
Risk Management Framework for Information Systems and Organizations

A 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.

Draft NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

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 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-37, Rev. 2, **149 pages** (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 information systems and organizations. The RMF includes a disciplined, structured, and flexible process for organizational asset valuation; control selection, implementation, and assessment; system 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 system development life cycle. Executing the RMF tasks enterprise-wide helps to link essential risk management processes at the system level to risk management processes at the organization level. In addition, it establishes responsibility and accountability for the controls implemented in organizational information systems and inherited by those systems. 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

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

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

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

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.

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.

DRAFT

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](#).

DRAFT

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.

DRAFT

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.

The RMF includes references to specific sections in 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	1
1.1	BACKGROUND	1
1.2	PURPOSE AND APPLICABILITY	2
1.3	TARGET AUDIENCE	3
1.4	ORGANIZATION OF THIS SPECIAL PUBLICATION	3
CHAPTER TWO	THE FUNDAMENTALS	5
2.1	ORGANIZATION-WIDE RISK MANAGEMENT	5
2.2	INFORMATION SECURITY AND PRIVACY UNDER THE RMF	9
2.3	SYSTEM AND SYSTEM ELEMENTS	11
2.4	CONTROL ALLOCATION	13
2.5	SECURITY AND PRIVACY POSTURE	14
2.6	SUPPLY CHAIN RISK MANAGEMENT	15
CHAPTER THREE	THE PROCESS	19
3.1	PREPARE	22
3.2	CATEGORIZE	37
3.3	SELECT	41
3.4	IMPLEMENT	48
3.5	ASSESS	51
3.6	AUTHORIZE	59
3.7	MONITOR	66
APPENDIX A	REFERENCES	74
APPENDIX B	GLOSSARY	78
APPENDIX C	ACRONYMS	95
APPENDIX D	ROLES AND RESPONSIBILITIES	96
APPENDIX E	SUMMARY OF RMF TASKS	106
APPENDIX F	SYSTEM AND COMMON CONTROL AUTHORIZATIONS	118
APPENDIX G	LIFE CYCLE CONSIDERATIONS	135

1 CHAPTER ONE

2 INTRODUCTION

3 THE NEED FOR INFORMATION SECURITY, PRIVACY, AND RISK MANAGEMENT

4 Organizations depend on information systems¹ to successfully carry out their missions and
5 business functions and those systems are constantly subject to serious threats. While the
6 threats to information systems necessarily include environmental disruptions and human
7 or machine errors, in today's environment the most significant threats to systems come from
8 purposeful attacks that are often disciplined, well-organized, and well-funded. These attacks are
9 generally, and in a growing number of cases, very sophisticated. When successful, attacks on
10 information systems can result in serious or catastrophic damage to not just the organizational
11 assets and operations,² but also to individuals, other organizations, and the Nation.³ Given the
12 significant and ever-increasing danger of those threats, it is imperative that organizations remain
13 vigilant and that leaders and managers at all organizational levels understand their responsibilities
14 and are accountable for protecting organizational assets and for managing security risks.⁴

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

29 1.1 BACKGROUND

30 NIST in its partnership with the Department of Defense, the Office of the Director of National
31 Intelligence, and the Committee on National Security Systems, developed a *Risk Management*
32 *Framework* (RMF) to improve information security, strengthen risk management processes, and
33 encourage reciprocity among organizations. In July 2016, the Office of Management and Budget

¹ An *information system* is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [See 44 U.S.C. Sec. 3502]. The term information system includes, for example, general-purpose computing systems; 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.

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

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

⁴ 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.

