing to protect information in a way that is commensurate with risk. Organizations can use tailored baselines to customize 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 specific communities of interest and can also extend the supplemental guidance where necessary. Organization-wide tailored baselines may be more stringent or less stringent than the baselines identified in NIST Special Publication 800-53 and are applied to multiple systems. Tailored baselines may be mandated for use by certain laws, executive orders, directives, regulations, policies, or standards. In some 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 (or overlays) have been developed by communities of interest for cloud and shared systems, services, and applications; industrial control systems; national security systems; weapons and space-based systems; high-value assets; mobile device management; federal public key infrastructure; and privacy risks.

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 organization-level view of these considerations and can serve as inputs to a Framework profile. The resulting prioritized list of cybersecurity outcomes developed at the organization and mission/business process levels can be helpful in facilitating consistent, risk-based decisions at the system level during the execution of the RMF steps. Profiles, the precursor to control selection in the Cybersecurity Framework, can also be used to guide and inform the development of the tailored control baselines described above.

References: NIST Special Publication 800-53; NIST Special Publication 800-160, Volume 1 (Business or Mission Analysis and Stakeholder Needs and Requirements Definition Processes); NIST Cybersecurity Framework (Core, Profiles).

COMMON CONTROL IDENTIFICATION

Commented [A4]: Formerly in Select, Task 2-1

Task 5 Identify, document, 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; organization- and system-level risk assessment results.

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

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

Supporting Roles: Mission or Business Owner; Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Common Control Provider; System Owner.

Discussion: Common controls are controls that can be inherited by one or more information systems. Common controls can include controls from any NIST Special Publication 800-53 control family, for example, physical and environmental protection controls, system boundary and monitoring controls, personnel security controls, policies and procedures, acquisition controls, account and identity management controls, audit log and accountability controls, or complaint management controls for receiving privacy-related inquiries from the public. Organizations identify and select the set of common controls and allocate those controls to the organizational entities designated as common control providers. Common controls may differ based upon a variety of factors, such as hosting location, system architecture, and the 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, department, or agency level; bureau or subcomponent level; or individual program level. Organizations may establish one or more lists of common controls that can be inherited by the systems in the organization.

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 organization 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 information 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 controls designated as common controls. Common control providers may also be system owners when the common controls are resident within an information system. Organizations select senior officials or executives to serve as authorizing officials for common controls. The senior agency official for privacy is responsible for designating common privacy controls and for documenting them in the organization's privacy program plan. 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 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 security and privacy assessment reports; producing a plan of action and milestones for common controls determined to have unacceptable 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 and 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 6 Prioritize organizational systems with the same impact level.

Potential Inputs: System categorization information for organizational systems; system descriptions; organization- and system-level risk assessment results.

Potential Outputs: Organizational systems prioritized into low, moderate, and high impact sub-categories.

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

Supporting Roles: Senior Agency Information Security Officer; Senior Agency Official for Privacy; Mission or Business Owner; System Owner; Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative.

Discussion: This task is carried out *only* after organizational systems have been categorized (see RMF *Categorize* step, Task 1). This task requires organizations to apply the "high water mark" concept to each of their information systems categorized in accordance with FIPS Publication 199. The application of the high-water mark concept results in systems designated as low impact, moderate impact, or high impact. Organizations desiring additional granularity in their 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 control selection and the tailoring of control baselines when responding to identified risks.[47] Impact-level prioritization can also be used to determine those systems that are critical to organizational missions and business operations (also known 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 level of the organization and are based on information system categorization data reported by individual system owners.

References: FIPS Publication 199; NIST Special Publication 800-30; NIST Special Publication 800-39 (Organization and System Levels); NIST Special Publication 800-59; NIST Special Publication 800-60, Volume 1; NIST Special Publication 800-60, Volume 2; NIST Special Publication 800-160, Volume 1 (System Requirements Definition Process); CNSS Instruction 1253; NIST Cybersecurity Framework (Core [Identify Function]).

CONTINUOUS MONITORING STRATEGY—ORGANIZATION

Task 7 Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.

Potential Inputs: Risk management strategy; organization- and system-level risk assessment results; organizational security and privacy policies.

Potential Outputs: An implemented organizational continuous monitoring strategy.

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

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

Discussion: An important aspect of risk management is the ability to monitor the effectiveness of controls implemented within or inherited by information systems on an ongoing basis. An effective organization-wide continuous monitoring strategy is essential to efficiently and cost-effectively carrying out such monitoring. 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 postures of their information systems over time and to maintain the initial system or common control authorizations. This includes the potential for changing missions/business functions, stakeholders, technologies, vulnerabilities, threats, risks, and suppliers of systems, components, or services.

[47] Organizations can also use this task in conjunction with the optional RMF *Prepare*-Organization Level step, Task 4, to develop organization-wide tailored baselines for the more granular impact designations, for example, organization-wide tailored baselines for low-moderate systems and high-moderate systems.

The organizational continuous monitoring strategy addresses monitoring requirements at the organization, mission/business process, and information system levels. The continuous monitoring strategy also identifies the minimum frequency of monitoring for implemented controls across the organization and defines the organizational control assessment approach. The continuous monitoring strategy may also define security and privacy reporting requirements including recipients of the reports.[48] The criteria for determining the minimum frequency with which controls are to be monitored post implementation, is established in collaboration with selected organizational officials including, for example, the senior accountable official for risk management or risk executive (function); senior agency information security officer; senior agency official for privacy; chief information officer; system owners; common control providers; and authorizing officials or their designated representatives. An organizational risk assessment can 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 controls using automated tools and supporting databases facilitates near real-time risk management for information systems, and supports ongoing authorization and more efficient use of resources. The senior accountable official for risk management or the risk executive (function) approves the continuous monitoring strategy including the minimum frequency with which controls are to be monitored.

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

PREPARE TASKS—SYSTEM LEVEL

Table 2 provides a summary of tasks and expected outcomes for the RMF *Prepare* step at the *system* level. A mapping of Cybersecurity Framework categories, subcategories, and constructs is also provided.

TABLE 2: PREPARE TASKS AND OUTCOMES—SYSTEM LEVEL

Tasks	Outcomes
TASK 1 MISSION OR BUSINESS FOCUS	• Missions, business functions, and mission/business processes that the system is intended to support are identified. [Cybersecurity Framework: **Profile**; **Implementation Tiers**; **ID.BE**]
TASK 2 ORGANIZATIONAL STAKEHOLDERS	• The stakeholders having an interest in the system are identified. [Cybersecurity Framework: **ID.AM**; **ID.BE**]
TASK 3 ASSET IDENTIFICATION	• Stakeholder assets are identified and prioritized. [Cybersecurity Framework: **ID.AM**]
TASK 4 AUTHORIZATION BOUNDARY	• The authorization boundary (i.e., system-of-interest) is determined.
TASK 5 INFORMATION TYPES	• The types of information processed, stored, and transmitted by the system are identified. [Cybersecurity Framework: **ID.AM-5**]
TASK 6 INFORMATION LIFE CYCLE	• For systems that process PII, the information life cycle is identified.
TASK 7 RISK ASSESSMENT—SYSTEM	• A system-level risk assessment is completed or an existing risk assessment is updated. [Cybersecurity Framework: **ID.RA**]

[48] For greater efficiency, the information security continuous monitoring (ISCM) and privacy continuous monitoring (PCM) strategies may be consolidated into a single unified continuous monitoring strategy. Similarly, the ISCM and PCM programs may also be consolidated into a single unified continuous monitoring program.

Tasks	Outcomes
TASK 8 PROTECTION NEEDS—SECURITY AND PRIVACY REQUIREMENTS	• Protection needs and security and privacy requirements are defined and prioritized. [Cybersecurity Framework: **ID.GV; PR.IP**]
TASK 9 ENTERPRISE ARCHITECTURE	• The placement of the system within the enterprise architecture is determined.
TASK 10 SYSTEM REGISTRATION	• The system is registered for purposes of management, accountability, coordination, and oversight. [Cybersecurity Framework: **ID.GV**]

Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.

MISSION OR BUSINESS FOCUS

Task 1 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: Mission or Business Owner.

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

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

Discussion: Organizational missions and business functions influence the design and development of the mission or 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 associated security and privacy architectures. 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 Publication 800-39 (Organization and Mission/Business Process Levels); NIST Special Publication 800-64; NIST Special Publication 800-160, Volume 1 (Business or Mission Analysis, Portfolio Management, and Project Planning Processes); NIST Cybersecurity Framework (Core [Identify Function]); NIST Interagency Report 8179 (Criticality Analysis Process B).

ORGANIZATIONAL STAKEHOLDERS

Task 2 Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.

Potential Inputs: Organizational mission statement; information specifying the missions, business functions, and mission/business processes that the system will support; other mission/business process information; organizational security and privacy policies and procedures; organizational charts; information about individuals or groups (internal and external) that have an interest in and decision-making responsibility for the system.

Potential Outputs: List of system stakeholders.

Primary Responsibility: System Owner.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Mission or Business Owner; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

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

Discussion: Stakeholders include individuals, organizations, or representatives that have an interest in the system across the entire system life cycle—for design, development, implementation, delivery, operation, and sustainment of the information 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 information system. For example, this may occur during the development, operation, and maintenance 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 of considerations related to the supply chain.

References: NIST Special Publication 800-39 (Organization Level); NIST Special Publication 800-64; NIST Special Publication 800-160, Volume 1 (Stakeholder Needs and Requirements Definition and Portfolio Management Processes); NIST Special Publication 800-161; NIST Cybersecurity Framework (Core [Identify Function]).

ASSET IDENTIFICATION

Task 3 Identify assets that require protection.

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

Potential Outputs: Set of assets to be protected.

Primary Responsibility: System Owner.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Mission or Business Owner; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

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

Discussion: Assets are the tangible and intangible items that are of value to achievement of organizational mission or business objectives. Tangible assets are physical in nature and include the physical elements of the system's operational environment (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 assets include the information needed to carry out the missions or business functions, to deliver services, and for system management and operation; classified information and controlled unclassified information; and all forms of documentation associated with the information system. Intangible assets can also include the image or reputation of an organization, as well as the privacy interests of the individuals whose information will be processed by the system. The organization defines the scope of stakeholder assets to be considered for protection. Assets that require protection are identified based on stakeholder concerns and the contexts in which the assets are used. This includes the missions or business functions of the organization; the other systems that interact with the system; and stakeholders whose assets are utilized by the mission or business functions or by the system.

References: NIST Special Publication 800-39 (Organization Level); NIST Special Publication 800-64; NIST Special Publication 800-160, Volume 1 (Stakeholder Needs and Requirements Definition Process);

NIST Interagency Report 8179 (Criticality Analysis Process C); NIST Cybersecurity Framework (Core [Identify Function]); NARA CUI Registry.

AUTHORIZATION BOUNDARY

Task 4 Determine the authorization boundary of the system.

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

Potential Outputs: Documented authorization boundary.

Primary Responsibility: System Owner.

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Enterprise Architect.

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

Discussion: Authorization boundaries establish the scope of protection for information systems (i.e., what the organization agrees to protect under its management control or within the scope of its responsibilities). Authorization boundaries are determined by authorizing officials with input from the system owner based on mission, management, or budgetary responsibility. Clear delineation of authorization boundaries is important for accountability and for security categorization, especially in situations where lower-impact systems are connected to higher-impact systems. Each system consists of a set of interacting elements (i.e., information resources)[49] organized to achieve one or more stated purposes and to support the organization's missions and business processes. Each system element is implemented to fulfill specified stakeholder requirements including security and privacy requirements. System elements include human elements, technology/machine elements, and physical/environmental elements.

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 (see Figure 4). For systems processing PII, it is essential that privacy and security programs collaborate to develop a common understanding of the authorization boundary. Privacy risks arise from the processing of PII, which may occur outside of what the security program typically considers the authorization 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 the authorization boundary.

References: NIST Special Publication 800-18; NIST Special Publication 800-39 (System Level); NIST Special Publication 800-47; NIST Special Publication 800-64; NIST Special Publication 800-160, Volume 1 (System Requirements Definition Process); NIST Cybersecurity Framework (Core [Identify Function]).

INFORMATION TYPES

Task 5 Identify the types of information to be processed, stored, and transmitted by the system.

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

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

Primary Responsibility: System Owner; Information Owner or Steward.

Supporting Role: Mission or Business Owner; System Security or Privacy Officer.

[49] *System elements* are implemented via hardware, software, or firmware; physical structures or devices; or people, processes, and procedures. The term *system component* is used to indicate those system elements that are implemented specifically via hardware, software, and firmware.

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

Discussion: 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 information system and a precondition for determining the security categorization. The National Archives and Records Administration (NARA) has defined a set of information types as part of its Controlled Unclassified Information (CUI) program. Organizations may define additional information types needed to support organizational missions, business functions, and mission/business processes that are not defined in the CUI Registry or in NIST Special Publication 800-60, Volume 2.

References: NIST Special Publication 800-39 (System Level); NIST Special Publication 800-60, Volume 1; NIST Special Publication 800-60, Volume 2; NIST Special Publication 800-122; NIST Cybersecurity Framework (Core [Identify Function]); NARA CUI Registry.

INFORMATION LIFE CYCLE

Task 6 For systems that process PII, identify and understand all parts of 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 how PII is being processed throughout its life cycle by the system.

Primary Responsibility: Senior Agency Official for Privacy; System Owner; Information Owner or Steward.

Supporting Roles: Chief Information Officer; Mission or Business Owner.

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

Discussion: The information life cycle for PII includes the creation, collection, use, processing, storage, dissemination, maintenance, disclosure, or disposal of (i.e., collectively "processing") PII. An information system may need to process PII in whole or in part of its life cycle to achieve the organization's missions or business functions. Identifying and understanding all parts of the information life cycle helps inform the organization's privacy risk assessment and subsequent selection and implementation of controls.

Identifying the life cycle of PII by using tools such as a data map enables organizations to understand how PII is being processed so that organizations can better assess where privacy risks could arise and controls could be applied most effectively. It is important for organizations to consider the appropriate delineation of the authorization boundary and the system's interaction with other systems because the way PII enters and leaves the system can significantly affect the privacy risk assessment. The components of the system are identified with sufficient granularity to support a privacy risk assessment.

References: NIST Interagency Report 8062.

RISK ASSESSMENT (SYSTEM)

Task 7 Conduct a system-level risk assessment and update the risk assessment on an ongoing basis.

Potential Inputs: Assets to be protected; information specifying the missions, business functions, and mission/business processes the system will support; business impact analyses or criticality analyses; information about system stakeholders; information about other systems that interact with the system; threat information; data map; system design documentation; risk management strategy; organization-level risk assessment results.

Potential Outputs: Risk assessment report.

Primary Responsibility: System Owner; System Privacy Officer.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Authorizing Official or Authorizing Official Designated Representative; Mission or Business Owner; Information Owner or Steward; System Security Officer.

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

Discussion: Assessment of security risk includes identification of threat sources[50] and threat events affecting assets, whether and how the assets are vulnerable to the threats, the likelihood that an asset vulnerability will be exploited by a threat, and the impact (or consequence) of loss of the assets. As a key part of the risk assessment, assets are prioritized based on the adverse impact or consequence of asset loss. The meaning of loss is defined for each asset type 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. Interpretations of information 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 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 protection needs and security requirements.

Privacy risk assessments are conducted to determine the likelihood that a given operation the system is taking when processing PII could create an adverse effect on individuals—and the potential impact on individuals.[51] Privacy risk assessments are influenced by contextual factors. Contextual factors can include, but are not limited to, the sensitivity level of the PII, including specific elements or in aggregate; the types of organizations using or interacting with the system and individuals' perceptions about the organizations with respect to privacy; individuals' understanding about the nature and purpose of the processing; and individuals' privacy interests. technological expertise or demographic characteristics that influence their understanding or behavior. The privacy risks to individuals may affect individuals' decisions to engage with the system thereby impacting mission or business objectives, or may create legal liability, reputational risks, or other types of risks for the organization. Impacts to the organization are not privacy risks. However, these impacts can guide and inform organizational decision-making and influence prioritization and resource allocation for risk response. Section 2.2 provides information on the overlapping areas in security and privacy risk assessments, which may present opportunities for collaboration.

Risk assessments are conducted throughout the SDLC and support various RMF steps. Risk assessment results are used to 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 method of reporting results.

References: FIPS Publication 199; FIPS Publication 200; NIST Special Publication 800-30; NIST Special Publication 800-39 (Organization Level); NIST Special Publication 800-59; NIST Special Publication 800-60, Volume 1; NIST Special Publication 800-60, Volume 2; NIST Special Publication 800-64; NIST Special Publication 800-160, Volume 1 (Stakeholder Needs and Requirements Definition and Risk Management Processes); NIST Special Publication 800-161 (Assess); NIST Interagency Report 8062; NIST Interagency Report 8179; NIST Cybersecurity Framework (Core [Identify Function]); CNSS Instruction 1253.

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

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

PROTECTION NEEDS—SECURITY AND PRIVACY AND REQUIREMENTS

Task 8 Define the protection needs and security and privacy requirements for the system.

Potential Inputs: System design documentation; organization- and system-level risk assessment results; 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; information about system stakeholders; data map of the information life cycle for PII; information about other systems that interact with the system; supply chain information; threat information; laws, regulations, or policies that apply to the system; risk management strategy.

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

Primary Responsibility: Mission or Business Owner; System Owner; System Privacy Officer; Information Owner or Steward.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; System Security Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

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

Discussion: The protection needs are an expression of the protection capability required in the system. Protection needs include the security characteristics[52] of the system and the security behavior of the system in its intended operational environment and across all system life cycle phases. The protection needs reflect the relative priorities of stakeholders, results of negotiations among stakeholders in response to conflicts, opposing priorities, contradictions, and stated objectives, and thus, are inherently subjective. The protection needs are documented to ensure that the reasoning, assumptions, and constraints associated with those needs are available for future reference. The protection needs are subsequently transformed into security and privacy requirements and associated constraints on system requirements, and the measures needed to validate that all requirements have been met.

Security and privacy requirements[53] constitute a formal, more granular expression of protection needs across all SDLC phases, the associated life cycle processes, and protections for the assets associated with the system. Security and privacy requirements may be obtained from a variety of sources including, for example, laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments. These requirements are a part of the formal expression of required characteristics of the system—encompassing security, privacy, and assurance.[54] 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 manage security requirements and express those requirements in Framework Profiles defined for the organization. For instance, multiple requirements can be aligned and even deconflicted using the *Function-Category-Subcategory* structure of the Framework Core. The Framework *profiles* can then be used to inform the development of tailored security control baselines described in the RMF *Prepare-Organization Level* step, Task 4.

References: NIST Special Publication 800-39 (Organization Level); NIST Special Publication 800-64; NIST Special Publication 800-160, Volume 1 (Stakeholder Needs and Requirements Definition Process);

[52] For example, a fundamental security characteristic is that the system-of-interest exhibits only specified behaviors, interactions, and outcomes.

[53] The term *requirements* can have discrete meanings. For example, legal and policy requirements impose obligations to which organizations must adhere. Security and privacy requirements, however, are derived from the protection needs for the system and those protection needs can derive from legal or policy requirements, mission or business needs, risk assessments, or other sources.

[54] *Assurance* is having confidence about the ability of the system-of-interest to remain trustworthy with respect to security and privacy across all forms of adversity resulting from malicious or non-malicious intent.

NIST Special Publication 800-161 (Multi-Tiered Risk Management); NIST Interagency Report 8179; NIST 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: Security and privacy requirements; organization- and system-level risk assessment results; enterprise architecture information; security architecture information; privacy architecture information; asset information.

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

Primary Responsibility: Mission or Business Owner; Enterprise Architect; Security or Privacy Architect.

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

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

Discussion: System complexity can impact the risk and the ability of organizations to successfully carry out their missions and business functions. An enterprise architecture can help provide greater understanding of information and operational technologies included in the initial design and development of information systems and should be considered a prerequisite for achieving resilience and survivability of those systems in the face of increasingly sophisticated threats. 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 provides an opportunity for organizations to consolidate, standardize, and optimize information and technology assets. An effectively implemented enterprise architecture produces systems that are more transparent and therefore, easier to understand and protect. Enterprise architecture also establishes a clear and unambiguous connection from investments to measurable performance improvements. The placement of a system within the enterprise architecture is important as it provides greater visibility and understanding about the other organizational systems that will be connected to the system and can also be effectively used to establish security domains for increased levels of protection for the system.

The security architecture and the privacy architecture are integral parts of the enterprise architecture. The security and privacy architectures represent the specific parts of the enterprise architecture related to the implementation of security and privacy requirements. The primary purpose of the security and privacy architectures is to ensure that security and privacy requirements are consistently and cost-effectively achieved in organizational systems and are aligned with the risk management strategy. The security and privacy architectures provide a roadmap that facilitates traceability from the strategic goals and objectives of organizations, through protection needs and security and privacy requirements, to specific security and privacy solutions provided by people, processes, and technologies.

References: NIST Special Publication 800-39 (Mission/Business Process Level); NIST Special Publication 800-64; NIST Special Publication 800-160, Volume 1 (System Requirements Definition Process); NIST Cybersecurity Framework (Core [Identify Function]; Profiles); Common Approach to Federal Enterprise Architecture; Federal Enterprise Architecture Framework.

SYSTEM REGISTRATION

Commented [A5]: Previously in Categorize, Task 1-3.

Task 10 Register the system with organizational program/management offices.

Potential Inputs: Organizational policy on system registration; system information.

Potential Outputs: Registered system in accordance with organizational policy.

Primary Responsibility: System Owner.

Supporting Role: Mission or Business Owner; Chief Information Officer; System Security or Privacy Officer.

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

Discussion: System registration, in accordance with organizational policy, serves to inform the governing organization of plans to develop the system or the existence of the system; the key characteristics of the system; and the expected security and privacy implications for the organization due to the ongoing use and operation of the system. System registration provides organizations with an effective management/tracking tool to facilitate incorporation of the system into the enterprise architecture, implementation of protections that are commensurate with risk, and security and privacy posture reporting in accordance with applicable laws, executive orders, directives, regulations, policies, standards, or guidelines. As part of the system registration process, organizations add the system to the organization-wide system inventory. The system registration information is updated with the system categorization and system characterization information upon completion of the *Categorize* step.

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

3.2 CATEGORIZE[55]

Purpose

The purpose of the ***Categorize*** step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.

CATEGORIZE TASKS

Table 3 provides a summary of tasks and expected outcomes for the RMF *Categorize* step. A mapping of Cybersecurity Framework categories, subcategories, and constructs is also provided.

TABLE 3: CATEGORIZE TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 SECURITY CATEGORIZATION	• A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed. [Cybersecurity Framework: **ID.AM-5**] • Security categorization results are documented in the system security and supply chain risk management plans. [Cybersecurity Framework: **Profile**] • 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.
TASK 2 SECURITY CATEGORIZATION REVIEW AND APPROVAL	• The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.
TASK 3 SYSTEM DESCRIPTION	• The characteristics of the system are described and documented. [Cybersecurity Framework: **Profile**]

Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.

SECURITY CATEGORIZATION

Task 1 Categorize the system and document the security categorization results.

Potential Inputs: Risk management strategy; organizational risk tolerance; authorization boundary (i.e., system-of-interest) information; organization- and system-level risk assessment results; information types processed, stored, or transmitted by the system; list of security requirements allocated to the system and to

[55] The RMF *Categorize* step is a precondition for the selection of security controls. However, for privacy, there are other factors considered by organizations that guide and inform the selection of privacy controls. These factors are described in the RMF *Prepare-System Level* step, Task 7.

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.

Commented [A6]: Potential Inputs and Pontential Outputs were added for each task.

Primary Responsibility: System Owner; Information Owner or Steward.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Authorizing Official or Authorizing Official Designated Representative; System Security or Privacy Officer.

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

Discussion: Security categorization determinations consider potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation. The categorization process is carried out by the system owner and the information owner or steward in cooperation and collaboration with senior leaders and executives with mission, business function, or risk management responsibilities. This ensures that individual systems are categorized based on the mission and business objectives of the organization. The system owner and information owner or 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 organizational missions or business functions resulting from the loss of confidentiality, integrity, or availability of information. 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 can be cross-referenced in a privacy plan when the system processes PII.

Commented [A7]: Supplemental Guidance was updated to Discussion throughout.

The security categorization results for the system can be further refined by the organization to facilitate an impact-level prioritization of systems with the same impact level (see RMF *Prepare-Organization Level* step, Task 6). 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 Publication 800-30; NIST Special Publication 800-39 (System Level); NIST Special Publication 800-59; NIST Special Publication 800-60, Volume 1; NIST Special Publication 800-60, Volume 2; NIST Special Publication 800-160, Volume 1 (Stakeholder Needs and Requirements Definition and System Requirements Definition Processes); NIST Interagency Report 8179; CNSS Instruction 1253; NIST Cybersecurity Framework (Core [Identify Function]).

SECURITY CATEGORIZATION REVIEW AND APPROVAL

Task 2 Review and approve the security categorization results and decision.

Potential Inputs: 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; list of high-value assets for the organization.

Potential Outputs: Approval of security categorization for the system.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative; Senior Agency Official for Privacy.[56]

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

[56] This role is active for information systems processing PII.

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

Discussion: For information systems that process PII, the senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review. Security categorization results and decisions are reviewed by the authorizing official or a designated representative to ensure that the security category selected for the information system is consistent with the mission and business functions of the organization and the need to adequately protection those missions and functions. The authorizing official or designated representatives reviews the categorization results and decision from an organization-wide perspective, including how the decision aligns with the other categorization decisions for all other organizational systems. The authorizing official collaborates with the senior agency official for risk management or the risk executive (function) to ensure that the categorization decision for the system is consistent with the risk management strategy for the organization and satisfies any requirements for high-value assets. As part of the approval process, the authorizing official can provide specific guidance to the system owner with respect to any limitations on baseline tailoring activities for the system that occur at the RMF *Select* step, Task 3. If the security categorization decision is not approved, the system owner initiates steps to repeat the categorization process and resubmits the adjusted results to the authorizing official or designated representative. System registration information is subsequently updated with the approved security categorization information (see RMF *Prepare-System Level* step, Task 10).

References: FIPS Publication 199; NIST Special Publication 800-30; NIST Special Publication 800-39 (Organization Level); NIST Special Publication 800-160, Volume 1 (Stakeholder Needs and Requirements Definition Process); CNSS Instruction 1253; NIST Cybersecurity Framework (Core [Identify Function]).

SYSTEM DESCRIPTION

Task 3 Document the characteristics of the system.

Potential Inputs: System design and requirements documentation; authorization 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 or system component inventory; system categorization; information on system use, users, and roles; data map of the information life cycle for PII.

Potential Outputs: Documented system description.

Primary Responsibility: System Owner.

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

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

Discussion: A description of the characteristics of the system is documented in the security and privacy plans, included in attachments to the plans, or referenced in other standard sources for the information generated as part of the SDLC. 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 RMF steps.

Examples of 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; SDLC phase; results of the categorization process and privacy risk assessment; authorization boundary; laws, directives, policies, regulations, or standards affecting individuals' privacy and the security of the system; architectural description of the system including network topology; information types; hardware, firmware, and software components that

are part of the system; hardware, software, and system interfaces (internal and external); information flows 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; maintenance or other relevant agreements; ownership/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. System registration information is updated with the system characterization information (see RMF *Prepare-System Level* step, Task 10).

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

~~**Milestone Checkpoint #1**~~

- ~~Has the organization completed a ***security categorization*** of the information system (informed by the initial risk assessment) including the information to be processed, stored, and transmitted by the system?~~
- ~~Are the results of the security categorization process for the information system consistent with the organization's ***enterprise architecture*** and commitment to ***protecting organizational mission/business processes***?~~
- ~~Do the results of the security categorization process reflect the organization's ***risk management strategy***?~~
- ~~Has the organization adequately described the ***characteristics*** of the information system?~~
- ~~Has the organization ***registered*** the information system for purposes of management, accountability, coordination, and oversight?~~

Commented [A8]: The Milestone Checkpoints at the end of each Step were deleted and replaced with the Outcome Summary Tables before each Step.

3.3 SELECT

Purpose

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

SELECT TASKS

Table 4 provides a summary of tasks and expected outcomes for the RMF *Select* step. A mapping of Cybersecurity Framework categories, subcategories, and constructs is also provided.

TABLE 4: SELECT TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 SECURITY AND PRIVACY REQUIREMENTS ALLOCATION	• Security and privacy requirements are allocated to the system and to the environment in which the system operates. [Cybersecurity Framework: **ID.GV**]
TASK 2 CONTROL SELECTION	• Control baselines necessary to protect the system commensurate with risk are selected. [Cybersecurity Framework: **Profile**] • Controls are assigned as system-specific, hybrid, or common controls. [Cybersecurity Framework: **Profile**; **PR.IP**]
TASK 3 CONTROL TAILORING	• Controls are tailored producing tailored control baselines. [Cybersecurity Framework: **Profile**]
TASK 4 SECURITY AND PRIVACY PLANS	• Security and privacy controls and associated tailoring actions are documented in the security and privacy plans or equivalent documents. [Cybersecurity Framework: **Profile**]
TASK 5 CONTINUOUS MONITORING STRATEGY—SYSTEM	• A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed. [Cybersecurity Framework: **ID.GV**; **DE.CM**]
TASK 6 SECURITY AND PRIVACY PLAN REVIEW AND APPROVAL	• Security and privacy plans reflecting the selection of controls necessary to protect the system commensurate with risk are reviewed and approved by the authorizing official.

Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.

SECURITY AND PRIVACY REQUIREMENTS ALLOCATION

Task 1 Allocate security and privacy requirements to the information system and to the environment in which the system operates.

Potential Inputs: System categorization; organization- and system-level risk assessment results; organizational policy on system registration; documented protection needs and security and privacy requirements; list of common control providers and common controls available for inheritance; system description; system element information; system component inventory; relevant laws, regulations, and policies.

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 Architect; Privacy Architect or System Privacy Officer.

Supporting Roles: Chief Information Officer; Authorizing Official or Authorizing Official Designated Representative; Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner.

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

Discussion: Organizations allocate security and privacy requirements to facilitate the control selection and implementation processes at the organization, information system, and system element (i.e., component) levels. The allocation of security and privacy requirements to the system and to the environment[57] in which the system operates, determines which controls are designated as system-specific, common, and hybrid during the control selection process. Requirements allocation also identifies the specific system elements (i.e., components) to which controls are assigned. The allocation of security and privacy requirements saves resources and facilitates streamlining of the risk management process by ensuring that requirements are not implemented on multiple systems or multiple components within a system when implementation of a common control or a system-level control on a specific component provides the needed protection capability. Common controls satisfy security and privacy requirements allocated to the organization and provide a security and privacy protection capability that is inherited by one or more systems (common controls are identified as part of the RMF *Prepare-Organization Level* step, Task 5). Hybrid controls satisfy security and privacy requirements allocated to the system and to the organization and provide a security and privacy protection capability that is partially inherited by one or more systems. And finally, system-specific controls satisfy security and privacy requirements allocated to the system and provide a security and privacy protection capability only for that system. Security and privacy protection capabilities may also be allocated to specific system components rather than to every component within a system. For example, system-specific controls associated with management of audit logs may be allocated to a log management server and thus need not be implemented on every system component.

References: NIST Special Publication 800-39 (Organization, Mission/Business Process, and System Levels); NIST Special Publication 800-64; NIST Special Publication 800-160, Volume 1 (System Requirements Definition Process); NIST Cybersecurity Framework (Core [Identify Function]; Profiles); Common Approach to Federal Enterprise Architecture; Federal Enterprise Architecture Framework.

CONTROL SELECTION

Task 2 Select the controls for the system.

Potential Inputs: System categorization information; organization- and system-level risk assessment results; 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; risk management strategy; organizational security and privacy policy; federal or organization-approved or mandated baselines or overlays; Cybersecurity Framework profiles.

Potential Outputs: Controls selected for the system.

Primary Responsibility: System Owner; ~~Information Security Architect;~~ Common Control Provider.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; Systems Security or Privacy Engineer; System Security or Privacy Officer.

[57] The environment of operation for an information system refers to the physical surroundings in which the system processes, stores, and transmits information. For example, *security requirements* are allocated to the facilities where the system is located and operates. Those security requirements can be satisfied by the physical security controls in NIST Special Publication 800-53.

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

Discussion: There are two approaches that can be used for the initial selection of controls: a *baseline* control selection approach, or an *organization-generated* control selection approach. The baseline control selection approach uses control baselines, which are pre-defined sets of controls representing broad-based, balanced, information security and privacy programs that serve as a starting point for the protection of information and information systems. Security control baselines are selected based on the system security categorization (see RMF *Categorize* step, Task 1) and the security requirements derived from stakeholder protection needs, laws, executive orders, regulations, policies, directives, instructions, and standards. Privacy controls are selected based on a privacy risk assessment and privacy requirements derived from laws, executive orders, regulations, directives, policies, standards, guidelines, and stakeholder protection needs. Organizations can choose to develop or employ a privacy control baseline to select an initial set of privacy controls. Control baselines are provided in NIST Special Publication 800-53. After the appropriate pre-defined control baseline is selected, organizations tailor the baseline in accordance with the tailoring guidance provided (see RMF *Select* step, Task 3).

The organization-generated control selection approach differs from the baseline control selection approach because the organization does not start with a pre-defined set of controls. Rather, the organization develops a set of security requirements using a life cycle-based systems engineering process (e.g., ISO/IEC/IEEE 15288 and NIST Special Publication 800-160, Volume 1) as described in the RMF *Prepare-System Level* step, Task 8. The *requirements engineering* process generates a specific set of security requirements that can subsequently be used to guide and inform the selection of a set of controls to satisfy the requirements. Similarly, organizations can use the Cybersecurity Framework to develop *framework profiles* as a set of organization-specific security requirements—guiding and informing control selection from NIST Special Publication 800-53. Tailoring at the system level may be required after the organization-generated control selection (see RMF *Select* step, Task 3). In instances where organizations do not use a baseline approach for selecting an initial set of privacy controls, the organizations can select privacy controls as part of an organization-generated control selection approach.

References: FIPS Publication 199; FIPS Publication 200; NIST Special Publication 800-30; NIST Interagency Report 8062; NIST Special Publication 800-53; NIST Special Publication 800-160, Volume 1 (System Requirements Definition, Architecture Definition, and Design Definition Processes); NIST Special Publication 800-161 (Respond and Chapter 3); NIST Interagency Report 8179; CNSS Instruction 1253; NIST Cybersecurity Framework (Core [Identify, Protect, Detect, Respond, Recover Functions]; Profiles).

CONTROL TAILORING

Task 3 Tailor the controls selected for the system.

Potential Inputs: Initial control baselines; organization- and system-level risk assessment results; 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; risk management strategy; organizational security and privacy policy; federal or organization-approved or mandated overlays.

Potential Outputs: List of tailored controls for the system (i.e., tailored control baselines).

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; Systems Security or Privacy Engineer; System Security or Privacy Officer.

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

Discussion: After selecting the applicable control baselines, organizations tailor the controls based on the specific conditions within the organization. Such conditions can include, for example, organizational missions or business functions, threats, privacy risks, type of system, risk tolerance, or the environments in

which the system operates. The tailoring process includes identifying and designating common controls in the control baselines (see RMF *Prepare-Organization Level* step, Task 5); applying scoping considerations to the remaining baseline controls; selecting compensating controls, if needed; assigning specific values to organization-defined control parameters through either assignment or selection statements; supplementing baselines with additional controls; and providing specification information for control implementation.[58] Organizations have flexibility to determine the amount of detail to include in justifications or supporting rationale required for tailoring decisions. For example, the justification or supporting rationale for scoping decisions related to a high-impact system (or high value asset) may necessitate greater specificity than similar decisions for a low-impact system. Such determinations are consistent with organizational missions and business functions; stakeholder needs; and any relevant laws, executive orders, regulations, directives, or policies.

Organizations use risk assessments to inform and guide the tailoring process. 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. Privacy risk assessments, including the contextual factors therein, will also influence tailoring when an information system processes PII.[59] 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 with the acknowledgement and approval of the organization. Organizations may also consider federally or organizationally mandated or approved overlays, tailored baselines, or Cybersecurity Framework Profiles when conducting tailoring (see RMF *Prepare-Organization Level* step, Task 4).

References: FIPS Publication 199; FIPS Publication 200; NIST Special Publication 800-30; NIST Special Publication 800-53; NIST Special Publication 800-160, Volume 1 (System Requirements Definition, Architecture Definition, and Design Definition Processes); NIST Special Publication 800-161 (Respond and Chapter 3); NIST Interagency Report 8179; CNSS Instruction 1253; NIST Cybersecurity Framework (Core [Identify, Protect, Detect, Respond, Recover Functions]; Profiles).

SECURITY AND PRIVACY PLANS

Task 4 Document the security and privacy controls for the system in security and privacy plans.

Potential Inputs: System categorization information; organization- and system-level risk assessment results; 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; risk management strategy; organizational security and privacy policy; list of selected controls for the system.

Potential Outputs: Security and privacy plans for the system.

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; Systems Security or Privacy Engineer; System Security or Privacy Officer.

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

Discussion: Security and privacy plans contain an overview of the security and privacy requirements for the system and the security and privacy controls selected to satisfy the requirements. The security and privacy plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of

[58] The tailoring process is fully described in NIST Special Publication 800-53.
[59] NIST Interagency Report 8062 provides a discussion of context and its function in a privacy risk model.

the control. The security and privacy control documentation describes how system-specific and hybrid controls are implemented and the plans and expectations regarding the functionality ~~or possibly no functionality at all).~~of the system. The description of the planned security and privacy control implementation includes planned inputs, expected behavior, and expected outputs where appropriate, typically for those controls that are implemented in the hardware, software, or firmware components of the system. Common controls (i.e., inherited controls) are also identified in the security and privacy plans. There is no requirement to provide implementation details for inherited common controls. Rather, those details are provided in the security and privacy plans for common control providers and are made available to system owners.

Organizations may develop a single, integrated security and privacy plan or maintain separate plans. In certain situations, organizations may choose to document control selection and tailoring information in documents equivalent to security and privacy plans, for example, in systems engineering or life cycle artifacts or documents. Privacy programs collaborate on the development of the security component of an integrated plan in two principal respects. When controls provide protections with respect to managing the confidentiality, integrity, and availability of PII, privacy programs collaborate to ensure that the plan reflects the appropriate selection of these controls, as well as clearly delineate roles and responsibilities for their implementation and assessment. When organizations have separate security and privacy plans, organizations cross-reference the controls in both plans to help to maintain awareness and accountability. The senior agency official for privacy reviews and approves the privacy plan (or integrated plan) before the plan is provided to the authorizing official or designated representative for review (See RMF *Select* step, Task 6).

Documentation of planned 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 or system elements), use automated support tools, and coordinate across the organization to reduce redundancy and increase the efficiency and cost-effectiveness of control documentation. The documentation also addresses platform dependencies and includes any additional information necessary to describe how the capability required is to be achieved at the level of detail sufficient to support control implementation and assessment. Documentation for control implementations follows best practices for hardware and software development and for systems security and privacy engineering disciplines and is also consistent with established policies and procedures for documenting SDLC activities. In certain situations, security controls can be implemented in ways that create privacy risks. The privacy program supports documentation of privacy risk considerations and the specific implementations intended to mitigate them.

For controls that are mechanism-based, organizations take 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 controls. For certain controls, organizations obtain 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 guide and inform the organizational approach used to plan for and implement controls, documenting the process helps to ensure traceability in meeting the security and privacy requirements.

References: FIPS Publication 199; FIPS Publication 200; NIST Special Publication 800-18; NIST Special Publication 800-30; NIST Special Publication 800-53; NIST Special Publication 800-160, Volume 1 (System Requirements Definition, Architecture Definition, and Design Definition Processes); NIST Special Publication 800-161 (Respond and Chapter 3); NIST Interagency Report 8179; CNSS Instruction 1253; NIST Cybersecurity Framework (Core [Identify, Protect, Detect, Respond, Recover Functions]; Profiles).

CONTINUOUS MONITORING STRATEGY—SYSTEM

Task 5 Develop and implement a system-level strategy for monitoring control effectiveness to supplement the organizational continuous monitoring strategy.

Potential Inputs: Organizational risk management strategy; organizational continuous monitoring strategy; organization- and system-level risk assessment results; 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.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Chief Information Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; Security or Privacy Architect; Systems Security or Privacy Engineer; System Security or Privacy Officer.

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

Discussion: An important aspect of risk management is the ongoing monitoring of controls implemented within or inherited by an information system. An effective continuous monitoring strategy at the system level is developed and implemented in coordination with the organizational continuous monitoring strategy early in the SDLC (i.e., during initial system design or procurement decision). The system-level continuous monitoring strategy supplements the organizational continuous monitoring strategy—that is, the system-level strategy addresses monitoring those controls for which monitoring is not provided as part of the organizational continuous monitoring strategy and implementation for the organization.[60] The system-level continuous monitoring strategy identifies the frequency of monitoring for controls not addressed by the organizational strategy and defines the approach to be employed for assessing those controls. The system-level continuous monitoring strategy, consistent with the organizational strategy, may define how changes to the system are to be monitored; how security and privacy risk assessments are to be conducted; and the security and privacy posture reporting requirements including recipients of the reports. The system-level continuous monitoring strategy can be included in security and privacy plans.

For controls that are not addressed by the organizational continuous monitoring strategy, the criteria for determining the frequency with which controls are monitored post-implementation, 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 or 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. Controls that are volatile (i.e., where the control or the control implementation is most likely to change over time),[61] critical to certain aspects of the protection needs for the organization, or identified in plans of action and milestones, may require more frequent assessment. The approach to control assessments during continuous monitoring may include for example, the detection of the status of system components; analysis of historical and operational data; and the reuse of assessment procedures and assessment results that supported the initial authorization decision.

The authorizing official or designated representative approves the continuous monitoring strategy including the minimum frequency with which each control is to be monitored. The approval of the strategy can be

[60] The PCM strategy includes all of the available privacy controls implemented throughout the organization at all risk management levels (i.e., organization, mission/business process, and information system). The strategy ensures that the controls are effectively monitored on an ongoing basis by assigning an organization-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. If, during the development of a new system, there is a need to create or use a privacy control not included in the PCM strategy, the SAOP is consulted to determine whether it is appropriate for the proposed use case. If there is a decision to implement and start using a new privacy control, the organization's PCM strategy would need to be updated to include the new control with an organization-defined monitoring frequency.

[61] Volatility is most prevalent in those controls implemented in the hardware, software and firmware components of the system. For example, replacing or upgrading an operating system, a database system, application, or a network router may change the security controls provided by the vendor or original equipment manufacturer. Moreover, configuration settings may also require adjustments over time as organizational missions, business functions, threats, risks, and risk tolerance changes.

obtained in conjunction with the security and privacy plan approval. The monitoring of controls begins at the start of the operational phase of the SDLC and continues through the disposal phase.

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

SECURITY AND PRIVACY PLAN REVIEW AND APPROVAL

Task 6 Review and approve the security and privacy plans for the system.

Potential Inputs: Completed system security and privacy plans; organization- and system-level risk assessment results.

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

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative.

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

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

Discussion: The review of the security and privacy plans by the authorizing official or designated representative with support from the senior accountable official for risk management or risk executive (function), chief information officer, senior agency information security officer, and senior agency official for privacy helps determine if the plans are complete, consistent, and satisfy the stated security and privacy requirements for the system. Based on the results of this review and analysis, the authorizing official or designated representative may recommend changes to the security and privacy plans. If the security or privacy plans are unacceptable, the system owner or common control provider makes appropriate changes to the plans. If the 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 SDLC and risk management process. The authorizing official or designated representative, by approving the security and privacy plans, agrees to the set of controls (i.e., system-specific, hybrid, or common controls) and the description of the proposed implementation of the controls to meet the security and privacy requirements for the system and the environment in which the system operates. The approval of the security and privacy plans allows the risk management process to proceed to the next step in the RMF (i.e., the implementation of selected 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 or system components.

References: NIST Special Publication 800-30; NIST Special Publication 800-53; NIST Special Publication 800-160, Volume 1 (System Requirements Definition, Architecture Definition, and Design Definition Processes); CNSS Instruction 1253.

Milestone Checkpoint #2

- Has the organization allocated all security controls to the ***information system*** as system-specific, hybrid, or common controls?
- Has the organization used its ***risk assessment*** (either formal or informal) to inform and guide the security control selection process?
- Has the organization identified ***authorizing officials*** for the information system and all common controls inherited by the system?
- Has the organization ***tailored*** the baseline security controls to ensure that the controls, if implemented, adequately mitigate risks to organizational operations and assets, individuals, other organizations, and the Nation?
- Has the organization addressed ***minimum assurance requirements*** for the security controls employed within and inherited by the information system?

- Has the organization consulted information system owners when ***identifying common controls*** to ensure that the security capability provided by the inherited controls is sufficient to deliver adequate protection?
- Has the organization ***supplemented*** the ***common controls*** with system-specific or hybrid controls when the security control baselines of the common controls are less than those of the information system inheriting the controls?
- Has the organization documented the common controls inherited from ***external providers***?
- Has the organization developed a ***continuous monitoring strategy*** for the information system (including monitoring of security control effectiveness for system-specific, hybrid, and common controls) that reflects the organizational risk management strategy and organizational commitment to protecting critical missions and business functions?
- Have appropriate organizational officials ***approved*** security plans containing system-specific, hybrid, and common controls?

3.4 IMPLEMENT

Purpose

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

IMPLEMENT TASKS

Table 5 provides a summary of tasks and expected outcomes for the RMF *Implement* step. A mapping of Cybersecurity Framework categories, subcategories, and constructs is also provided.

TABLE 5: IMPLEMENT TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 CONTROL IMPLEMENTATION	• Controls specified in the system security and privacy plans are implemented. [Cybersecurity Framework: **PR.IP-1**] • Systems security and privacy engineering methodologies are used to implement the controls specified in the system security and privacy plans. [Cybersecurity Framework: **PR.IP-2**]
TASK 2 BASELINE CONFIGURATION	• The configuration baseline is established. [Cybersecurity Framework: **PR.IP-1**] • The system security and privacy plans are updated based on information obtained during the implementation of the controls. [Cybersecurity Framework: **Profile**]

Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.

CONTROL IMPLEMENTATION

Task 1 Implement the controls in the security and privacy plans.

Potential Inputs: Approved system security and privacy plans; system design documents; organizational security and privacy policies and procedures; enterprise architecture information; security architecture information; 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; organization- and system-level risk assessment results.

Potential Outputs: Implemented controls.

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Information Owner or Steward; Security or Privacy Architect; Systems Security or Privacy Engineer; System Security or Privacy Officer; Enterprise Architect; System Administrator.

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

Discussion: Organizations implement the controls listed in the security and privacy plans. The control implementation is consistent with the organization's enterprise architecture and the associated security and privacy architectures. The security and privacy architectures serve as a resource to guide and inform the allocation of controls to a system or system component. Not all controls need to be allocated to every system component. Controls providing a specific security or privacy capability are only allocated to those system components that require the specific security or privacy capability. The security categorization, the privacy risk assessment, the security and privacy architectures, and the allocation of controls work together to help achieve a suitable balance between security and privacy protections and the mission-based function of the system.

Organizations use best practices when implementing controls, including systems security and privacy engineering methodologies, concepts, and principles. Risk assessments guide and inform decisions regarding the cost, benefit, and risk trade-offs in using different technologies or policies for control implementation. Organizations also ensure that mandatory configuration settings are established and implemented on system components in accordance with federal and organizational policies. When organizations have no direct control over what 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 (e.g., NIST Cryptographic Module Validation Program Testing Laboratories, National Information Assurance Partnership Common Criteria Testing Laboratories). In addition, organizations address, where applicable, assurance requirements when implementing controls. Assurance requirements are directed at the activities that control developers and implementers carry out 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. The assurance requirements address quality of the design, development, and implementation of the controls.[62]

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 implement common controls. System owners can refer to the authorization packages prepared by common control providers when making determinations regarding the adequacy of common controls inherited by their systems. During implementation, it may be determined that common controls previously selected to be inherited by the system do not meet the protection needs of the system. For common controls that do not meet the protection needs of the systems inheriting the controls or when common controls are found to have unacceptable deficiencies, the system owners identify compensating or supplementary controls to be implemented. 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. 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 SDLC facilitates early identification of 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 authorize step to avoid delays or costly repetition of assessments. Assessment results that are subsequently reused in other phases of the SDLC meet the reuse requirements established by the organization.[63]

References: FIPS Publication 200; NIST Special Publication 800-30; NIST Special Publication 800-53; NIST Special Publication 800-53A; NIST Special Publication 800-160, Volume 1 (Implementation, Integration, Verification, and Transition Processes); NIST Special Publication 800-161; NIST Interagency Report 8062; NIST Interagency Report 8179; CNSS Instruction 1253.

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

[63] See the RMF *Assess* step and NIST Special Publication 800-53A for information on assessments and reuse of assessment results.

BASELINE CONFIGURATION

Task 2 Establish the initial configuration baseline for the system by documenting changes to planned control implementation.

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

Supporting Roles: Information Owner or Steward; Security or Privacy Architect; Systems Security or Privacy Engineer; System Security or Privacy Officer; Enterprise Architect; System Administrator.

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

Discussion: Despite the specific control implementation details in the security and privacy plans and the system design documents, it is not always possible to implement controls as planned. Therefore, as control implementations are carried out, the security and privacy plans are updated with as-implemented control implementation details. The updates include revised descriptions of 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 information system including any information technology component (i.e., hardware, software, and firmware) configurations and include configuration settings and other technical implementation details. The configuration baselines are essential to providing 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 posture of the organization and the system.

References: NIST Special Publication 800-53; NIST Special Publication 800-128; NIST Special Publication 800-160, Volume 1 (Implementation, Integration, Verification, and Transition, Configuration Management Processes); CNSS Instruction 1253.

~~**Milestone Checkpoint #3**~~

- ~~Has the organization ***allocated*** security controls as system-specific, hybrid, or common controls consistent with the enterprise architecture and information security architecture?~~
- ~~Has the organization demonstrated the use of sound ***information system and security engineering methodologies*** in integrating information technology products into the information system and in implementing the security controls contained in the security plan?~~
- ~~Has the organization documented how ***common controls*** inherited by organizational information systems have been implemented?~~
- ~~Has the organization documented how ***system-specific*** and ***hybrid*** security controls have been implemented within the information system taking into account specific technologies and platform dependencies?~~
- ~~Has the organization taken into account the ***minimum assurance requirements*** when implementing security controls?~~

3.5 ASSESS

Purpose

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

ASSESS TASKS

Table 6 provides a summary of tasks and expected outcomes for the RMF *Assess* step. A mapping of Cybersecurity Framework categories, subcategories, and constructs is also provided.

TABLE 6: ASSESS TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 ASSESSOR SELECTION	• An assessor or assessment team is selected to conduct the control assessments. • The appropriate level of independence is achieved for the assessor or assessment team selected.
TASK 2 ASSESSMENT PLAN	• Documentation needed to conduct the assessments is provided to the assessor or assessment team. • 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 the level of effort required.
TASK 3 CONTROL ASSESSMENTS	• Control assessments are conducted in accordance with the security and privacy assessment plans. • 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 control assessments is maximized to increase the speed, effectiveness, and efficiency of the assessments.
TASK 4 SECURITY AND PRIVACY ASSESSMENT REPORTS	• Security and privacy assessment reports that provide findings and recommendations are completed.
TASK 5 REMEDIATION ACTIONS	• Remediation actions to address deficiencies in the controls implemented in the system and its environment of operation are taken. • System security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions. [Cybersecurity Framework: **Profile**]
TASK 6 PLAN OF ACTION AND MILESTONES	• A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. [Cybersecurity Framework: **ID.RA-6**]

Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.

ASSESSOR SELECTION

Task 1 Select the appropriate assessor or assessment team for the type of assessment to be conducted.

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

Potential Outputs: Selection of assessor or assessment team responsible for conducting the control assessment.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative; Senior Agency Official for Privacy.

Supporting Roles: Senior Agency Information Security Officer.

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

Discussion: Organizations consider both the technical expertise and level of independence required in selecting control assessors.[64] Organizations ensure that control assessors possess the required skills and technical expertise to develop the assessment plans and to conduct assessments of program management, system-specific, hybrid, and common controls, as appropriate. This includes general knowledge of risk management concepts as well as comprehensive knowledge of and experience with the specific hardware, software, and firmware components implemented. Security control assessments in support of initial and subsequent system, common, and program management authorizations are conducted by independent assessors if the system is categorized as moderate or high impact. An independent assessor is an individual or group capable of conducting an impartial assessment. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with respect to the determination of control effectiveness or the development, operation, or management of the system, common controls, or program management controls.

Independent assessment services can be obtained from 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. The authorizing official or designated representative determines the required level of independence for control assessors based on the results of the security categorization process 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 control assessments be accomplished by individuals that are in the developmental, operational, 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, and senior agency information security officer, to guide and inform the decisions regarding assessor independence in the types of special circumstances described above. For assessment of program management controls, the assessor is independent of the entity that manages and implements the program management controls.

The senior agency official for privacy is responsible for identifying assessment methodologies and metrics to determine if privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks. The senior agency official for privacy is also responsible for conducting assessments of privacy controls and documenting the results of the assessments. At the discretion of the organization, privacy controls may be assessed by an independent assessor. In all cases, however, the senior agency official for privacy is responsible and accountable for the

[64] In accordance with OMB Circular A-130, an independent evaluation of privacy program and practices is not required. However, an organization may choose to employ independent privacy assessments at the organization's discretion.

organization's privacy program, including any privacy functions performed by independent assessors. The senior agency official for privacy is also responsible for providing privacy-related information to the authorizing official.

References: FIPS Publication 199; NIST Special Publication 800-30; NIST Special Publication 800-53A.

ASSESSMENT PLAN

Commented [A9]: Previously Task 4-1, Assessment Preparation

Task 2 Develop, review, and approve plans to assess implemented controls.

Potential Inputs: System security and privacy plans; program management control information; common control documentation; organizational security and privacy program 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: Authorizing Official or Authorizing Official Designated Representative; Control Assessor.

Commented [A10]: Previously was a Supporting Role

Supporting Roles: Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner; Common Control Provider; Information Owner or Steward; System Security or Privacy Officer.

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

Discussion: Security and privacy assessment plans are developed by control assessors based on the implementation information contained in system security and privacy plans, program management control documentation, and common control documentation. Organizations may choose to develop a single, integrated security and privacy assessment plan for the system. An integrated assessment plan clearly delineates roles and responsibilities for control assessment. Assessment plans provide the objectives for control assessments and specific assessment procedures for each control. Assessment plans also reflect 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; program management control assessments; continuous monitoring; and assessments conducted after remediation actions.

Assessment plans are reviewed and approved by the authorizing official or the designated representative of the authorizing official to ensure that the plans are consistent with the security and privacy objectives of the organization; employ procedures, techniques, tools, and automation to support continuous monitoring and near real-time risk management; and are cost-effective. Approved assessment plans establish expectations for the control assessments and the level of effort for the assessment. Approved assessment plans help to ensure that an appropriate level of resources is applied toward determining control effectiveness while providing the necessary level of assurance in making such determinations. 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 and/or assessments results/evidence from the provider.

References: NIST Special Publication 800-53A; NIST Special Publication 800-160, Volume 1 (Verification and Validation Processes); NIST Special Publication 800-161.

CONTROL ASSESSMENTS

Task 3 Assess the controls in accordance with the assessment procedures described in the security and privacy assessment plans.

Potential Inputs: Security and privacy assessment plans; system security and privacy plans; external assessment or audit results (if applicable).

Potential Outputs: Completed control assessments and associated assessment evidence.

Primary Responsibility: Control Assessor.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; System Owner; Common Control Provider; Information Owner or Steward; Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Security or Privacy Officer.

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

Discussion: Control assessments determine the extent to which the selected 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 the organization. The system owner, common control provider, and/or organization rely on the technical skills and expertise of assessors to assess implemented controls using the assessment procedures specified in assessment plans and provide recommendations on how to respond to control deficiencies to reduce or eliminate identified vulnerabilities or unacceptable risks. The senior agency official for privacy serves as the control assessor for the privacy controls and is responsible for conducting an initial assessment of the privacy controls prior to operation, and for assessing the controls periodically thereafter at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.[65] The assessor findings are a factual reporting of whether the controls are operating as intended and whether any deficiencies[66] in the controls are discovered during the assessment.

Control assessments occur as early as practicable in the SDLC, preferably during the development phase. These types of assessments are referred to as developmental testing and evaluation and validate that the controls are implemented correctly and are consistent with the established information security and privacy architectures. Developmental testing and evaluation activities include, for example, design and code reviews, regression testing, and application scanning. Security and privacy deficiencies identified early in the SDLC 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 into agreements or contracts to begin the development phase. The results of control assessments during the SDLC can also be used (consistent with reuse criteria) during the authorization process to avoid unnecessary delays or costly repetition of assessments. Organizations can maximize the use of automation to conduct control assessments to increase the speed, effectiveness, and efficiency of the assessments, and to support continuous monitoring of the security and privacy posture of organizational systems.

Applying and assessing controls throughout the development process may be appropriate for iterative development processes. When iterative development processes such as agile development are employed, an iterative assessment may be conducted as each cycle is completed. A similar process is used for assessing controls in commercial information technology products that are used within the system. Organizations may choose to begin assessing 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., controls that are inherited by the system) are assessed separately (by assessors chosen by common control providers or the organization) and need not be assessed as part of a system-level assessment.

Organizations ensure that assessors have access to the information system and environment of operation where the controls are implemented and to the appropriate documentation, records, artifacts, test results, and other materials needed to assess the controls. This includes situations when the 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

[65] The senior agency official for privacy can delegate the assessment functions, consistent with applicable policies.
[66] Only deficiencies in controls that can be exploited by threat agents are considered vulnerabilities.

as determined by the authorizing official.[67] Security control assessments in support of 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 mandated, facilitates reuse of assessment results to support ongoing authorization and reauthorization, if required.

To make the risk management process more efficient and cost-effective, organizations may choose to establish reasonable and appropriate criteria for reusing assessment results as part of organization-wide assessment policy or in the security and privacy program plans. For example, a recent audit of a system may have produced information about the effectiveness of selected controls. Another opportunity to reuse previous assessment results may come from external programs that test and evaluate security and privacy features of commercial information technology products (e.g., NIST Cryptographic Module Validation Program, Common Criteria Evaluation and Validation Program). If prior assessment results from the system developer are available, the control assessor, under appropriate circumstances, may incorporate those results into the assessment. And finally, assessment results can be reused to support reciprocity, for example, assessment results supporting an authorization to use (see Appendix F). Additional information on assessment result reuse is available in NIST Special Publication 800-53A.

References: NIST Special Publication 800-53A; NIST Special Publication 800-160, Volume 1 (Verification and Validation Processes).

SECURITY AND PRIVACY ASSESSMENT REPORTS

Task 4 Prepare the security and privacy assessment reports documenting the findings and recommendations from the control assessments.

Potential Inputs: Completed control assessments[68] and associated assessment evidence.

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

Primary Responsibility: Control Assessor.

Supporting Roles: System Owner; Common Control Provider; System Security or Privacy Officer.

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

Discussion: The results of the security and privacy control assessments, including recommendations for correcting deficiencies in the implemented controls, are documented in the assessment reports[69] by control assessors. Organizations may choose to develop a single, integrated security and privacy assessment report. Assessment reports are key documents in the system or common control authorization package developed for authorizing officials. The assessment reports include information based on assessor findings, necessary to determine the effectiveness of the controls implemented within or inherited by the information system. Assessment reports are an important factor in a determination of risk to organizational operations and assets, individuals, other organizations, and the Nation by the authorizing official. The format and level of detail provided in assessment reports are appropriate for the type of control assessment conducted, for example, developmental testing and evaluation; independent verification and validation; independent assessments supporting information system or common control authorizations or reauthorizations; self-assessments; assessments after remediation actions; assessments during continuous monitoring; and independent audits or evaluations. The reporting format may also be prescribed by the organization.

[67] In accordance with OMB Circular A-130, an independent evaluation of privacy program and practices is not required. However, an organization may choose to employ independent privacy assessments at the organization's discretion.

[68] A *privacy control assessment* is defined in OMB Circular A-130 as both an assessment and a formal document detailing the process and the outcome of the assessment. In this guideline, a privacy assessment report is identified as a separate output, but it should be considered as part of the privacy control assessment.

[69] If a comparable report meets the requirements of what is to be included in an assessment report, then the comparable report would itself constitute the assessment report.

Control assessment results obtained during the system development lifecycle are documented in an interim report, and included in the final security and privacy assessment reports. Development of interim reports that document assessment results from relevant phases of the SDLC reinforces the concept that assessment reports are evolving documents. Interim reports are used, as appropriate, to inform the final assessment report. Organizations may choose to develop an executive summary from the control assessment findings. The executive summary provides authorizing officials and other interested individuals in the organization with an abbreviated version of the assessment reports that includes a synopsis of the assessment, findings, and the recommendations for addressing deficiencies in the controls.

References: NIST Special Publication 800-53A; NIST Special Publication 800-160, Volume 1 (Verification and Validation Processes).

REMEDIATION ACTIONS

Task 5 Conduct initial remediation actions on the 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 with findings and recommendations; system security and privacy plans; security and privacy assessment plans; organization- and system-level risk assessment results.

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; updated system security and privacy plans including any changes to the control implementations.

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

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; ~~Chief Information Officer;~~ Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner; Information Owner or Steward; Systems Security or Privacy Engineer; System Security or Privacy Officer.

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

Discussion: The security and privacy assessment reports describe deficiencies in the controls implemented within the system or the common controls available for inheritance that could not be resolved during the development of the system or that are discovered post-development. Such control deficiencies may result in security and privacy risks. The findings generated during assessments provide information that facilitates a disciplined and structured approach to responding to those risks in accordance with the organizational risk tolerance and priorities. Findings from a system-level control assessment may necessitate an update to both the system risk assessment and the organizational risk assessment.[70] The updated risk assessment and any inputs from the senior accountable official for risk management or risk executive (function) determines the initial remediation actions and the prioritization of those actions. System owners and common control providers may decide, based on a risk assessment, that certain findings are inconsequential and present no significant security or privacy risk. Such findings are retained in the security and privacy assessment reports and monitored during the monitoring step. The authorizing official is responsible for reviewing and understanding the assessor findings and for accepting the security and privacy risks from operating an information system or the use of common controls. The authorizing official, in consultation with system owners and other organizational officials, may decide that certain findings do, in fact, represent significant, unacceptable risk and require immediate remediation actions.

In all cases, organizations review assessor findings to determine the significance of the findings (i.e., the potential adverse impact on organizational operations and assets, individuals, other organizations, or the

[70] Risk assessments are conducted as needed at the organizational level, mission/business level, and at the system level throughout the SDLC. Risk assessment is specified as part of the RMF *Prepare-Organization Level* step, Task 3 and RMF *Prepare-System Level* step, Task 6.

Nation) and whether the findings warrant any 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 or correcting the deficiencies that pose the greatest risk. If deficiencies in controls are corrected, the assessors reassess the remediated controls. 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 the organization. The assessors update the security and privacy assessment reports with the findings from the reassessment, but do not change the original assessment results. The security and privacy plans are updated based on the findings of the 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 control assessments, the security and privacy plans contain an accurate description of implemented controls, including compensating controls.

Organizations can prepare an addendum to the security and privacy assessment reports that provides system owners and common control providers an opportunity to respond to the initial assessment findings. 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's or common control provider's perspective on the findings, including additional explanatory material, rebutting certain findings, and correcting the record. The addendum does not change or influence the initial assessor findings provided in the reports. Information provided in the addendum is considered by authorizing officials when making risk-based authorization decisions. Organizations implement a process to determine the actions to take regarding the control deficiencies identified during the assessment. This process can help address the vulnerabilities and risks, false positives, and any other factors that provide useful information to authorizing officials regarding the security and privacy posture 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 Publication 800-53A; ~~NIST Special Publication 800-30;~~ NIST Special Publication 800-160, Volume 1 (Verification and Validation Processes).

PLAN OF ACTION AND MILESTONES

Commented [A11]: Moved from the Authorize Step, Task 1.

Task 6 Prepare the plan of action and milestones based on the findings and recommendations of the security and privacy assessment reports excluding any initial remediation actions taken.

Potential Inputs: Updated security and privacy assessment reports; updated system security and privacy plans; organization- and system-level 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.

Supporting Roles: Information Owner or Steward; System Security or Privacy Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

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

Discussion: The plan of action and milestones, prepared for the authorizing official by the system owner or the common control provider, is included as part of the authorization package. It describes the actions that are planned to correct deficiencies in the controls identified during the assessment of the controls and during continuous monitoring. The plan of action and milestones identifies the tasks to be accomplished with a recommendation for completion before or after system authorization; resources required to

accomplish the tasks; milestones established to meet the tasks; and the scheduled completion dates for the milestones and tasks. The plan of action and milestones is reviewed by the authorizing official to ensure there is agreement with the remediation actions planned to correct the identified deficiencies. It is subsequently used to monitor progress in completing the actions. Deficiencies are accepted by the authorizing official as residual risk, or are remediated during the assessment or prior to the submission of the authorization package to the authorizing official. Plan of action and milestones entries are not necessary when deficiencies are accepted by the authorizing official as residual risk. However, security and privacy deficiencies identified during assessment and monitoring are documented in the assessment reports, which can be 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 obtained from control assessments, audits, and continuous monitoring and in accordance with applicable laws, executive orders, directives, policies, regulations, standards, or guidance.

Organizations ~~define a strategy~~ implement a consistent process for developing plans of action and milestones that facilitates a prioritized approach to risk mitigation that is uniform across the organization. A risk assessment guides the prioritization process for items included in the plan of action and milestones. The process ensures that plans of action and milestones are informed by the security categorization of the system and privacy risk assessments; the specific deficiencies in the controls; the criticality of the identified control deficiencies (i.e., the direct or indirect effect that the deficiencies may have on the security and privacy posture of the system, and therefore, on the risk exposure of the organization; or the ability of the organization to perform its mission or business functions); and the organization's proposed risk mitigation approach to address the identified deficiencies in the controls, including, for example, prioritization of risk mitigation actions and allocation of risk mitigation resources.

References: NIST Special Publication 800-30; NIST Special Publication 800-53A; NIST Special Publication 800-160, Volume 1 (Verification and Validation Processes); NIST Interagency Report 8062~~OMB Memorandum 02-01~~.

~~Milestone Checkpoint #4~~

- ~~Has the organization developed a comprehensive ***plan*** to assess the security controls employed within or inherited by the information system?~~
- ~~Was the assessment plan ***reviewed*** and ***approved*** by appropriate organizational officials?~~
- ~~Has the organization considered the appropriate level of assessor ***independence*** for the security control assessment?~~
- ~~Has the organization provided all of the essential supporting ***assessment-related materials*** needed by the assessor(s) to conduct an effective security control assessment?~~
- ~~Has the organization examined opportunities for ***reusing assessment results*** from previous assessments or from other sources?~~
- ~~Did the assessor(s) complete the ***security control assessment*** in accordance with the stated assessment plan?~~
- ~~Did the organization receive the completed ***security assessment report*** with appropriate findings and recommendations from the assessor(s)?~~
- ~~Did the organization take the necessary ***remediation actions*** to address the most important weaknesses and deficiencies in the information system and its environment of operation based on the findings and recommendations in the security assessment report?~~
- ~~Did the assessor ***reassess the remediated controls*** for effectiveness to provide the authorization official with an unbiased, factual security assessment report on the weaknesses or deficiencies in the system?~~
- ~~Did the organization update appropriate ***security plans*** based on the findings and recommendations in the security assessment report and any subsequent changes to the information system and its environment of operation?~~

3.6 AUTHORIZE

Purpose

The purpose of the *Authorize* step is to provide security and privacy 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.

AUTHORIZE TASKS

Table 7 provides a summary of tasks and expected outcomes for the RMF *Authorize* step. A mapping of Cybersecurity Framework categories, subcategories, and constructs is also provided.

TABLE 7: AUTHORIZE TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 AUTHORIZATION PACKAGE	• An authorization package, which may be generated by a security or privacy management tool, is developed for submission to the authorizing official.
TASK 2 RISK ANALYSIS AND DETERMINATION	• A risk determination by the authorizing official that reflects the risk management strategy including risk tolerance, is rendered.
TASK 3 RISK RESPONSE	• Risk responses for determined risks are provided. [Cybersecurity Framework: **ID.RA-6**]
TASK 4 AUTHORIZATION DECISION	• The authorization for the system or the common controls is approved or denied.
TASK 5 AUTHORIZATION REPORTING	• Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.

Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.

AUTHORIZATION PACKAGE

Task 1 Assemble the authorization package and submit the package to the authorizing official for an ~~adjudication~~ authorization decision.

Potential Inputs: System security, privacy, and supply chain risk management plans; 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), which may be generated from a security or privacy management tool[71] for submission to the authorizing official.

[71] 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 to reduce or eliminate hard copy documentation.0

Primary Responsibility: System Owner; Common Control Provider; Senior Agency Official for Privacy.[72]

Supporting Roles: System Security or Privacy Officer; Senior Agency Information Security Officer; Control Assessor.

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

Discussion: Authorization packages[73] include the security and privacy plans, along with the supply chain risk management plan, 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. Organizations maintain version and change control as the information in the authorization package is updated. 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, and can be used for reauthorization actions, if required.

The senior agency official for privacy reviews the authorization package for systems that process PII to ensure compliance with applicable privacy requirements and to manage privacy risks, prior to authorizing officials making risk determination and acceptance decisions.

The information in the authorization package is used by authorizing officials to make informed, risk-based decisions. When controls are provided to an organization by an external provider through contracts, interagency agreements, lines of business arrangements, licensing agreements, or supply chain arrangements, the organization ensures that the information needed to make risk-based decisions is made available by the provider.

The authorization package 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. Organizations can use automated support tools in preparing and managing the content of the authorization package. Such tools provide an effective vehicle for maintaining and updating information for authorizing officials regarding the ongoing security and privacy posture of information systems within the organization.

When an information system is under ongoing authorization, the authorization package is presented to the authorizing official via automated reports in order to provide information to the authorizing official in the most efficient and timely manner possible.[74] Information to be presented to the authorizing official in security and privacy assessment reports is generated in the format and with the frequency determined by the organization using security and privacy information from the information security and privacy continuous monitoring programs.

The security and privacy assessment reports presented to the authorizing official includes security and privacy information regarding implemented system-specific, hybrid, and common controls. The authorizing official uses, whenever practicable, 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 frequency at which the authorization documents are updated is in accordance with the risk management objectives of the organization using automated or manual update processes.[75]

[72] This role is active for information systems processing PII.

[73] If a comparable report meets the requirements of what is to be included in an authorization package, then the comparable report would itself constitute the authorization package.

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

[75] 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.

References: NIST Special Publication 800-18; NIST Special Publication 800-160, Volume 1 (Risk Management Process); NIST Special Publication 800-161 (SCRM Plans).

RISK ANALYSIS AND DETERMINATION

Task 2 Analyze and determine the risk ~~to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.~~ from the operation or use of the system or the provision of common controls.

Potential Inputs: Authorization package; supporting assessment evidence or other documentation as required; information provided by the senior accountable official for risk management or risk executive (function); organizational risk management strategy and risk tolerance; organization- and system-level risk assessment results.

Potential Outputs: Risk determination.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy.

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

Discussion: The authorizing official or designated representative, in collaboration with the senior agency information security officer and the senior agency official for privacy (for information systems processing PII), analyzes the information in the authorization package to verify agreement with and understanding of risk determinations made by the control assessor, system owner, or common control provider, and finalizes the determination of risk. Further discussion with the control assessor, system owner, or common control provider may be necessary to help ensure a thorough understanding of risk by the authorizing official.

Risk assessments are employed, if needed, to provide information[76] that may influence the risk analysis and determination. The senior accountable official for risk management or risk executive (function) may 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 either the operation or use of the system or the provision of common controls. Such information may include, for example, organizational risk tolerance, dependencies among systems and controls, mission and business requirements, the criticality of the missions or business functions supported by the system, or the risk management strategy.

The authorizing official analyzes the information provided by the senior accountable official for risk management or risk executive (function) and information provided by the system owner or common control provider in the authorization package when making a risk determination. The information provided by the senior accountable official for risk management or risk executive (function) is documented and included, to the extent it is relevant, as part of the authorization decision (see RMF *Authorize* step, Task 4). The authorizing official may also use an automated security management and reporting tool to annotate senior accountable official for risk management or risk executive (function) input.

When the system is operating under an ongoing authorization, the risk determination task is effectively unchanged. The authorizing official analyzes the relevant security and privacy information provided by the automated security/privacy management and reporting tool to determine the current security and privacy posture of the system.

References: NIST Special Publication 800-30; NIST Special Publication 800-39 (Organization, Mission/Business Process, and System Levels); NIST Special Publication 800-137; NIST Special Publication 800-160, Volume 1 (Risk Management Process); NIST Interagency Report 8062.

[76] NIST Special Publication 800-30 provides guidance on conducting security risk assessments. NIST Interagency Report 8062 provides information about privacy risk assessments and associated risk factors.

RISK RESPONSE

Task 3 Identify and implement a preferred course of action in response to the risk determined.

Potential Inputs: Authorization package; risk determination; organization- and system-level risk assessment results.

Potential Outputs: Risk responses for determined risks.

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy; System Owner or Common Control Provider; Information Owner or Steward; Systems Security or Privacy Engineer; System Security or Privacy Officer.

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

Discussion: After risk is analyzed and determined, organizations can respond to risk in a variety of ways, including acceptance of risk and mitigation of risk. Existing risk assessment results and risk assessment techniques may be used to help determine the preferred course of action for the risk response.[77] 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 deficiency found during the assessment process remains documented in the security and privacy assessment reports and is monitored for changes to the risk factors.[78] Because the authorizing official is the only person who can accept risk, the authorizing official is responsible for reviewing the assessment reports and the plans of action and milestones and determining whether identified risks need to be mitigated prior to authorization. Decisions on the most appropriate course of action for responding to risk may 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 addressing 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 response decisions, there remains a degree of residual risk. Organizations determine acceptable degrees of residual risk based on organizational risk tolerance.

References: NIST Special Publication 800-30; NIST Special Publication 800-39 (Organization, Mission/Business Process, and System Levels); NIST Special Publication 800-160, Volume 1 (Risk Management Process); NIST Interagency Report 8062; NIST Interagency Report 8179; NIST Cybersecurity Framework (Core [Identify Function]).

AUTHORIZATION DECISION ~~RISK ACCEPTANCE~~

Task 4 Determine if the risk from the operation or use of the information system or the provision or use of common controls ~~to organizational operations, organizational assets, individuals, other organizations, or the Nation~~ 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.

[77] NIST Special Publication 800-39 provides additional information on risk response.

[78] The four security risk factors are threat, vulnerability, likelihood, and impact. NIST Special Publication 800-30 and NIST Special Publication 800-39 provide information about security risk assessments and associated risk factors. NIST Interagency Report 8062 and Section 2.2 provide additional information on privacy risk factors and conducting privacy risk assessments.

Primary Responsibility: Authorizing Official.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy; Authorizing Official Designated Representative.

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

Discussion: The explicit acceptance of risk is the responsibility of the authorizing official and cannot be delegated to other officials within the organization. The authorizing official considers many factors when deciding if the risk to the organization's operations (including mission, functions, image, and reputation) and 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.[79] The authorizing official issues an authorization decision for the system or for organization-designated common controls after reviewing the information in the authorization package, input from other organizational officials (see RMF *Authorize* step, Task 2), and other relevant information that may affect the authorization decision. The authorization package provides the most current information on the security and privacy posture of the system or the common controls. ~~Risk executive (function) inputs are documented and become part of the security authorization decision. Security authorization decisions, including inputs from the risk executive (function), are conveyed to information system owners and common control providers and made available to interested parties within the organization (e.g., information system owners and authorizing officials for interconnected systems, chief information officers, information owners/stewards, senior managers).~~

The authorization decision is conveyed by the authorizing official to the system owner or common control provider, and other organizational officials, as appropriate.[80] The authorization decision also conveys the specific terms and conditions for the authorization to operate; the authorization termination date or time-driven authorization frequency; input from the senior accountable official for risk management or risk executive (function), if provided; and for common control authorizations, the system impact level supported by the common controls. ~~The *authorization decision document* conveys the final security authorization decision from the authorizing official to the information system owner or common control provider, and other organizational officials, as appropriate. The authorization decision document contains the following information: (i) authorization decision; (ii) terms and conditions for the authorization; and (iii) authorization termination date. The security *authorization decision* indicates to the information system owner whether the system is: (i) authorized to operate; or (ii) not authorized to operate. The *terms and conditions* for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.~~

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 not authorized to use. For common controls, the authorization decision indicates to the common control provider and to the system owners of inheriting systems, whether the common controls are authorized to be provided or not authorized to be provided. The terms and conditions for the common control 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.

[79] While balancing security and privacy considerations with mission and business needs is paramount to achieving an acceptable risk-based authorization decision, there may be instances when the authorizing official and senior agency official for privacy cannot reach a final resolution regarding the appropriate protection for PII and the information systems that process PII. OMB Circular A-130 provides guidance on how to resolve such instances.

[80] Organizations are encouraged to employ automated security/privacy management and reporting tools whenever feasible, 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. It is recognized that certain controls are not conducive to the use of automated tools and therefore, manual methods are acceptable in those situations.

The authorization termination date is established by the authorizing official and indicates when the authorization expires. Organizations may eliminate the authorization termination date if the system is operating under an ongoing authorization—that is, the continuous monitoring program is sufficiently robust and mature to provide the authorizing official with the needed information to conduct ongoing risk determination and risk acceptance activities regarding the security and privacy posture of the system and the ongoing effectiveness of the controls employed within and inherited by the system. ~~The *authorization termination date*, established by the authorizing official, indicates when the security authorization expires. Authorization termination dates are influenced by federal and/or organizational policies which may establish maximum authorization periods. Organizations may choose to eliminate the authorization termination date if 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 with regard to the security state of the information system and the ongoing effectiveness of security controls employed within and inherited by the system.~~

The authorization decision is included with the authorization package and is transmitted to the system owner or common control provider. Upon receipt of the authorization decision and the authorization package, the system owner or common control provider acknowledges and implements the terms and conditions of the authorization. The organization ensures that the authorization package, including the authorization decision for systems and common controls, is made available to organizational officials including, for example, system owners inheriting common controls; chief information officers; senior accountable officials for risk management or risk executive (function); senior agency information security officers; senior agency officials for privacy; and system security and privacy officers. The authorizing official verifies on an ongoing basis as part of continuous monitoring (see RMF *Monitor* step, Task 2) that the established terms and conditions for authorization are being followed by the system owner or common control provider.

When the system is operating under an 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 continuing to provide common controls. Under ongoing authorization, the authorization frequency is specified in lieu of an authorization termination date. The authorizing official reviews the information with the specific time-driven authorization frequency defined by the organization as part of the continuous monitoring strategy and determines if the risk of continued system operation or the provision of common controls remains acceptable. If the risk remains acceptable, the authorizing official acknowledges the acceptance in accordance with organizational processes. If not, the authorizing official indicates that the risk is no longer acceptable and requires further risk response or a full denial of the authorization.

The organization determines the level of formality for the process of communicating and acknowledging continued risk acceptance by the authorizing official. The authorizing official may continue to establish and convey the specific 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 management and reporting tool as part of an automated authorization decision.

If control assessments are conducted by qualified assessors with the ~~required degree~~level of independence[81] required based on federal or organizational policies~~, appropriate security standards and guidelines,and the needs of the authorizing official,~~ and the requisite security and privacy standards and guidelines, the assessment results support ongoing authorization and may be applied to a reauthorization. Organizational policies regarding ongoing authorization and reauthorization are consistent with laws, executive orders, directives, regulations, and policies.

~~The authorization decision document is attached to the original security authorization package containing the supporting documentation and transmitted to the information system owner or common control provider. Upon receipt of the authorization decision document and original authorization package, the information system owner or common control provider acknowledges and implements the terms and~~

[81] In accordance with OMB Circular A-130, an independent evaluation of privacy program and practices is not required. However, an organization may choose to employ independent privacy assessments at the organization's discretion.

~~conditions of the authorization and notifies the authorizing official. The organization ensures that authorization documents for both information systems and for common controls are made available to appropriate organizational officials (e.g., information system owners inheriting common controls, risk executive (function), chief information officers, senior information security officers, information system security officers). Authorization documents, especially information dealing with information system vulnerabilities, are: (i) marked and appropriately protected in accordance with federal and organizational policies; and (ii) 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 information system owner or common control provider.~~

The authorizing official consults with the Senior Accountable Official for Risk Management or the Risk Executive (Function) prior to making the final authorization decision for the information system or the common controls. Because there are potentially significant dependencies among organizational systems and with external systems, the authorization decisions of individual systems are carried out in consideration of the current residual risk and PO&AMs of the organization and the risk tolerance of the organization.

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

References: NIST Special Publication 800-39 (Organization, Mission/Business Process, and System Levels); NIST Special Publication 800-160, Volume 1 (Risk Management Process).

AUTHORIZATION REPORTING

Task 5 Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.

Potential Inputs: Authorization decision.

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

Primary Responsibility: Authorizing Official or Authorizing Official Designated Representative.

Supporting Roles: System Owner or Common Control Provider; Information Owner or Steward; System Security or Privacy Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

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

Discussion: 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 head of agency. Authorizing officials also report exploitable deficiencies (i.e., vulnerabilities) in the system or controls noted during the assessment and continuous monitoring that represent significant security or privacy risk. Organizations determine, and the organizational policy reflects, what constitutes a significant security or privacy risk for reporting. Deficiencies that represent significant vulnerabilities and security/privacy risk can be reported using the subcategories, categories, and functions described in the NIST Cybersecurity Framework. Authorization decisions may be tracked and reflected as part of the organization-wide system registration process at the organization's discretion (see RMF *Prepare-System Level* step, Task 10).

References: NIST Special Publication 800-39 (Organization, Mission/Business Process, and System Levels); NIST Special Publication 800-160, Volume 1 (Decision Management and Project Assessment and Control Processes); NIST Cybersecurity Framework (Core [Identify, Protect, Detect, Respond, Recover Functions]).

Milestone Checkpoint #5

- Did the organization develop a ***plan of action and milestones*** reflecting organizational priorities for addressing the remaining weaknesses and deficiencies in the information system and its environment of operation?
- Did the organization develop an appropriate ***authorization package*** with all key documents including the security plan, security assessment report, and plan of action and milestones (if applicable)?
- Did the final ***risk determination*** and ***risk acceptance*** by the authorizing official reflect the risk management strategy developed by the organization and conveyed by the risk executive (function)?

Was the ***authorization decision*** conveyed to appropriate organizational personnel including information system owners and common control providers?

3.7 MONITOR

Purpose

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

MONITOR TASKS

Table 8 provides a summary of tasks and expected outcomes for the RMF *Monitor* step. A mapping of Cybersecurity Framework categories, subcategories, and constructs is also provided.

TABLE 8: MONITOR TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 SYSTEM AND ENVIRONMENT CHANGES	• The information system and environment of operation are monitored in accordance with the continuous monitoring strategy. [Cybersecurity Framework: **DE.CM**; **ID.GV**]
TASK 2 ONGOING ASSESSMENTS	• Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy.
TASK 3 ONGOING RISK RESPONSE	• The output of continuous monitoring activities is analyzed and responded to appropriately. [Cybersecurity Framework: **RS.AN**]
TASK 4 AUTHORIZATION UPDATES	• Risk management documents are updated based on continuous monitoring activities. [Cybersecurity Framework: **RS.IM**]
TASK 5 SECURITY AND PRIVACY REPORTING	• A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives.
TASK 6 ONGOING AUTHORIZATION	• Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.
TASK 7 SYSTEM DISPOSAL	• A system disposal strategy is developed and implemented, as needed.

Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.

SYSTEM AND ENVIRONMENT CHANGES

Task 1 ~~Determine the security impact of proposed or actual changes to~~ Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.

Potential Inputs: Organizational continuous monitoring strategy; organizational configuration management policy and procedures; organizational policy and procedures for handling unauthorized system changes; system security and privacy plans; configuration change requests/approvals; system design

documentation; security and privacy assessment reports; plans of action and milestones; information from 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 or Common Control Provider; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Commented [A12]: Moved from supporting role

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Authorizing Official or Authorizing Official Designated Representative; Information Owner or Steward; System Security or Privacy Officer.

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

Discussion: Systems are in a constant state of change with changes occurring in the technology or machine elements, human elements, and physical or environmental elements. Changes to the technology or machine elements include for example, upgrades to hardware, software, or firmware; changes to the human elements include for example, staff turnover or a reduction in force; and modifications to the surrounding physical and environmental elements include for example, changes in the location of the facility or the physical access controls protecting the facility. A disciplined and structured approach to managing, controlling, and documenting changes to systems and environments of operation, and adherence with terms and conditions of the authorization, is an essential element of security and privacy programs. Organizations establish configuration management and control processes to support configuration and change management.[82] ~~The information system owner and common control provider use this information in assessing the potential security impact of the changes. Documenting proposed or actual changes to an information system or its environment of operation and subsequently assessing the potential impact those changes may have on the security state of the system or the organization is an important aspect of security control monitoring and maintaining the security authorization over time. Information system changes are generally not undertaken prior to assessing the security impact of such changes. Organizations are encouraged to maximize the use of automation when managing changes to the information system or its environment of operation.~~

~~Security impact analysis conducted by the organization, determines the extent to which proposed or actual changes to the information system or its environment of operation can affect or have affected the security state of the system. Changes to the information system or its environment of operation may affect the security controls currently in place (including system-specific, hybrid, and common controls), produce new vulnerabilities in the system, or generate requirements for new security controls that were not needed previously. If the results of the security impact analysis indicate that the proposed or actual changes can affect or have affected the security state of the system, corrective actions are initiated and appropriate documents revised and updated (e.g., the security plan, security assessment report, and plan of action and milestones). The information system owner or common control provider consults with appropriate organizational officials/entities (e.g., configuration control board, senior information security officer, information system security officer) prior to implementing any security-related changes to the information system or its environment of operation. The authorizing official or designated representative uses the revised and updated security assessment report in collaboration with the senior information security officer and risk executive (function) to determine if a formal reauthorization action is necessary. Most routine changes to an information system or its environment of operation can be handled by the organization's continuous monitoring program, thus supporting the concept of ongoing authorization and near real-time risk management. Conducting security impact analyses is part of an ongoing assessment of risk. As risk assessments are updated and refined, organizations use the results to modify security plans based on the most recent threat and vulnerability information available. Updated risk assessments provide a foundation for prioritizing/planning risk responses. The authorizing official or designated representative, in collaboration with the risk executive (function), confirms as needed, determinations of residual risk. The~~

[82] NIST Special Publication 800-128 provides guidance on security-focused configuration management (SecCM). Note that the SecCM process described in Special Publication 800-128 includes a related monitoring step.

~~risk executive (function) notifies the authorizing official of any significant changes in the organizational risk posture.~~

Common activities within organizations can cause changes to systems or the environments of operation and can have a significant impact on the security and privacy posture of systems. Examples include installing or disposing of hardware, making changes to configurations, and installing patches outside of the established configuration change control process. Unauthorized changes may occur because of purposeful attacks by adversaries or inadvertent errors by authorized personnel. Thus, in addition to adhering to the established configuration management process, organizations monitor for unauthorized changes to systems and analyze information about unauthorized changes that have occurred to determine the root cause of the unauthorized change. In addition to monitoring for unauthorized changes, organizations continuously monitor systems and environments of operation for any authorized changes that impact the privacy posture of systems.[83]

Once the root cause of an unauthorized change (or an authorized change that impacts the privacy posture of the system) has been determined, organizations respond accordingly (see RMF *Monitor* step, Task 3). For example, if the root cause of an unauthorized change is determined to be an adversarial attack, multiple actions could be taken such as invoking incident response processes, adjusting intrusion detection and prevention tools and firewall configurations, or implementing additional or stronger controls to reduce the risk of future attacks. If the root cause of an unauthorized change is determined to be a failure of staff to adhere to established configuration management processes, remedial training for certain individuals may be warranted.

References: NIST Special Publication 800-30; ~~NIST Special Publication 800-53A;~~ NIST Special Publication 800-128; NIST Interagency Report 8062.

ONGOING ~~SECURITY CONTROL~~ ASSESSMENTS

Task 2 Assess the ~~technical, management, and operational security~~ controls implemented within and inherited by the ~~information~~ system in accordance with the continuous monitoring strategy.

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

Potential Outputs: Updated security and privacy assessment reports.

Primary Responsibility: Control Assessor.

Supporting Roles: Authorizing Official or Authorizing Official Designated Representative; System Owner or Common Control Provider; Information Owner or Steward; System Security or Privacy Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

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

Discussion: After the initial system or common control authorization, the organization assesses all controls implemented within and inherited by the system on an ongoing basis. The frequency of monitoring for control effectiveness is based on the organizational continuous monitoring strategy ~~developed by the information system owner or common control provider and approved by the authorizing official and senior information security officer.~~and can be supplemented by the system-level continuous monitoring strategy, as needed. Adherence to terms and conditions specified by the authorizing official as part of the authorization decision are also monitored (see RMF *Monitor* step, Task 1).

[83] For information about the distinction between authorized and unauthorized system behavior, see the discussion of security and privacy in Section 2.2.

For ongoing control assessments, control assessors have the required degree of independence as determined by the authorizing official ~~(See Appendix D.13 and Appendix F.4)~~.[84] The 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 may allow for reuse of assessment results in support of ongoing authorization and when reauthorization is required. ~~Organizations can use the current year's assessment results to meet the annual FISMA security control assessment requirement.~~

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 the testing and evaluation of systems as part of the SDLC or an 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 consistent with the reuse policy established for the organization and are supplemented with additional assessments as needed. The reuse of assessment results is critical in achieving a cost-effective, fully integrated security program capable of producing the evidence necessary to determine the security posture of information systems and the organization. The use of automation to support control assessments facilitates a greater frequency, volume, and coverage of assessments~~that is consistent with the monitoring strategy established by the organiation~~.

References: NIST Special Publication 800-53A; NIST Special Publication 800-137; NIST Special Publication 800-160, Volume 1 (Verification, Validation, Operation, and Maintenance Processes).

ONGOING RISK RESPONSE ~~REMEDIATION ACTIONS~~

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

Potential Inputs: Security and privacy assessment reports; organization- and system-level risk assessment results; system security and privacy plans; plans of action and milestones.

Potential Outputs: Mitigation actions or risk acceptance decisions; updated security and privacy assessment reports.

Primary Responsibility: Authorizing Official; System Owner; Common Control Provider.

Commented [A13]: Moved from supporting role

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Official for Privacy; Authorizing Official Designated Representative; Information Owner or Steward; System Security or Privacy Officer; Systems Security or Privacy Engineer; Security or Privacy Architect.

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

Discussion: Assessment information produced by an assessor during continuous monitoring is provided to the system owner and the common control provider in updated security and privacy assessment reports or via reports from automated security/privacy management and reporting tools. The authorizing official determines the appropriate risk response to the assessment findings or approves responses proposed by the system owner and common control provider. The system owner and common control provider subsequently initiate ~~remediation actions on outstanding items listed in the plan of actions and milestones and findings produced during the ongoing monitoring of security controls.~~implement the appropriate risk response. 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, if called upon, provide recommendations for remediation actions. Recommendations for

[84] In accordance with OMB Circular A-130, an independent evaluation of privacy program and practices is not required. However, an organization may choose to employ independent privacy assessments at the organization's discretion.

remediation actions may also be provided by an automated security/privacy management and reporting tool. An organizational assessment of risk (RMF *Prepare-Organization Level* step, Task 3) and system-level risk assessment results (RMF *Prepare-System Level* step, Task 7) help inform the decisions regarding ongoing risk response. Controls that are modified, enhanced, or added as part of ongoing risk response are reassessed by assessors to ensure that the new, modified, or enhanced controls have been implemented correctly, are operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements of the system.

References: NIST Special Publication 800-30; NIST Special Publication 800-53; NIST Special Publication 800-53A; NIST Special Publication 800-137; NIST Special Publication 800-160, Volume 1 (Risk Management Process); NIST Interagency Report 8062; NIST Cybersecurity Framework (Core [Respond Functions]); CNSS Instruction 1253.

AUTHORIZATION ~~KEY~~ 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; organization- and system-level risk assessment results; system security and privacy plans; plans of action and milestones.

Potential Outputs: Updated security and privacy assessment reports;[85] updated plans of action and milestones; updated risk assessment results; updated system security and privacy plans.

Primary Responsibility: System Owner; Common Control Provider.

Supporting Roles: Information Owner or Steward; System Security or Privacy Officer; Senior Agency Official for Privacy.

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

Discussion: To ~~facilitate~~ achieve ~~the~~ near real-time risk management~~of risk associated with the operation and use of the information system~~, the organization updates security and privacy plans, security and privacy assessment reports, and plans of action and milestones on an ongoing basis. Updates to the security and privacy plans reflect any modifications to controls based on risk mitigation activities carried out by system owners or common control providers. Updates to control assessment reports reflect the additional assessment activities carried out to determine control effectiveness based on implementation details in the security and privacy plans. Plans of action and milestones are updated based on progress made on the current outstanding items listed in the plan; address security and privacy risks discovered as part of control effectiveness monitoring; and describe how the system owner or common control provider intends to address those security and privacy risks. The updated information raises awareness of the security and privacy posture of the system and the common controls inherited by the system, thereby, supporting near real-time risk management and the ongoing authorization process.

The frequency of updates to risk management-related information is at the discretion of the system owner, common control provider, and authorizing officials ~~organization~~ in accordance with federal and organizational policies and is consistent with the organizational and system-level continuous monitoring strategies. The updates to information regarding the security and privacy posture 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. The use of automated support tools and organization-wide security and privacy program management practices help ensure that authorizing officials can readily access the current security and privacy posture of the system. This provides essential information for continuous monitoring and ongoing

[85] If a comparable report meets the requirements of what is to be included in an assessment report (e.g., a report generated from a security or privacy management and reporting tool), then the comparable report would itself constitute the assessment report.

authorization and promotes the near real-time management of risk to organizational operations and assets, individuals, other organizations, and the Nation.

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 systems through configuration management procedures is necessary to achieve transparency and traceability in the security and privacy activities of the organization; to obtain individual accountability for any security- and privacy-related actions; and to understand emerging trends in the security and privacy programs of the organization.

~~Status reports occur at appropriate intervals to transmit significant security-related information about the information system (including information regarding the ongoing effectiveness of security controls employed within and inherited by the system), but not so frequently as to generate unnecessary work. The authorizing official uses the security status reports in collaboration with the senior information security officer and risk executive (function) to determine if a formal reauthorization action is necessary. Security status reports are appropriately marked, protected, and handled in accordance with federal and organizational policies. At the discretion of the organization, security status reports can be used to help satisfy FISMA reporting requirements for documenting remedial actions for any security-related weaknesses or deficiencies. Note that this status reporting is intended to be ongoing, not to be interpreted as requiring the time, expense, and formality associated with the information provided for the initial approval to operate. Rather, the reporting is conducted in the most cost-effective manner consistent with achieving the reporting objectives.~~

References: NIST Special Publication 800-53A.

SECURITY ~~STATUS~~AND PRIVACY POSTURE REPORTING

Task 5 Report the security and privacy posture of the system ~~(including the effectiveness of security controls employed within and inherited by the system)~~ to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.

Potential Inputs: Security and privacy assessment reports; plans of action and milestones; organization- and system-level risk assessment results; organization- and system-level continuous monitoring strategy; system security and privacy plans.

Potential Outputs: Security and privacy posture reports.

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

Supporting Roles: System Security or Privacy Officer.

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

Discussion: The results of monitoring activities are documented and reported to the authorizing official and other selected organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy. Other organizational officials who may receive security and privacy posture reports include, for example, chief information officer, senior agency information security officer, senior agency official for privacy, senior agency official for risk management or risk executive (function), information owner or steward, incident response roles, and contingency planning roles. Security and privacy ~~status~~ posture reporting can be event-driven, time-driven, or event- and time-driven.[86] The reports provide the authorizing official and other organizational officials with information regarding the security and privacy posture of the systems including the effectiveness of implemented controls. Security and privacy posture reports describe the ongoing monitoring activities employed by system owners or common control

[86] See Appendix F for more information about time- and event-driven authorizations and reporting.

providers. The reports also include information about security and privacy risks in the systems and environments of operation discovered during control assessments, auditing, and continuous monitoring and how system owners or common control providers plan to address those risks. ~~Security status reports also address vulnerabilities in the information system and its environment of operation discovered during the security control assessment, security impact analysis, and security control monitoring and how the information system owner or common control provider intends to address those vulnerabilities.~~

Organizations have flexibility in the breadth, depth, formality, form, and format of security and privacy posture reports. The goal is efficient ongoing communication with the authorizing official and other organizational officials as necessary, conveying the current security and privacy posture of systems and environments of operation and how the current posture affects individuals, organizational missions, and business functions. At a minimum, security and privacy posture reports summarize changes to the security and privacy plans, security and privacy assessment reports, and plans of action and milestones that have occurred since the last report. The use of automated security/privacy management and reporting tools by the organization facilitates the effectiveness and timeliness of security and privacy posture reporting.

The frequency of security and privacy posture reports is at the discretion of the organization and in compliance with federal and organizational policies. 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 posture reports and consult with the senior accountable official for risk management or risk executive (function), senior agency information security officer, and senior agency official for privacy to determine if a reauthorization action is necessary. Security and privacy posture reports are marked, protected, and handled in accordance with federal and organizational policies. Security and privacy posture reports can be used to satisfy FISMA reporting requirements for documenting remediation actions for security- and privacy-related weaknesses or deficiencies. Such reporting is intended to be ongoing and should not be 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 Publication 800-53A; NIST Special Publication 800-137; NIST Cybersecurity Framework (Core [Identify, Protect, Detect, Respond, Recover Functions]).

ONGOING AUTHORIZATION ~~RISK DETERMINATION AND ACCEPTANCE~~

Task 6 Review the security and privacy posture of the system ~~(including the effectiveness of security controls employed within and inherited by the system)~~ on an ongoing basis to determine whether the risk ~~to organizational operations, organizational assets, individuals, other organizations, or the Nation~~remains acceptable.

Potential Inputs: Security and privacy posture reports;[87] plans of action and milestones; organization- and system-level 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.

Supporting Roles: Senior Accountable Official for Risk Management or Risk Executive (Function); Senior Agency Information Security Officer; Senior Agency Official for Privacy; Authorizing Official Designated Representative.

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

[87] If a comparable report meets the requirements of what is to be included in a security or privacy posture report (e.g., a report generated from a security or privacy management and reporting tool), then the comparable report would itself constitute the posture report.

Discussion: In accordance with the guidance in the RMF *Authorize* step, Task 4, the authorizing official or designated representative reviews the security and privacy posture of the system (including the effectiveness of implemented 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 risks may change based on the information provided in the security and privacy posture reports because the reports may indicate changes to any of the security or privacy risk factors. Determining how changing conditions affect organizational mission or business risk is essential for managing privacy risk and maintaining adequate security. By carrying out ongoing risk determination and risk acceptance, authorizing officials can maintain system and common control authorizations over time and transition to ongoing authorization. Reauthorization actions occur only in accordance with federal or organizational policies. The authorizing official conveys updated risk determination and acceptance results to the senior accountable official for risk management or the risk executive (function).

The use of automated support tools to capture, organize, quantify, visually display, and maintain security and privacy posture information promotes 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 in an automated fashion and providing the data to decision makers at different levels within the organization in an easy-to-understand format.

References: NIST Special Publication 800-30; NIST Special Publication 800-39 (Organization, Mission/Business Process, and System Levels), NIST Special Publication 800-160, Volume 1 (Risk Management Process); NIST Interagency Report 8062.

~~INFORMATION~~SYSTEM ~~REMOVAL AND~~ DISPOSAL

Task 7 Implement a system disposal strategy and execute required actions when a system is removed from operation.

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

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

Primary Responsibility: System Owner.

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

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

Discussion: When a system is removed from operation, several risk management-related actions are required. Organizations ensure that all controls addressing system 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 that is being removed from service. Security and privacy posture reports reflect the security and privacy status of the system. Users and application owners hosted on the disposed system are notified as appropriate, and any control inheritance relationships are reviewed and assessed for impact. This task also applies to system components that are removed from operation. ~~This task also applies to subsystems that are removed from information systems or decommissioned. The effects of the subsystem removal or disposal are assessed with respect to the overall operation of the information system where the subsystem resided, or in the case of dynamic subsystems, the information systems where the subsystems were actively~~

~~employed.~~Organizations that remove a system from operation update the inventory of information systems to reflect the removal of the system.

References: NIST Special Publication 800-30; ~~NIST Special Publicatoin 800-53A;~~ NIST Special Publication 800-88; NIST Interagency Report 8062.

~~**Milestone Checkpoint #6**~~

- ~~Is the organization effectively monitoring changes to the ***information system*** and its ***environment of operation*** including the effectiveness of deployed ***security controls*** in accordance with the continuous monitoring strategy?~~
- ~~Is the organization effectively analyzing the ***security impacts*** of identified changes to the information system and its environment of operation?~~
- ~~Is the organization conducting ***ongoing assessments of security controls*** in accordance with the monitoring strategy?~~
- ~~Is the organization taking the necessary ***remediation actions*** on an ongoing basis to address identified weaknesses and deficiencies in the information system and its environment of operation?~~
- ~~Does the organization have an effective process in place to report the ***security status*** of the information system and its environment of operation to the authorizing officials and other designated senior leaders within the organization on an ongoing basis?~~
- ~~Is the organization updating critical ***risk management documents*** based on ongoing monitoring activities?~~
- ~~Are authorizing officials conducting ***ongoing security authorizations*** by employing effective continuous monitoring activities and communicating updated risk determination and acceptance decisions to information system owners and common control providers?~~

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; 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 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 controls, *rightsizing* RMF activities for mission and business success.

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, STANDARDS, AND GUIDELINES

Commented [A14]: Changes are not tracked in this Appendix.

LAWS AND EXECUTIVE ORDERS

1. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
2. Federal Information Security Modernization Act (P.L. 113-283), December 2014.
3. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013.
4. Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure

POLICIES, DIRECTIVES, REGULATIONS, AND INSTRUCTIONS

1. Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems, March 2014. https://www.cnss.gov
2. Committee on National Security Systems Instruction 4009, *National Information Assurance Glossary*, April 2015. https://www.cnss.gov
3. Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf
4. Office of Management and Budget Circular No. A-130, *Managing Information as a Strategic Resource*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
5. Office of Management and Budget Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf

STANDARDS, GUIDELINES, INTERAGENCY REPORTS, AND MISCELLANEOUS

1. Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, January 2013. https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf
2. International Organization for Standardization/International Electrotechnical Commission 27001:2013, *Information Technology -- Security techniques -- Information security management systems – Requirements*, October 2013. https://www.iso.org/standard/54534.html

3. International Organization for Standardization/International Electrotechnical Commission 15408-1:2009, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
4. International Organization for Standardization/International Electrotechnical Commission 15408-2:2008, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements*, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf
5. International Organization for Standardization/International Electrotechnical Commission 15408-3:2008, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements*, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf
6. International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, *Systems and software engineering — Systems life cycle processes*, May 2015.
7. National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. https://doi.org/10.6028/NIST.FIPS.199
8. National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. https://doi.org/10.6028/NIST.FIPS.200
9. National Institute of Standards and Technology Special Publication (SP) 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006. https://doi.org/10.6028/NIST.SP.800-18r1
10. National Institute of Standards and Technology Special Publication (SP) 800-30 Revision 1, *Guide for Conducting Risk Assessments*, September 2012. https://doi.org/10.6028/NIST.SP.800-30r1
11. National Institute of Standards and Technology Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011. https://doi.org/10.6028/NIST.SP.800-39
12. National Institute of Standards and Technology Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002. https://doi.org/10.6028/NIST.SP.800-47
13. National Institute of Standards and Technology Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (includes updates as of 01-22-2015). https://doi.org/10.6028/NIST.SP.800-53r4

14. National Institute of Standards and Technology Special Publication (SP) 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, December 2014 (includes updates as of 12-18-2014). https://doi.org/10.6028/NIST.SP.800-53Ar4

15. National Institute of Standards and Technology Special Publication (SP) 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003. https://doi.org/10.6028/NIST.SP.800-59

16. National Institute of Standards and Technology Special Publication (SP) 800-60 Revision 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008. https://doi.org/10.6028/NIST.SP.800-60v1r1

17. National Institute of Standards and Technology Special Publication (SP) 800-60, Revision 1, *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008. https://doi.org/10.6028/NIST.SP.800-60v2r1

18. National Institute of Standards and Technology Special Publication (SP) 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008. https://doi.org/10.6028/NIST.SP.800-64r2

19. National Institute of Standards and Technology Special Publication (SP) 800-88 Revision 1, *Guidelines for Media Sanitization*, December 2014. https://doi.org/10.6028/NIST.SP.800-88r1

20. National Institute of Standards and Technology Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010. https://doi.org/10.6028/NIST.SP.800-122

21. National Institute of Standards and Technology Special Publication (SP) 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011. https://doi.org/10.6028/NIST.SP.800-128

22. National Institute of Standards and Technology Special Publication (SP) 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011. https://doi.org/10.6028/NIST.SP.800-137

23. National Institute of Standards and Technology Special Publication (SP) 800-160, Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, November 2016 (includes updates as of 03-21-2018). https://doi.org/10.6028/NIST.SP.800-160v1

24. National Institute of Standards and Technology Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015. https://doi.org/10.6028/NIST.SP.800-161

25. National Institute of Standards and Technology Special Publication 171, Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, December 2016. https://csrc.nist.gov/CSRC/media/Publications/sp/800-171a/draft/documents/sp800-171a-draft-20180220.pdf

26. National Institute of Standards and Technology Special Publication 171A (Draft), *Assessing Security Requirements for Controlled Unclassified Information*, February 2018. https://csrc.nist.gov/CSRC/media/Publications/sp/800-171a/draft/documents/sp800-171a-draft-20180220.pdf

27. National Institute of Standards and Technology Special Publication (SP) 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, August 2017. https://doi.org/10.6028/NIST.SP.800-181

28. National Institute of Standards and Technology Internal Report (NISTIR) 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017. https://doi.org/10.6028/NIST.IR.8062

29. National Institute of Standards and Technology Interagency Report (NISTIR) 8170 (Draft), *The Cybersecurity Framework: Implementation Guidance for Federal Agencies*, May 2017. https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf

30. National Institute of Standards and Technology Internal Report (NISTIR) 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*, April 2018. https://doi.org/10.6028/NIST.IR.8179

31. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 2018. https://doi.org/10.6028/NIST.CSWP.04162018

32. National Archives and Records Administration, *Controlled Unclassified Information (CUI) Registry*. https://www.archives.gov/cui

33. Executive Office of the President, *The Common Approach to Federal Enterprise Architecture*, May 2012. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf

34. Executive Office of the President, *Federal Enterprise Architecture Framework, Version 2*, January 2013. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Commented [A15]: Changes are not tracked in this Appendix.

Appendix B provides definitions for terminology used within Special Publication 800-37. Sources for terms used in this publication are cited as applicable. Where no citation is noted, the source of the definition is Special Publication 800-37.

adequate security [OMB Circular A-130]	Security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.
agency [OMB Circular A-130]	Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.
allocation	The process an organization employs to determine whether controls are defined as system-specific, hybrid, or common. The process an organization employs to assign controls to specific information system components responsible for providing a security or privacy capability (e.g., router, server, remote sensor).
application	A software program hosted by an information system.
assessment	See *Control Assessment*.
assessment plan	The objectives for the control assessments and a detailed roadmap of how to conduct such assessments.
assessor	The individual, group, or organization responsible for conducting a security or privacy assessment.
assurance [ISO/IEC 15026, Adapted]	Grounds for justified confidence that a [security or privacy] claim has been or will be achieved. *Note 1:* Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated. *Note 2:* Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims.
audit log [CNSSI 4009]	A chronological record of system activities, including records of system accesses and operations performed in a given period.

audit trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to result.
authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See *authentication*.
authorization boundary [OMB Circular A-130]	All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.
authorization package [OMB Circular A-130]	The essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the provision of a designated set of common controls. At a minimum, the authorization package includes an executive summary, system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.
authorization to operate [OMB Circular A-130]	The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.
authorizing official [OMB Circular A-130]	A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.
authorizing official designated representative	An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with the authorization process.
availability [44 U.S.C. Sec. 3542]	Ensuring timely and reliable access to and use of information.
baseline	See *control baseline*.
baseline configuration [NIST SP 800-128, adapted]	A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

capability	A combination of mutually reinforcing controls implemented by technical means, physical means, and procedural means. Such controls are typically selected to achieve a common information security- or privacy-related purpose.
chain of trust (supply chain)	A certain level of trust in supply chain interactions such that each participant in the consumer-provider relationship provides adequate protection for its component products, systems, and services.
chief information officer [OMB Circular A-130]	The senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.
chief information security officer	See *Senior Agency Information Security Officer*.
classified information	See classified national security information.
classified national security information [CNSSI 4009]	Information that has been determined pursuant to Executive Order (E.O.) 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
commodity service	A system service provided by a commercial service provider to a large and diverse set of consumers. The organization acquiring or receiving the commodity service possesses limited visibility into the management structure and operations of the provider, and while the organization may be able to negotiate service-level agreements, the organization is typically not able to require that the provider implement specific controls.
common control [OMB Circular A-130]	A security or privacy control that is inherited by multiple information systems or programs.
common control provider	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., controls inheritable by organizational systems).
common criteria [CNSSI 4009]	Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems.
compensating controls	The security and privacy controls implemented in lieu of the controls in the baselines described in NIST Special Publication 800-53 that provide equivalent or comparable protection for a system or organization.
component	See *system component*.

confidentiality [44 U.S.C. Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
configuration control [CNSSI 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
configuration item [NIST SP 800-128]	An aggregation of system components that is designated for configuration management and treated as a single entity in the configuration management process.
configuration management [NIST SP 800-128]	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
configuration settings [NIST SP 800-128]	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.
continuous monitoring	Maintaining ongoing awareness to support organizational risk decisions.
continuous monitoring program	A program established to collect information in accordance with preestablished metrics, utilizing information readily available in part through implemented security controls. *Note:* Privacy and security continuous monitoring strategies and programs can be the same or different strategies and programs.
control assessment	The testing or evaluation of the controls in an information system or an organization 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 or privacy requirements for the system or the organization.
control assessor	The individual, group, or organization responsible for conducting a control assessment. See *assessor*.
control baseline	A collection of controls specifically assembled or brought together to address the protection needs of a group, organization, or community of interest.
control effectiveness	A measure of whether a given control is contributing to the reduction of information security or privacy risk.
control enhancement	Augmentation of a control to build in additional, but related, functionality to the control; increase the strength of the control; or add assurance to the control.

control inheritance [CNSSI 4009]	A situation in which a system or application receives protection from controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *common control*.
controlled unclassified information [32 CFR part 2002]	Information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.
countermeasures [FIPS 200]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a system. Synonymous with *security controls* and *safeguards*.
cybersecurity [OMB Circular A-130]	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
developer	A general term that includes developers or manufacturers of systems, system components, or system services; systems integrators; vendors; and product resellers. Development of systems, components, or services can occur internally within organizations or through external entities.
enterprise [CNSSI 4009]	An organization with a defined mission/goal and a defined boundary, using systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, human resources, financial management, security, and systems, information and mission management. See *organization*.
enterprise architecture [44 U.S.C. Sec. 3601]	A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.
environment of operation [OMB Circular A-130]	The physical surroundings in which an information system processes, stores, and transmits information.
event [NIST SP 800-61, Adapted]	Any observable occurrence in a system.

executive agency [OMB Circular A-130]	An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an independent establishment as defined in 5 U.S.C. Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C. Chapter 91.
external system (or component)	A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required controls or the assessment of control effectiveness.
external system service	A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required controls or the assessment of control effectiveness.
external system service provider	A provider of external system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
external network	A network not controlled by the organization.
federal agency	See *executive agency*.
federal enterprise architecture [FEA Program Management Office]	A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
federal information system [40 U.S.C. Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
firmware [CNSSI 4009]	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. See *hardware* and *software.*
hardware [CNSSI 4009]	The material physical components of a system. See *software* and *firmware*.
high-impact system [FIPS 200]	A system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of high.
hybrid control [OMB Circular A-130]	A security or privacy control that is implemented for an information system in part as a common control and in part as a system-specific control. See *common control* and *system-specific control*.

impact	With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.
impact value [FIPS 199]	The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate or high.
incident [44 U.S.C. Sec. 3552]	An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
independent verification and validation [CNSSI 4009]	A comprehensive review, analysis, and testing, (software and/or hardware) performed by an objective third party to confirm (i.e., verify) that the requirements are correctly defined, and to confirm (i.e., validate) that the system correctly implements the required functionality and security requirements.
industrial control system [NIST SP 800-82]	General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).
information [OMB Circular A-130]	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.
information owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
information resources [44 U.S.C. Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
information security [44 U.S.C. Sec. 3542]	The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
information security architecture [OMB Circular A-130]	An embedded, integral part of the enterprise architecture that describes the structure and behavior of the enterprise security processes, security systems, personnel and organizational subunits, showing their alignment with the enterprise's mission and strategic plans.

information security program plan [OMB Circular A-130]	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
information security risk [NIST SP 800-30]	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or systems.
information steward	An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
information system [44 U.S.C. Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
information system boundary	See *authorization boundary*.
information system security officer [CNSSI 4009]	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
information technology [OMB Circular A-130]	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.
information technology product	See *system component*.
information type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management) defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.

interface [CNSSI 4009]	Common boundary between independent systems or modules where interactions take place.
integrity [44 U.S.C. Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
joint authorization	Authorization involving multiple authorizing officials.
low-impact system [FIPS 200]	A system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS Publication 199 potential impact value of low.
media [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration memory chips, and printouts (but excluding display media) onto which information is recorded, stored, or printed within a system.
moderate-impact system [FIPS 200]	A system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of moderate and no security objective is assigned a potential impact value of high.
national security system [44 U.S.C. Sec. 3542]	Any system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
network	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
network access	Access to a system by a user (or a process acting on behalf of a user) communicating through a network including, for example, a local area network, a wide area network, and Internet.

operational technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.
operations technology	See *operational technology*.
organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure including, for example, federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or as appropriate, any of their operational elements.
overlay [OMB Circular A-130]	A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. See *tailoring* and *tailored control baseline*.
personally identifiable information [OMB Circular A-130]	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.
plan of action and milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
potential impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (FIPS Publication 199 low); a serious adverse effect (FIPS Publication 199 moderate); or a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
privacy architect	Individual, group, or organization responsible for ensuring that the system privacy requirements necessary to protect individuals' privacy are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and information systems processing PII.
privacy control [OMB Circular A-130]	The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. *Note:* Controls can be selected to achieve multiple objectives; those controls that are selected to achieve both security and privacy objectives require a degree of collaboration between the organization's information security program and privacy program.

privacy control assessment [OMB Circular A-130]	The assessment of privacy controls to determine whether the controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks. A privacy control assessment is both an assessment and a formal document detailing the process and the outcome of the assessment.
privacy control baseline	A collection of controls specifically assembled or brought together by a group, organization, or community of interest to address the privacy protection needs of individuals.
privacy impact assessment [OMB Circular A-130]	An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.
privacy plan [OMB Circular A-130]	A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.
privacy posture	The privacy posture represents the status of the information systems and information resources (e.g., personnel, equipment, funds, and information technology) within an organization based on information assurance resources (e.g., people, hardware, software, policies, procedures) and the capabilities in place to comply with applicable privacy requirements and manage privacy risks and to react as the situation changes.
privacy program plan [OMB Circular A-130]	A formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.
privacy requirement	A requirement that applies to an information system or an organization that is derived from applicable laws, executive orders, directives, policies, standards, regulations, procedures, and/or mission/business needs with respect to privacy. *Note:* The term *privacy requirement* can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.

privacy-related information	Information that describes the privacy posture of an information system or organization.
provenance	The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data.
reciprocity	Agreement among participating organizations to accept each other's security assessments to reuse system resources and/or to accept each other's assessed security posture to share information.
records [44 U.S.C. § 3301]	All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.
resilience [CNSSI 4009]	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
risk [OMB Circular A-130]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
risk assessment [NIST SP 800-30]	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.
risk executive (function)	An individual or group within an organization that helps to ensure that security risk-related considerations for individual systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and managing risk from individual systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

risk management [OMB Circular A-130]	The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.
risk mitigation [CNSSI 4009]	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
risk response [OMB Circular A-130]	Accepting, avoiding, mitigating, sharing, or transferring risk to agency operations, agency assets, individuals, other organizations, or the Nation.
sanitization [NIST SP 800-88]	A process to render access to target data on the media infeasible for a given level of effort. Clear, purge, and destroy are actions that can be taken to sanitize media.
scoping considerations	A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of controls in the control baselines. Considerations include policy/regulatory, technology, physical infrastructure, system component allocation, operational/environmental, public access, scalability, common control, and security objective.
security [CNSSI 4009]	A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach.
security architect	Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.
security categorization	The process of determining the security category for information or a system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See *security category*.
security category [OMB Circular A-130]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on agency operations, agency assets, individuals, other organizations, and the Nation.

security control [OMB Circular A-130]	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.
security control assessment [OMB Circular A-130]	The testing or evaluation of security 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 requirements for an information system or organization.
security control baseline [OMB Circular A-130]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. See also *control baseline*.
security objective [FIPS 199]	Confidentiality, integrity, or availability.
security plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. The security plan describes the authorization boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems. See *system security plan*.
security posture [CNSSI 4009]	The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. Synonymous with *security status*.
security requirement [FIPS 200, Adapted]	A requirement levied on an information system or an organization that is derived from applicable laws, executive orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. *Note:* Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.
security-relevant information	Information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.
senior agency information security officer [44 U.S.C. Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

senior agency official for privacy [OMB Circular A-130]	The senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.
software [CNSSI 4009]	Computer programs and associated data that may be dynamically written or modified during execution.
subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
supply chain [OMB Circular A-130]	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
supply chain risk [OMB Circular A-130]	Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
supply chain risk [OMB Circular A-130]	The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.
system [CNSSI 4009]	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. See *information system.* *Note:* Systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.
[ISO/IEC/IEEE 15288]	Combination of interacting elements organized to achieve one or more stated purposes. *Note 1:* There are many types of systems. Examples include: general and special-purpose information systems; command, control, and communication systems; crypto modules; central processing unit and graphics processor boards; industrial/process control systems; flight control systems; weapons, targeting, and fire control systems; medical devices and treatment systems; financial, banking, and merchandising transaction systems; and social networking systems. *Note 2:* The interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities. *Note 3:* System of systems is included in the definition of system.
system boundary	See *authorization boundary*.
system component [NIST SP 800-128]	A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.

system development life cycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.
system privacy officer	Individual with assigned responsibility for maintaining the appropriate operational privacy posture for a system or program.
systems privacy engineer	Individual assigned responsibility for conducting systems privacy engineering activities.
systems privacy engineering	Process that captures and refines privacy requirements and ensures their integration into information technology component products and information systems through purposeful privacy design or configuration.
systems security engineer	Individual assigned responsibility for conducting systems security engineering activities.
systems security engineering	Process that captures and refines security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration.
system security officer	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
system security plan	See *security plan*.
system-related privacy risk [OMB Circular A-130]	Risk to an individual or individuals associated with the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their PII. See *risk*.
system-related security risk [NIST SP 800-30]	Risk that arises through the loss of confidentiality, integrity, or availability of information or systems and that considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See *risk*.
system-specific control [OMB Circular A-130]	A security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system.
tailored control baseline	A set of controls resulting from the application of tailoring guidance to a control baseline. See *tailoring* and *overlay*.
tailoring [OMB Circular A-130]	The process by which security control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation. The tailoring process may also be applied to privacy controls. See *overlay*.

threat [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
threat source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. See *threat agent*.
trustworthiness [CNSSI 4009]	The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.
trustworthiness (system)	The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats and individuals' privacy.
trustworthy information system [OMB Circular A-130]	An information system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.
system user	Individual, or (system) process acting on behalf of an individual, authorized to access a system.
vulnerability [CNSSI 4009]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. *Note:* The term *weakness* is synonymous for *deficiency*. Weakness may result in security and/or privacy risks.
vulnerability assessment [CNSSI 4009]	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CUI	Controlled Unclassified Information
DoD	Department of Defense
EO	Executive Order
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OT	Operations Technology
PCM	Privacy Continuous Monitoring
PII	Personally Identifiable Information
RMF	Risk Management Framework
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SecCM	Security-focused Configuration Management

Commented [A16]: Changes are not tracked in this appendix.

APPENDIX D

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.[88] 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.[89] 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 and privacy risks. Many risk management roles defined in this publication have counterpart roles defined in the SDLC processes carried out by organizations. Organizations align their risk management roles with similar (or complementary) roles defined for the SDLC whenever possible.[90]

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 is the only organizational official who can accept the security and privacy risk to organizational operations, organizational assets, and individuals.[91] 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 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 can deny authorization to operate an information system or if the system is operational, halt operations, if unacceptable risks exist. Authorizing officials coordinate their activities with the risk executive (function), chief information officer, senior information security officer, common control providers, information system owners, information system security officers, security control assessors, and other interested parties during the security authorization process. With the increasing complexity of missions/business processes, partnership arrangements, and the use of external/shared services, it is possible that a particular information system may involve multiple authorizing officials. If so, agreements are established among the authorizing officials and documented in the security plan.~~

[88] Organizations may define other roles (e.g., facilities manager, human resources manager, systems administrator) to support the risk management process.

[89] Organizations ensure that there are no conflicts of interest when assigning the same individual to multiple risk management roles. See RMF *Prepare-Organization Level* step, Task 1.

[90] For example, the SDLC role of system developer or program manager can be aligned with the role of system owner; and the role of mission or business owner can be aligned with the role of authorizing official. NIST Special Publication 800-64 provides guidance on information security in the SDLC.

[91] 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.

Commented [A17]: SP 800-37 Rev. 1 did not list the roles in alphabetical order.

Formatted: Right: 0"

Authorizing officials coordinate their activities with common control providers, system owners, chief information officers, senior agency information security officers, senior agency officials 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 co-authorizing officials.[92] If so, agreements are established between the co-authorizing officials and documented in the security and privacy plans. Authorizing officials are responsible and accountable for ensuring that activities and functions associated with authorization that are delegated to authorizing official designated representatives are carried out as specified. The role of authorizing official is an inherent U.S. Government function and is assigned to government personnel only.

AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE

The *authorizing official designated representative* is an organizational official designated by the authorizing official who is empowered to act on behalf of the authorizing official to coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations. ~~Authorizing official designated representatives can be empowered by authorizing officials to make certain decisions with regard to the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring the implementation of plans of action and milestones, and the assessment and/or determination of risk. The designated representative may also be called upon to prepare the final authorization package, obtain the authorizing official's signature on the authorization decision document, and transmit the authorization package to appropriate organizational officials.~~ This includes carrying out many of the activities related to the execution of the RMF. The only activity that cannot be delegated by the authorizing official to the designated representative is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk~~to organizational operations and assets, individuals, other organizations, and the Nation~~).

CHIEF INFORMATION OFFICER

The *chief information officer*[93] 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 and supply chain risk management considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, the SDLC, and acquisitions;

[92] OMB Circular A-130 provides additional information about authorizing officials and co-authorizing officials.

[93] 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.

- 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 information systems that process personally identifiable information, the chief information officer and authorizing officials coordinate any determination about the allocation of resources dedicated to the protection of those information systems with the senior agency official for privacy. 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 is an inherent U.S. Government function and is assigned to government personnel only.

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., controls inherited by organizational systems).[94] Common control providers also are responsible for ensuring the documentation of organization-defined common controls in security and privacy plans (or the 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 control assessment reports; and producing plans of action and milestones for controls having deficiencies. Security and privacy plans, security and privacy assessment reports, and plans of action and milestones for common controls (or summary of such information) are made available to the system owners of systems inheriting common controls after the information is reviewed and approved by the authorizing officials accountable for those common controls.

The senior agency official for privacy is responsible for designating which privacy controls may be treated as common controls. Privacy controls that are designated as common controls are documented in the organization's privacy program plan.[95] The senior agency official for privacy has oversight responsibility for common controls in place or planned for meeting applicable privacy requirements and managing privacy risks and is responsible for assessing those controls. At the discretion of the organization, privacy controls that are designated as common controls may be assessed by an independent assessor. In all cases, however, the senior agency official for privacy retains responsibility and accountability for the organization's privacy program, including any privacy functions performed by independent assessors. Privacy plans and privacy control

[94] 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.

[95] A privacy program plan is a formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program; the role of the Senior Agency Official for Privacy and other privacy officials and staff; the strategic goals and objectives of the privacy program; the resources dedicated to the privacy program; and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

assessment reports are made available to systems owners whose systems inherit privacy controls that are designated as common 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 controls and control enhancements implemented within or inherited by a system to determine the effectiveness of the controls (i.e., 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). ~~The system owner and common control provider rely on the security and privacy expertise and judgment of the assessor to assess the controls implemented within and inherited by the system using the assessment procedures specified in the security and privacy assessment plans. Multiple control assessors who are differentiated by their expertise in specific control requirements or technologies may be required to accurately conduct the assessment. Prior to initiating the control assessment, assessors review the security and privacy plans to facilitate development of the security assessment plan.~~ Control assessors provide an assessment of the severity of the deficiencies discovered in the system and its environment of operation and can recommend corrective actions to address identified vulnerabilities. Finally, control assessors prepare security and privacy assessment reports containing the results and findings from the assessment.

The required level of assessor independence is determined by the conditions of the 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.~~ When a security control 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 an impartial and unbiased 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 information system owner and common control provider rely on the security expertise and the technical judgment of the assessor to: (i) assess the security controls employed within and inherited by the information system using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and address identified vulnerabilities.~~

The senior agency official for privacy is responsible for assessing privacy controls and for providing privacy-related information to the authorizing official. At the discretion of the organization, privacy controls may be assessed by an independent assessor. In all cases, however, the senior agency official for privacy retains responsibility and accountability for the privacy program of the organization, including any privacy functions performed by the independent assessors.

ENTERPRISE ARCHITECT

The *enterprise architect* is an individual or group responsible for working with the leadership and subject matter experts in an organization to build a holistic view of the organization's missions and business functions, mission/business processes, information, and information technology assets. With respect to information security and privacy, enterprise architects:

- Implement an enterprise architecture strategy that facilitates effective security and privacy solutions;
- Coordinate with security and privacy architects to determine the optimal placement of systems/system elements within the enterprise architecture and to address security and privacy issues between systems and the enterprise architecture;
- Assist in reducing complexity within the IT infrastructure to facilitate security;
- Assist with determining appropriate control implementations and initial configuration baselines as they relate to the enterprise architecture;
- Collaborate with system owners and authorizing officials to facilitate authorization boundary determinations and allocation of controls to system elements;
- Serve as part of the Risk Executive (function); andAssist with integration of the organizational risk management strategy and system-level security and privacy requirements into program, planning, and budgeting activities, the SDLC, acquisition processes, and systems engineering processes.

HEAD OF AGENCY

The *head of agency* is the senior official in an organization with the responsibility for ensuring that privacy interests are protected and that PII is managed responsibly within the organization. The agency head is ~~the highest-level senior official or executive within an organization with the overall responsibility to also~~ also responsible for providing security protections commensurate with the risk to organizational operations, organizational 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 the information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. The heads of agencies ensure that:

- Information security and privacy 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;
- Senior agency officials for privacy are designated who are responsible and accountable for ensuring compliance with applicable privacy requirements, managing privacy risk, and the organization's privacy program; and
- The organization has adequately trained personnel to assist in complying with security and privacy requirements in legislation, executive orders, policies, directives, instructions, standards, and guidelines.

The head of agency establishes the organizational commitment to security and privacy and the actions required to effectively manage security and privacy risk and protect the missions and business functions being carried out by the organization. The head of agency or establishes

security and privacy accountability and provides active support and oversight of monitoring and improvement for the security and privacy programs. Senior leadership commitment to security and privacy 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 or 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 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 establishing 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 risk management strategy, play an active part in the SDLC, and may also serve in the role of authorizing official.

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 officers, and any other stakeholders having a vested interest in the mission/business success of organizations.

The risk executive (function) ensures that risk-related considerations for systems (including authorization decisions for those systems and the common controls inherited by those systems), are viewed from an organization-wide perspective regarding the organization's strategic goals and objectives in carrying out its core missions and business functions. The risk executive (function) ensures that managing risk is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risk to ensure mission/business success.

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 provides a strategic view of security-related risks for the organization[96] and that guides and informs organizational risk decisions (including how risk is framed, assessed, responded to, and monitored over time);
- Provide a comprehensive, organization-wide, holistic approach for addressing risk—an approach that provides a greater understanding of the integrated operations of the organization;
- 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);
- Identify the organizational risk posture based on the aggregated risk from the operation and use of systems and the respective environments of operation for which the organization is responsible;
- Provide oversight for the risk management activities carried out by organizations to help 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 (e.g., authorization officials and other senior leaders) 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 authorizations);
- 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;
- 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,

[96] 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.

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.

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 controls~~as system-specific, hybrid, or common controls~~. Security or privacy architects, in coordination with system security or privacy officers, advise authorizing officials, chief information officers, senior accountable officials for risk management or risk executive (function), senior agency information security officers, and senior agency officials for privacy on a range of security and privacy issues. Examples include establishing authorization boundaries; establishing security or privacy alerts; assessing the severity of deficiencies in the system or controls; developing effective plans of action and milestones; creating risk mitigation approaches; and potential adverse effects of identified vulnerabilities or privacy risks.

SENIOR ACCOUNTABLE OFFICIAL FOR RISK MANAGEMENT

The *senior accountable official for risk management* is the individual that leads and manages the risk executive (function) in an organization and is responsible for aligning information security management processes with strategic, operational, and budgetary planning processes. This official is the agency head or an individual designated by the agency head.

The senior accountable official for risk management determines the organizational structure and responsibilities of the risk executive (function). The head of the agency, in coordination with the senior accountable official for risk management, may retain the risk executive (function) or delegate the function to another organizational official or group. The senior accountable official for risk management and the risk executive (function) are inherent U.S. Government functions 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 achieving 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 is an inherent U.S. Government function 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 the senior official or executive with agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risk. Among other things, the senior agency official for privacy is responsible for: coordinating with the senior agency information security officer to ensure coordination of privacy and information security activities; reviewing and approving the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information; designating which privacy controls will be treated as program management, common, system-specific, and hybrid privacy controls; identifying assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks; reviewing and approving privacy plans for information systems prior to authorization, reauthorization, or ongoing authorization; reviewing authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information to ensure compliance with privacy requirements and manage privacy risks; conducting and documenting the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency; and establishing and maintaining a privacy continuous monitoring program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with privacy requirements and manage privacy risks.

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 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 a system.[97] 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 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)[98] 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

[97] Organizations may refer to system owners as program managers or business/asset owners.

[98] 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.

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.[99]

SYSTEM SECURITY OR PRIVACY OFFICER

The *system security or privacy officer*[100] is an individual responsible for ensuring that the security and privacy posture is maintained for an organizational system and 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 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 system-level 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 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 SDLC. Systems security and privacy engineering is a process that captures and refines security or privacy requirements for systems and helps to ensure that the requirements are effectively integrated into systems and system components through 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 controls within a system including software engineering methodologies; system and security or privacy engineering

[99] 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.

[100] 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.

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.

APPENDIX E

SUMMARY OF RMF TASKS

RMF TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

Commented [A18]: Changes are not tracked in this Appendix.

TABLE E-1: PREPARE TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
Organization Level		
TASK 1 **Risk Management Roles** Identify and assign individuals to specific roles associated with security and privacy risk management.	• Head of Agency • Chief Information Officer • Senior Agency Official for Privacy	• Authorizing Official or Authorizing Official Designated Representative • Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer
TASK 2 **Risk Management Strategy** Establish a risk management strategy for the organization that includes a determination of risk tolerance.	• Head of Agency	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 3 **Risk Assessment—Organization** Assess organization-wide security and privacy risk and update the results on an ongoing basis.	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy	• Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative
TASK 4 **Organization-Wide Tailored Control Baselines and Profiles (Optional)** Establish, document, and publish organization-wide tailored control baselines and/or profiles.	• Mission or Business Owner • Senior Accountable Official for Risk Management or Risk Executive (Function)	• Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 5 **Common Control Identification** Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.	• Senior Agency Information Security Officer • Senior Agency Official for Privacy	• Mission or Business Owner • Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative • Common Control Provider • System Owner

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 6 **Impact-Level Prioritization (Optional)** Prioritize organizational systems with the same impact level.	• Senior Accountable Official for Risk Management or Risk Executive (Function)	• Senior Agency Information Security Officer • Senior Agency Official for Privacy • Mission or Business Owner • System Owner • Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative
TASK 7 **Continuous Monitoring Strategy—Organization** Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Official for Privacy	• Chief Information Officer • Senior Agency Information Security Officer • Mission or Business Owner • System Owner • Authorizing Official or Authorizing Official Designated Representative
System Level		
TASK 1 **Mission or Business Focus** Identify the missions, business functions, and mission/business processes that the system is intended to support.	• Mission or Business Owner	• Authorizing Official or Authorizing Official Designated Representative • System Owner • Information Owner or Steward • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 2 **Organizational Stakeholders** Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.	• System Owner	• Authorizing Official or Authorizing Official Designated Representative • Mission or Business Owner • Information Owner or Steward • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 3 **Asset Identification** Identify assets that require protection.	• System Owner	• Authorizing Official or Authorizing Official Designated Representative • Mission or Business Owner • Information Owner or Steward • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 4 **Authorization Boundary** Determine the authorization boundary of the system.	• System Owner	• Chief Information Officer • Mission or Business Owner • Authorizing Official or Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Enterprise Architect

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 5 **Information Types** Identify the types of information to be processed, stored, and transmitted by the system.	• System Owner • Information Owner or Steward	• System Security or Privacy Officer • Mission or Business Owner
TASK 6 **Information Life Cycle** For systems that process PII, identify and understand all parts of the information life cycle.	• Senior Agency Official for Privacy • System Owner • Information Owner or Steward	• Chief Information Officer • Mission or Business Owner
TASK 7 **Risk Assessment (System)** Conduct a system-level risk assessment and update the risk assessment on an ongoing basis.	• System Owner • System Security or Privacy Officer	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Authorizing Official or Authorizing Official Designated Representative • Mission or Business Owner • Information Owner or Steward
TASK 8 **Protection Needs—Security and Privacy Requirements** Define the protection needs and security and privacy requirements for the system.	• Mission or Business Owner • System Owner • Information Owner or Steward • System Security or Privacy Officer	• Authorizing Official or Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 9 **Enterprise Architecture** Determine the placement of the system within the enterprise architecture.	• Mission or Business Owner • Enterprise Architect • Security or Privacy Architect	• Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner • Information Owner or Steward
TASK 10 **System Registration** Register the system with organizational program or management offices.	• System Owner	• Mission or Business Owner • Chief Information Officer • System Security or Privacy Officer

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

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **Security Categorization** Categorize the system and document the security categorization results.	• System Owner • Information Owner or Steward	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Authorizing Official or Authorizing Official Designated Representative • System Security or Privacy Officer
TASK 2 **Security Categorization Review and Approval** Review and approve the security categorization results and decision.	• Authorizing Official or Authorizing Official Designated Representative • Senior Agency Official for Privacy (for systems processing PII}	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 3 **System Description** Document the characteristics of the system.	• System Owner	• Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • System Security or Privacy Officer

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

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **Security and Privacy Requirements Allocation** Allocate security and privacy requirements to the information system and to the environment in which the system operates.	• Security Architect • Privacy Architect or System Privacy Officer	• Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative • Mission or Business Owner • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner
TASK 2 **Control Selection** Select the controls for the system.	• System Owner • Common Control Provider	• Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Systems Security or Privacy Engineer • System Security or Privacy Officer
TASK 3 **Control Tailoring** Tailor the controls selected for the system.	• System Owner • Common Control Provider	• Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Systems Security or Privacy Engineer • System Security or Privacy Officer
TASK 4 **Security and Privacy Plans** Document the security and privacy controls for the system in security and privacy plans.	• System Owner • Common Control Provider	• Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Systems Security or Privacy Engineer • System Security or Privacy Officer
TASK 5 **Continuous Monitoring Strategy—System** Develop and implement a system-level strategy for monitoring control effectiveness to supplement the organizational continuous monitoring strategy	• System Owner • Common Control Provider	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Security or Privacy Architect • Systems Security or Privacy Engineer • System Security or Privacy Officer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 6 **Security and Privacy Plan Review and Approval** Review and approve the security and privacy plans for the system.	• Authorizing Official or Authorizing Official Designated Representative	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy.

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

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

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

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **Assessor Selection** Select the appropriate assessor or assessment team for the type of assessment to be conducted.	• Authorizing Official or Authorizing Official Designated Representative • Senior Agency Official for Privacy	• Senior Agency Information Security Officer
TASK 2 **Assessment Plan** Develop, review, and approve plans to assess implemented controls.	• Authorizing Official or Authorizing Official Designated Representative • Control Assessor	• Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner • Common Control Provider • Information Owner or Steward • System Security or Privacy Officer
TASK 3 **Control Assessments** Assess the security and privacy controls in accordance with the assessment procedures described in the security and privacy assessment plans.	• Control Assessor	• Authorizing Official or Authorizing Official Designated Representative • System Owner • Common Control Provider • Information Owner or Steward • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Security or Privacy Officer
TASK 4 **Security and Privacy Assessment Reports** Prepare the security and privacy assessment reports documenting the findings and recommendations from the control assessments.	• Control Assessor	• System Owner • Common Control Provider • System Security or Privacy Officer
TASK 5 **Remediation Actions** Conduct initial remediation actions on the 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 Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner • Common Control Provider • Information Owner or Steward • Systems Security or Privacy Engineer • System Security or Privacy Officer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 6 **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 initial remediation actions taken.	• System Owner • Common Control Provider	• Information Owner or Steward • System Security or Privacy Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy

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

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **Authorization Package** Assemble the authorization package and submit the package to the authorizing official for an authorization decision.	• System Owner • Common Control Provider	• System Security or Privacy Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Control Assessor
TASK 2 **Risk Analysis and Determination** Analyze and determine the risk from the operation or use of the system or the provision of common controls.	• Authorizing Official or Authorizing Official Designated Representative	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 3 **Risk Response** Identify and implement a preferred course of action in response to the risk determined.	• Authorizing Official or Authorizing Official Designated Representative	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner or Common Control Provider • Information Owner or Steward • Systems Security or Privacy Engineer • System Security or Privacy Officer
TASK 4 **Authorization Decision** Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable.	• Authorizing Official	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Authorizing Official Designated Representative
TASK 5 **Authorization Reporting** Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.	• Authorizing Official or Authorizing Official Designated Representative	• System Owner or Common Control Provider • Information Owner or Steward • System Security or Privacy Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy

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

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 1 **System and Environment Changes** Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.	• System Owner or Common Control Provider • Senior Agency Information Security Officer • Senior Agency Official for Privacy	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • System Security or Privacy Officer
TASK 2 **Ongoing Assessments** Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy.	• Control Assessor	• Authorizing Official or Authorizing Official Designated Representative • System Owner or Common Control Provider • Information Owner or Steward • System Security or Privacy Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
TASK 3 **Ongoing Risk Response** Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones.	• Authorizing Official • System Owner • Common Control Provider	• Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy; Authorizing Official Designated Representative • Information Owner or Steward • System Security or Privacy Officer • Systems Security or Privacy Engineer • Security or Privacy Architect
TASK 4 **Authorization Updates** 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.	• System Owner • Common Control Provider	• Information Owner or Steward • System Security or Privacy Officer • Senior Agency Official for Privacy
TASK 5 **Security and Privacy Posture Reporting** Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.	• System Owner • Common Control Provider • Senior Agency Information Security Officer • Senior Agency Official for Privacy	• System Security or Privacy Officer

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

APPENDIX F

SYSTEM AND COMMON CONTROL ~~SECURITY~~ 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 posture of information systems 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 in an authorization package, which may consist of a report from an automated security/privacy management and reporting tool.[101] System and common control authorization occurs as part of the RMF *Authorize* step. A system authorization or a common control authorization can be an initial authorization, an 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 complete, zero-base review of the system or of common controls. The zero-base review of the system includes an assessment of all implemented system-level controls (including the system-level portion of the hybrid controls) and a review of the security status of inherited common controls as specified in security and privacy plans.[102] The zero-base review of common controls (other than common controls that are system-based) includes an assessment of all applicable controls (e.g., policies, operating procedures, implementation information) that contribute to the provision of a common control or set of common controls.
- *Ongoing authorization* is defined as the subsequent (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 and privacy posture of the system to determine whether the mission/business risk of continued system operation or the provision of common controls is acceptable. Ongoing

[101] 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.

[102] The zero-base review of a system does not require a zero-base review of the common controls that are available for inheritance by that system. The common controls are authorized under a separate authorization process with a separate authorization official accepting the risk associated with the provision of those controls. The review of the security and privacy plans containing common controls is necessary to understand the current state of the controls being inherited by organizational systems and factoring this information into risk-based decisions associated with the system.

authorization is fundamentally related to the ongoing understanding and ongoing acceptance of security and privacy risk and 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 may be time-driven or event-driven. However, under ongoing authorization, reauthorization is in most instances, an event-driven action initiated by the authorizing official or directed by the senior accountable official for risk management or risk executive (function) in response to an event that results in security and/or privacy risk above the level of risk previously accepted by the authorizing official. Reauthorization consists of a review of the system or the common controls similar to the review carried out during the initial authorization. The reauthorization differs from the initial authorization because the authorizing official can choose to initiate a complete zero-base review of the system or of the common controls or to initiate a targeted review based on the type of event that triggered the reauthorization. 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 be leveraged to support reauthorization. Reauthorization actions may necessitate a review of and changes to the organization's information security and privacy continuous monitoring strategies which may in turn affect ongoing authorization.

AUTHORIZATION PACKAGE

The *authorization package* provides a record of the results of the 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 common controls.[103] ~~Unless specifically designated otherwise by the chief information officer or authorizing official,~~ The system owner or common control provider is responsible for the development, compilation, and submission of the authorization package. This includes information 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: senior agency information security officer; senior agency official for privacy, senior accountable official for risk management or risk executive (function); control assessors; system security or privacy officer; and the continuous monitoring program. The authorization package[104] includes the following:

- Executive summary;
- Security and privacy plans;[105]
- Security and privacy assessment reports;[106] and
- Plans of action and milestones.

The executive summary provides a consolidated view of the security- and privacy-related information in the authorization package. The executive summary helps to identify and highlight

[103] Authorization packages for common controls that are not system-based may not include a security or privacy plan, but do include a record of common control implementation details.

[104] The authorizing official determines what additional supporting information or references may be required to be included in the authorization package.

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

[106] 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.

risk management issues associated with protecting organizational systems and the environments in which the systems operate. It 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.

The security and privacy plans~~, prepared by the information system owner or common control provider~~, provide an overview of the security and privacy requirements and describe the controls in place or planned for meeting those requirements. The plans provide sufficient information to understand the intended or actual implementation of the controls implemented within the system ~~or inherited by the information system.~~and indicate the controls that are implemented via inherited common controls. Additionally, privacy plans specifically describe the methodologies and metrics that will be used to assess the controls. The security and privacy plans may also include as supporting appendices or as references, additional security~~-~~ and privacy-related documents such as a privacy impact assessment, interconnection security agreements, security and privacy configurations, contingency plan, configuration management plan, incident response plan, and system-level continuous monitoring strategy. ~~In accordance with the *near real-time* risk management objectives of the security authorization process, the security plan is updated whenever events dictate changes to the security controls employed within or inherited by the information system. Updates to the security plan may be triggered by a variety of events, including for example: (i) a vulnerability scan of the information system or vulnerability assessment of the environment of operation; (ii) new threat information; (iii) weaknesses or deficiencies discovered in currently deployed security controls after an information system breach; (iv) a redefinition of mission priorities or business objectives invalidating the results of the previous security categorization process; and (v) a change in the information system (e.g., adding new hardware, software, or firmware; establishing new connections) or its environment of operation (e.g., moving to a new facility).~~ The security and privacy plans are updated whenever events dictate changes to the controls implemented within or inherited by the system.

The security and privacy assessment reports, prepared by the control assessor or generated by automated security/privacy management and reporting tools, provide 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 deficiencies identified in the security and privacy controls.[107] ~~Updates to the security assessment report help to ensure that the information system owner, common control provider, and authorizing officials maintain the appropriate awareness with regard to security control effectiveness. The overall effectiveness of the security controls directly affects the ultimate security state of the information system and decisions regarding explicit acceptance of risk.~~

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

[107] 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 deficiencies in the security and privacy controls.

made to the security and privacy controls implemented within or inherited by the system.[108] Updates to the assessment reports help to ensure that system owners, common control providers, and authorizing officials maintain an awareness of control effectiveness. The effectiveness of the security and privacy controls directly affects the security and privacy posture 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 deficiencies identified in the security and privacy controls during the assessment; and to address known vulnerabilities or privacy risks in the system.[109] The content and structure of plans of action and milestones are informed by the 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, ~~memoranda, or regulations~~ or standards. If the 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. ~~The most effective plans of action and milestones contain a robust set of actual weaknesses or deficiencies identified in the security controls employed within or inherited by the information system. Assuming that most information systems and the environments in which those systems are deployed, have more vulnerabilities than available resources can realistically address, organizations define a strategy for developing and implementing plans of action and milestones that facilitates 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 deficiencies in the controls;
- The criticality of the control deficiencies (i.e., the direct or indirect effect the deficiencies may have on the overall security and privacy posture of the system and hence on the risk exposure[110] of the organization);
- The risk mitigation approach of the organization to address the identified deficiencies in the controls; and
- The rationale for accepting certain deficiencies in the controls.

Organizational strategies for plans of action and milestones are guided and informed by the security categorization of the 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 known deficiencies in those systems or assets could potentially have the most significant adverse effects on their missions or business functions. Organizations prioritize deficiencies using information from risk assessments and the risk management strategy developed as part of the risk executive (function). Therefore, a high-impact system would have a prioritized list of deficiencies for that system, and similarly for

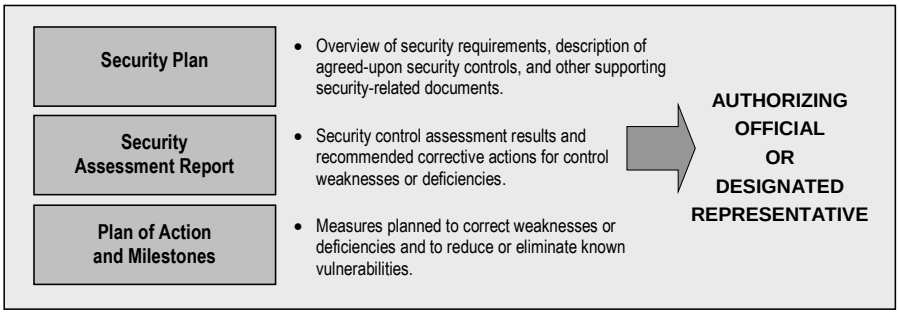
[108] Because the desired outcome of ongoing tracking and response to assessment findings to facilitate risk management decisions is the focus (rather than the specific process used), organizations have the flexibility to manage and update security assessment report information using any format or method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

[109] Implementation information about mitigation actions from plans of actions and milestones is documented in the system security plan.

[110] 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.

moderate-impact and low-impact systems. ~~In general, the plan of action and milestones strategy always addresses the highest-priority weaknesses or deficiencies within those prioritized systems.~~

~~After completion of the security plan, security assessment report, and plan of action and milestones, the information system owner or common control provider submits the final security authorization package to the authorizing official or designated representative. Figure F-1 illustrates the key sections of the authorization package.~~



~~**FIGURE F-1: SECURITY AUTHORIZATION PACKAGE**~~

AUTHORIZATION DECISIONS

Authorization decisions are based on the content of the authorization package ~~including inputs from the organization's risk executive (function) and any additional supporting documentation required by the authorizing official. The security authorization package provides comprehensive information on the security state of the information system. Risk executive (function) inputs, including the previously established overarching risk guidance derived from the risk management strategy, provide additional information to the authorizing official that may be relevant and affect the final authorization decision (e.g., organizational risk tolerance, organization's overall risk mitigation strategy, core mission and business requirements, dependencies among information systems, ongoing risk monitoring requirements, and other types of risks not directly associated with the information system or its environment of operation). Risk executive (function) inputs are documented and become part of the authorization decision. Organizations determine how the risk management strategy and risk-related guidance from the risk executive (function) influences/impacts the authorization decisions of authorizing officials. Security authorization decisions are conveyed to information system owners and common control providers and are made available to selected officials within the organization (e.g., information system owners inheriting common controls, authorizing officials for interconnected systems, chief information officers, senior information security officers, information owners/stewards). There are two types of authorization decisions that can be rendered by authorizing officials:~~ There are four types of authorization decisions that can be rendered by authorizing officials:

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

Authorization to Operate

If the authorizing official, after reviewing the authorization package ~~and any additional inputs provided by the risk executive (function),~~ 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 information system~~or for the common controls inherited by organizational information systems~~. The system is authorized to operate for a specified period in accordance with the terms and conditions established by the authorizing official. ~~For common control providers external to an information system, the authorization decision means that the common controls under their control are approved for *inheritance* by organizational information systems.~~An *authorization termination date* is established by the authorizing official as a condition of the authorization. The authorization termination date can be adjusted at any time by the authorizing official to reflect an increased level of concern regarding the security and privacy posture of the system. For example, the authorizing official may choose to authorize the system to operate only for a short time if it is necessary to test a system in the operational environment before all controls are fully in place, (i.e., the authorization to operate is strictly limited to the time needed to complete the testing objectives).[111] The authorizing official may choose to include operating restrictions such as limiting logical and physical access to a minimum number of users; restricting system use time periods; employing enhanced or increased audit logging, scanning, and monitoring; or restricting system functionality to include only the functions that require live testing.

The authorizing official considers results from the assessment of controls that are fully or partially implemented since if the system is ready to be tested in a live environment, many of the controls should already be in place. 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.[112] ~~The authorizing official takes specific actions to reduce or eliminate vulnerabilities identified during the execution of the Risk Management Framework unless the vulnerabilities have been explicitly accepted as part of the authorization decision. In addition, the information system owner or common control provider establishes a disciplined, structured, and repeatable process to monitor the ongoing effectiveness of the deployed security controls and the progress of any actions taken to correct or eliminate weaknesses or deficiencies. The plan of action and milestones submitted by the information system owner is used by the authorizing official to monitor the progress in correcting deficiencies and weaknesses noted during the security control assessment.~~

Common Control Authorization

A *common control authorization* is similar to an authorization to operate for systems. If the authorizing official, after reviewing the authorization package submitted by the common control provider, determines that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable, a common control authorization is issued. It is the responsibility of common control providers to indicate that the common controls selected by the organization have been implemented, assessed, and authorized and are available for inheritance by the organizational systems. Common control providers are also responsible for ensuring that the system owners inheriting the controls have access to appropriate documentation and tools.

Common controls are authorized for a specific time period in accordance with the terms and conditions established by the authorizing official and the organization. An *authorization*

[111] Formerly referred to as an interim authority to test.
[112] Additional information on event-driven triggers is provided below.

termination date is established by the authorizing official as a condition of the initial common control authorization. The termination date can be adjusted at any time to reflect the level of concern by the authorizing official regarding the security and privacy posture of the common controls that are available for inheritance. If the controls are under ongoing authorization, a time-driven authorization frequency is specified. Within any authorization type, an adverse event could occur that triggers the need to review the common control authorization. Common controls that are implemented in a system do not require a separate common control authorization because they receive an authorization to operate as part of the system authorization to operate.[113]

Authorization to Use

Commented [A19]: The content of this section is based on the 800-37 Rev. 1 concept of legeraged authorization.

An *authorization to use* applies to cloud and shared systems, services, and applications and 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).[114] An authorization to use is issued by a designated authorizing official from the customer organization in lieu of an authorization to operate. The authorizing official issuing an authorization to use has the same level of risk management responsibility and authority as an authorizing official issuing an authorization to operate or a common control authorization.[115]

The acceptance of the information in the authorization package from the provider organization is based on a need to use shared information technology resources, including for example, a system, an application, or a service. A customer organization can issue an authorization to use only after a valid authorization to operate has been issued by the provider organization.[116] The provider organization's authorization (to operate) is a statement of the acceptance of risk for the system, service, or application being provided. The customer organization's 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. 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 organization as the fundamental basis for determining risk.[117] When reviewing the authorization package, the customer organization considers various risk factors such as the

[113] In certain situations, system owners may inherit 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 controls is also made aware of the inheritance.

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

[115] 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.

[116] 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.

[117] 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).

time elapsed since the authorization results were produced; the environment of operation (if different from the environment reflected in the authorization package); the impact level of the information to be 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 risk in doing so.

If the customer organization determines that there is insufficient information in the provider authorization package or inadequate controls in place for establishing an acceptable level of risk, the organization may negotiate with the provider organization and request additional controls or security- and privacy-related information. This may include for example, supplementing controls for risk reduction; implementing compensating controls; conducting additional or more rigorous assessments; or establishing constraints on the use of the system, application, or service provided. The request for additional security- and privacy-related information may include information the provider organization produced or discovered in the use of the system that is not reflected in the authorization package. When the provider organization does not provide the requested 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 shared or cloud system, application, or service (as reflected in the current authorization package) and the risk of using the shared or cloud system, application, or service has been sufficiently mitigated, 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.[118] 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 does not require a termination date, but remains in effect while the customer organization continues to accept the security and privacy risk of using the shared or cloud system, application, or service; and the authorization to operate issued by the provider organization meets the requirements established by federal and organizational policies. It is incumbent on the customer organization to ensure that information from the monitoring activities conducted by the provider organization is shared on an ongoing basis and that the provider organization notifies the customer organization when there are significant changes to the system, application, or service that may affect the security and privacy posture of the provider. If desired, the authorization to use decision may specify 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. It is incumbent on the provider organization to notify the customer organization if there is a significant event that compromises or adversely affects the customer organization's information.

Figure F-1 illustrates the types of authorization decisions that can be applied to organizational systems and common controls and the risk management roles in the authorization process.

[118] 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.

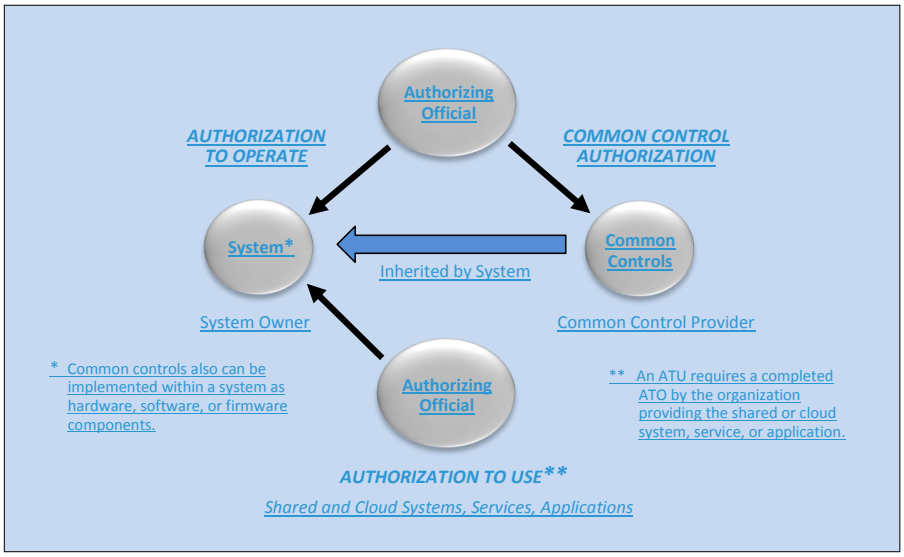


FIGURE F-1: TYPES OF AUTHORIZATION DECISIONS

Denial of Authorization ~~to Operate~~

If the authorizing official, after reviewing the authorization package, including any inputs provided by the senior accountable official for risk management or 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 information system is not authorized to operate and not placed into operation; common controls are not authorized to be provided to systems; or that the provider's system is not authorized for use by the customer organization. If the system is currently in operation, all activity is halted. ~~For common control providers external to an information system, the authorization decision means that the common controls under their control are *not* approved for *inheritance* by organizational information systems.~~ Failure to receive an authorization means that there are significant deficiencies in the controls. The authorizing official or designated representative works with the system owner or the common control provider to revise the plan of action and milestones to help ensure that measures are taken to correct the deficiencies. A special case of authorization denial is an *authorization rescission*. Authorizing officials can rescind a previous authorization decision 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.

AUTHORIZATION DECISION DOCUMENT

The authorization decision is transmitted from the authorizing official to system owners, common control providers, and other key organizational officials. The authorization decision includes the following information:

- Authorization decision;
- Terms and conditions for the authorization;
- ~~Authorization termination date; and~~
- ~~Risk executive (function) input (if provided).~~
- Time-driven authorization frequency or authorization termination date;
- Events that may trigger a review of the authorization decision (if any); and
- For common controls, the FIPS Publication 199 impact level supported by those controls.

The authorization decision indicates if the system is authorized to operate or authorized to be used; or if the common controls are authorized to be provided to system owners and inherited by organizational systems. ~~For common controls, the authorization decision means that the controls are approved for *inheritance* by organizational information 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. ~~The *authorization termination date*, established by the authorizing official, indicates when the security authorization expires and reauthorization is required. An authorizing official designated representative prepares the authorization decision document for the authorizing official with authorization recommendations, as appropriate. The authorization decision document is attached to the original authorization package and transmitted to the information system owner or common control provider.~~[119] 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 transmitted with the original authorization package to the system owner or common control provider.[120]

Upon receipt of the authorization decision and authorization package, the system owner and common control provider acknowledge, implement, and comply with the terms and conditions of the authorization~~and notifies the authorizing official~~. The system owner and common control provider retain the authorization decision and authorization package.[121] The organization ensures that authorization documents are available to organizational officials ~~(e.g., information system owners inheriting common controls, the risk executive [function], chief information officers, senior information security officers, information system security officers)~~ when requested. The contents of authorization ~~documentation~~ packages, including sensitive information regarding system vulnerabilities, privacy risks, and control deficiencies, are marked and protected in accordance with federal and organizational policy. Authorization decision 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

~~[119] Authorization decision documents may be digitally signed to ensure authenticity.~~

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

[121] 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.

The authorization to use is a streamlined version of the authorization to operate and includes:

- A risk acceptance statement; and
- Time- or event-driven triggers for review of the security and privacy posture of the provider organization shared cloud or system, application, or service (if any).

An authorization to use is issued by an authorizing official from a customer organization in lieu of an authorization to operate. The authorizing official has the same level of risk management responsibility and authority as an authorizing official issuing an authorization to operate or a common control authorization. The risk acceptance statement indicates 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 or cloud system, service, or application.

ONGOING AUTHORIZATION

Continuous monitoring strategies[122] promote effective and efficient 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 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 the current security and privacy posture of the system.[123] It also highlights the risks to organizational operations and assets, individuals, other organizations, and the Nation. Ultimately, continuous monitoring guides and informs the authorizing official's decision whether to authorize the continued operation of the system or the continued use of the 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 and privacy posture 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. Reauthorizations are unnecessary in situations where the continuous monitoring program provides authorizing officials with the information necessary to manage the risk arising from changes to the system or the environment in which the system operates. If a reauthorization is required, organizations maximize the use of status reports and relevant information about the security and privacy posture of the system that is produced during the continuous monitoring process to improve efficiency.

When a system or common controls are under ongoing authorization, the system or common controls may be authorized on a time-driven and/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 organization- and system-level continuous monitoring strategies. The system and common controls are authorized on an event-driven basis when organizational-defined trigger events occur. Whether the authorization is time-driven or event-driven, the authorizing official acknowledges the ongoing acceptance of identified risks. The

[122] 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.

[123] For greater efficiency, the information security continuous monitoring (ISCM) and privacy continuous monitoring (PCM) strategies may be consolidated into a single unified continuous monitoring strategy. Similarly, the ISCM and PCM programs may also be consolidated into a single unified continuous monitoring program.

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, systems may transition from a static, point-in-time authorization process to a dynamic, near real-time ongoing authorization process. To do so, the following conditions must be satisfied:

- The system or common control being considered for ongoing authorization has received an initial authorization based on a complete, zero-base review of the system or the common controls.[124]
- An organizational continuous monitoring program is in place that monitors implemented 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 standards and guidelines.[125]

The organization establishes and implements a process to designate that the two conditions are satisfied and the system or the common controls are transitioning to ongoing authorization. This includes the authorizing official acknowledging that the system or common control are now being managed by an ongoing authorization process and accepting the responsibility for performing all activities associated with that process. The transition to ongoing authorization is documented by the authorizing official by issuing a new authorization decision.[126] 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 and privacy 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 controls is generated and collected at the frequency specified in the organization's continuous monitoring strategy. This information may be collected using automated tools or other methods of assessment depending on the type and purpose of the control and desired rigor of the assessment. Automated tools may not generate security- and privacy-related information that is sufficient to support the authorizing official in making risk determinations. This may occur for various reasons, including for example, the tools do not generate information for every control or every part of a control; additional assurance is needed; or the tools do not generate information on specific technologies or platforms. In such cases, manual control assessments are conducted at organizationally-determined frequencies to cover any gaps in automated security- and privacy-related information

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

[125] 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 Special Publication 800-53A will address privacy assessments.

[126] 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.

generation. The manually-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 in an automated fashion, is produced and analyzed by an entity that meets the independence requirements established by the organization. The senior agency official for privacy is responsible for assessing privacy controls and for providing privacy-related information to the authorizing official. At the discretion of the organization, privacy controls may be assessed by an independent assessor. The independent assessor is impartial and free from any perceived or actual conflicts of interest regarding the development, implementation, assessment, operation, or 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-established frequency. This reinforces the concept of ongoing authorization. In accordance with CA-6 (along with the security and privacy assessment and monitoring frequency determinations established as part of the continuous monitoring strategy), organizations determine a frequency with which authorizing officials review security- and privacy-related information via the security or privacy management and reporting tool or manual process.[127] This near real-time information is used to determine whether the mission or business risk of operating the system or providing the common controls continues to be acceptable. NIST Special Publication 800-137 provides criteria for determining assessment and monitoring frequencies.

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. The organizational continuous monitoring process, supported by the organization's security and 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

[127] *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 risk), organizations must have in place, an organization-level and system-level continuous monitoring process to assess implemented controls on an ongoing basis. The findings or results from the continuous monitoring process provides information to authorization officials to support near-real time risk-based decision making.

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. At any time, the authorizing official may also determine independently that an immediate review is required. This review is conducted in addition to the time-driven frequency review defined in the organizational continuous monitoring strategy and occurs during ongoing authorization when the residual risk remains within the acceptable limits of organizational risk tolerance.[128]

Transitioning from Static Authorization to Ongoing Authorization

The intent of continuous monitoring is to monitor controls at a frequency that is sufficient to provide authorizing officials with the information necessary to make effective, risk-based decisions, whether by automated or manual means.[129] However, if a substantial portion of monitoring is not accomplished via automation, it will not be feasible or practical 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 controls are monitored by automated techniques. Organizations may begin by generating security- and privacy-related information from automated tools and fill in gaps by generating additional information from manual assessments. As additional automated monitoring functionality is added, processes can be adjusted.

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 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

[128] 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.

[129] Privacy continuous monitoring means maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

federal or organizational policy.[130] If a reauthorization action is required, organizations maximize the use of security and privacy 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~~(i.e., a continuous monitoring program is in place that monitors all implemented common, hybrid, and system-specific controls with the frequency specified in the continuous monitoring strategy),~~[131] 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 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 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 assessments associated with reauthorization, organizations leverage security- and privacy-related information generated by the ~~existing~~continuous monitoring program and fill in any gaps with manual ~~or procedural~~ assessments. Organizations may supplement automatically-generated assessment information with manually-generated information in situations where an increased level of assurance is needed. If security control assessments are conducted by qualified assessors with the necessary independence, ~~based on federal/organizational policies,~~ use appropriate security standards and guidelines, and are based on the needs of the authorizing official, the assessment results can be cumulatively applied to the reauthorization.[132] ~~The reauthorization action can be as simple as updating the security status information in the authorization package (i.e., the security plan, security assessment report, and plan of action and milestones). The authorizing official subsequently signs an updated authorization decision document based on the current determination and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation.~~[133]

The senior agency official for privacy is responsible for assessing privacy controls and those assessment results can be cumulatively applied to the reauthorization. Independent assessors may assess privacy controls at the discretion of the organization. The senior agency official for privacy reviews and approves the authorization packages for information systems that process PII prior to the authorizing official making a reauthorization decision. The reauthorization action may be as simple as updating 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 authorization decision document based on the current

[130] Decisions to initiate a formal reauthorization include inputs from the senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management/risk executive (function).
[131] 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.
[132] NIST Special Publication 800-53A describes the specific conditions when security-related information can be reused to support authorization actions.
~~[133] Decisions to initiate a formal reauthorization action include inputs from the risk executive (function) and the senior information security officer.~~

risk determination and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation. 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 (subject to organizational reuse policy).

~~In the event that there is a change in authorizing officials, the new authorizing official reviews the current authorization decision document, authorization package, and any updated documents created as a result of the ongoing monitoring activities. If the new authorizing official is willing to accept the currently documented risk, then the official signs a new authorization decision document, thus formally transferring responsibility and accountability for the information system or the common controls inherited by organizational information systems and explicitly accepting the risk to organizational operations and assets, individuals, other organizations, and the Nation. If the new authorizing official is not willing to accept the previous authorization results (including identified level of risk), a *reauthorization* action may need to be initiated or the new authorizing official may instead establish new terms and conditions for continuing the original authorization, but not extend the original authorization termination date. In all situations where there is a decision to reauthorize an information system or the common controls inherited by organizational information systems, the maximum reuse of authorization information is strongly encouraged to minimize the time and expense associated with the reauthorization effort.[134]~~

Commented [A20]: This section (from 800-37, Rev.1) was moved to the Event-Driven Triggers and Significant Changes section in the IPD of 800-37, Rev. 2.

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 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,

~~[134] The decision to initiate a formal reauthorization action can be based on a variety of factors, including for example, the acceptability of the previous authorization information provided in the authorization package, the length of time since the previous authorization decision, the risk tolerance of the new authorizing official, and current organizational requirements and/or priorities.~~

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 substantively affect the security or privacy posture ~~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 how information, including PII, is processed;
- Modifications to cryptographic modules or services; or
- Modifications to security and privacy controls.

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 represent a change that is likely to affect the security and privacy posture of the system. Organizations establish criteria for what constitutes 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 an impact analysis may be used to determine if changes to systems or common controls are significant and trigger an authorization action. If an authorization ~~a formal re-authorization~~ action is initiated, the organization targets only the specific 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*[135] is an official authorization decision ~~to employ identical copies of an information system or subsystem (including hardware, software, firmware, and/or applications) in specified environments of operation.~~that allows for a single authorization package to be developed for an archetype (i.e., common) version of a system. This includes, for example

[135] 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.

hardware, software, or firmware components that are deployed to multiple locations for use in specified environments of operation (e.g., installation and configuration requirements or operational security and privacy needs to be assumed by the hosting organization at a specific location). A type authorization is appropriate when the deployed system is comprised of identical instances of software, identical information types, functionally identical hardware, information that is processed in the same way, identical control implementations, or identical configurations. A type authorization is used in conjunction with authorized site-specific controls~~(e.g., physical and environmental protection controls, personnel security controls) inherited by the information system.[136] The RMF tasks listed in Chapter 3 address the authorization activities associated with the employment of system-specific, hybrid, and common controls.~~[137] or with a facility authorization as described below. A type authorization is issued by the authorizing official responsible for the development of the system[138] and represents an authorization to operate. At the site or facility where the system is deployed, the authorizing official who is responsible for the system at the site or facility accepts the risk of deploying the system and issues an authorization to use. The authorization to use leverages the information in the authorization packages for the archetype system and the facility common controls.

A *facility authorization* is an official authorization decision that is focused on specific 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.[139] Physical and 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; or training and awareness and personnel screening for facility staff. The facility authorizing official issues a common control authorization to describe the common controls available for inheritance by systems residing within the facility.

TRADITIONAL AND JOINT AUTHORIZATIONS ~~APPROACHES~~

Organizations can choose from two ~~three~~ approaches when planning for and conducting authorizations. These include an authorization with a *single* authorizing official or an authorization with *multiple* authorizing officials~~, or (iii) *leveraging* an existing authorization~~[140] .[141] 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, organizational assets,

~~[136] Site-specific controls are typically implemented by an organization as *common controls*.~~

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

[138] 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.

[139] 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.

[140] Authorization approaches can be applied to both information systems and to common controls inherited by one or more organizational information systems.

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

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, control selection and tailoring, a plan for assessing the controls to determine effectiveness, a plan of action and milestones, and a system-level continuous monitoring strategy is necessary for a successful joint authorization. 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 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.

~~The final approach, *leveraged authorization*, is employed when a federal agency[142] chooses to accept some or all of the information in an existing authorization package generated by another federal agency (hereafter referred to as the *owning* organization[143]) based on a need to use the same information resources (e.g., information system and/or services provided by the system). The leveraging organization reviews the owning organization's authorization package as the basis for determining risk to the leveraging organization.[144] When reviewing the authorization package, the leveraging organization considers risk factors such as the time elapsed since the authorization results were produced, the environment of operation (if different from the environment of operation reflected in the authorization package), the criticality/sensitivity of the information to be processed, stored, or transmitted, as well as the overall risk tolerance of the leveraging organization. If the leveraging organization determines that there is insufficient information in the authorization package or inadequate security measures in place for establishing an acceptable level of risk, the leveraging organization may negotiate with the owning organization for additional security measures and/or security-related information.[145] Additional security measures may include, for example, increasing the number of security controls, conducting additional assessments, implementing compensating controls, or establishing constraints on the use of the information system or services provided by the system. Security-related information may include, for example, other information that the owning organization may have discerned in the use or assessment of the information system that is not reflected in the authorization package. The additional security measures and/or security-related information may be provided by the leveraging organization, the information~~

~~[142] In this situation, federal agency includes any organizations that are subordinate to the agency. For example, NIST is a subordinate organization to the Department of Commerce.~~

~~[143] The term *owning* organization refers to the federal agency or subordinate organization that owns the authorization package. The information system may not be owned by the same organization that owns the authorization package, for example, in situations where the system/services are provided by an external provider.~~

~~[144] The sharing of the authorization package (including the security plan, security assessment report, plan of action and milestones, and authorization decision document) is accomplished under terms and conditions agreed upon by all parties (i.e., the owning organization and the leveraging organization).~~

~~[145] Negotiations with the owning organization may include other organizations (e.g., when the information system and/or services are provided to the owning organization in full or in part, by an external provider).~~

~~system developer, some other external third party, or some combination of the above.~~

~~The leveraged authorization approach provides opportunities for significant cost savings and avoids a potentially costly and time-consuming authorization process by the leveraging organization. Leveraging organizations generate an authorization decision document and reference, as appropriate, information in the authorization package from the owning organization. In situations where addition security measures are implemented, the leveraging organization documents those measures by creating an addendum to the original authorization package of the owning organization. This addendum may include, as appropriate, updates to the security plan, security assessment report, and/or plan of action and milestones. Consistent with the traditional authorization process described above, a single organizational official in a senior leadership position in the leveraging organization is both responsible and accountable for accepting the information system-related security risks that may impact the leveraging organization's operations and assets, individuals, other organizations, or the Nation. The leveraged authorization remains in effect as long as the leveraging organization accepts the information system-related security risks and the authorization meets the requirements established by federal and/or organizational policies. This requires the sharing of information resulting from continuous monitoring activities conducted by the owning organization (e.g., updates to the security plan, security assessment report, plan of action and milestones, and security status reports). To enhance the security of all parties, the leveraging organization can also share with the owning organization, the results from any RMF-related activities it conducts to supplement the authorization results produced by the owning organization.~~

~~For all three authorization approaches described above, risk management-related activities (including RMF tasks) involving external providers are carried out in accordance with the guidance provided in Appendices H and I.~~

LEVERAGING EXTERNAL PROVIDER CONTROLS AND ASSESSMENTS

Organizations should exercise caution when attempting to leverage external provider controls and assessment results. 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 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 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 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 necessary to ensure adequate protection for organizational assets.

APPENDIX G

LIFE CYCLE CONSIDERATIONS

OTHER FACTORS EFFECTING THE SUCCESSFUL EXECUTION OF THE RMF

All systems, including operational systems, systems under development, and systems that are undergoing modification or upgrade, are in some phase of the SDLC.[146] Defining requirements is a critical part of an SDLC process and begins in the *initiation* phase.[147] Security and privacy requirements are part of the functional and nonfunctional[148] requirements allocated to a system. The security and privacy requirements are incorporated into the SDLC simultaneously with the other 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 defined early in the SDLC and integrated with other system requirements, the resulting system has fewer deficiencies, and therefore, fewer privacy risks or security vulnerabilities that can be exploited in the future.

Integrating security and privacy requirements into the SDLC is the most effective, efficient, and cost-effective method to ensure that the organization's protection strategy is implemented. It also ensures that security- and privacy-related processes are not isolated from the other processes used 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 SDLC, the requirements are integrated into the organization's program, planning, and budgeting activities to help ensure that resources are available when needed and program and 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 ~~SDLC processes regardless of the type of life cycle processes employed,~~ 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 ~~well-established~~ concept of integrated project teams.[149] Organizational officials ensure that security and privacy professionals are part of the SDLC 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 controls needed to adequately mitigate security and privacy risks and protect organizational missions and business functions.

Finally, organizations maximize the use of security- and privacy-relevant information ~~(e.g., assessment results, information system documentation, and other artifacts)~~generated during the SDLC process to satisfy requirements for similar information needed for other security and privacy purposes. The reuse of such information is an effective method to reduce or eliminate duplication of effort, reduce documentation, promote reciprocity, and avoid unnecessary costs

[146] There are five phases in the SDLC including initiation; development and acquisition; implementation; operation and maintenance; and disposal. NIST Special Publication 800-64 provides guidance on the system development life cycle.
[147] Organizations may employ a variety of development processes including, for example, waterfall, spiral, or agile.
[148] Nonfunctional requirements include, for example, quality and assurance requirements.
[149] 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.

Commented [A21]: In 800-37, Rev. 1, Appendix G covered Continuous Monitoring. Much of this content has been incorporated into the relevant tasks in the Prepare and Monitor Step.

Also in 800-37, Rev. 1, Appendix H covered Operational Scenarios and Appendix I covered Security Controls in External Environemnts. Both Appendix H and I were deleted.

Commented [A22]: Note that some of the concepts and content was previously in Section 2.2 of 800-37, Revision 1.

that may result when security and privacy activities are conducted independently of the SDLC processes. ~~Similar security-relevant information concerning common controls, including security controls provided by external providers, is factored into the organization's risk management process. The judicious reuse of security-relevant information by organizations is an effective method to help eliminate duplication of effort, reduce documentation, promote reciprocity, and avoid unnecessary costs that may result when security activities are conducted independently of system development life cycle processes. In addition,~~ Reuse promotes consistency of information used in the development, implementation, assessment, operation, maintenance, and disposition of systems including security- and privacy-related considerations.

THE IMPORTANCE OF ARCHITECTURE AND ENGINEERING

Security architects, privacy architects, systems security engineers, and privacy engineers can play an essential role in the SDLC 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 controls in organizational information 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 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:

- Ensure that security and privacy requirements are integrated into systems and system components through purposeful security or privacy architecting, design, development, and configuration.
- Employ best practices when implementing controls within a system, including the use of software engineering methodologies; systems 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.