34 (OMB) revised [Circular A-130](#) to include specific responsibilities for privacy programs under the
35 RMF.⁵ The RMF emphasizes risk management by building security and privacy capabilities into
36 information systems throughout the SDLC; maintaining awareness of the security and privacy
37 posture of information systems on an ongoing basis through continuous monitoring processes;
38 and providing information to senior leaders and executives to facilitate decisions regarding the
39 acceptance of risk to organizational operations and assets, individuals, other organizations, and
40 the Nation arising from the operation and use of systems. The RMF:

- 41 • Provides a repeatable process designed to promote the protection of information and
42 information systems commensurate with risk;
- 43 • Emphasizes organization-wide preparation necessary to manage security and privacy risks;
- 44 • Facilitates the categorization of information and systems; the selection, implementation,
45 assessment, and monitoring of controls; and the authorization of information systems and
46 common controls;
- 47 • Promotes near real-time risk management and ongoing system and control authorization
48 through the implementation of robust continuous monitoring processes;
- 49 • Encourages the use of automation to provide senior leaders with the necessary information to
50 make cost-effective, risk-based decisions for information systems supporting their missions
51 and business functions;
- 52 • Facilitates the seamless integration of security and privacy requirements and controls into
53 enterprise architecture, SDLC, acquisition processes, and systems engineering processes;
- 54 • Connects risk management processes at the organization and mission/business process levels
55 to risk management processes at the information system level via a risk executive (function);⁶
56 and
- 57 • Establishes responsibility and accountability for controls implemented within information
58 systems and inherited by those systems.

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

62 1.2 PURPOSE AND APPLICABILITY

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

- 65 • To ensure that managing system-related security and privacy risk is consistent with the
66 mission and business objectives of the organization and the risk management strategy
67 established by the senior leadership through the risk executive (function);
- 68 • To achieve security and privacy protections for organizational information and information
69 systems through the implementation of appropriate risk response strategies;
- 70 • To facilitate the implementation of the [Framework for Improving Critical Infrastructure
71 Cybersecurity](#).⁷

⁵ [OMB Circular A-130](#), “Managing Federal Information as a Strategic Resource” (2016).

⁶ [OMB Memorandum M-17-25](#) defines a key organizational role of senior accountable official for risk management.

⁷ [Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure](#).

- 72 • To ensure that security and privacy requirements and controls are effectively integrated into
73 the enterprise architecture, SDLC processes, acquisition processes, and systems engineering
74 processes;⁸ and
- 75 • To support consistent, informed, and ongoing authorization decisions (through continuous
76 monitoring),⁹ transparency and traceability of security- and privacy-related information, and
77 reciprocity.¹⁰

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

85 1.3 TARGET AUDIENCE

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

- 88 • Individuals with mission or business ownership responsibilities or fiduciary responsibilities
89 including, for example, and heads of federal agencies;
- 90 • Individuals with information system development and acquisition responsibilities, including,
91 for example, program managers, procurement officials, component product and system
92 developers, systems integrators, and enterprise architects;
- 93 • Individuals with information system, security, or privacy management and/or oversight
94 responsibilities including, for example, senior leaders, risk executives, authorizing officials,
95 chief information officers, senior agency information security officers, and senior agency
96 officials for privacy;
- 97 • Individuals responsible for conducting security or privacy assessments and for monitoring
98 information systems, for example, control assessors, auditors, and system owners; and
- 99 • Individuals with security or privacy implementation and operational responsibilities, for
100 example, system owners, common control providers, information owners/stewards, mission
101 or business owners, security or privacy architects, and systems security or privacy engineers.

102 1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

103 The remainder of this special publication is organized as follows:

- 104 • [Chapter Two](#) describes the concepts associated with managing information system-related
105 security and privacy risk. This includes an organization-wide view of risk management and
106 the application of the RMF steps; the relationship between security and privacy and the

⁸ [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.

⁹ [NIST Special Publication 800-137](#) provides guidance on information security continuous monitoring programs. Future updates to this publication will also address privacy continuous monitoring.

¹⁰ *Reciprocity* is an agreement among participating organizations to accept each other's security and privacy assessment results to reuse system resources or to accept each other's assessed security and privacy posture to share information. Reciprocity does not apply to accepting the risk-based decisions of other organizations.

107 integration of privacy into the RMF; the establishment of a system-of-interest and system
108 elements; the allocation of controls to organizations and systems as system-specific, hybrid,
109 and common controls; the security and privacy posture of systems and organizations; and
110 consideration related to supply chain risk management.

111 • [Chapter Three](#) describes the tasks required to implement the steps in the RMF including:
112 organization-level and information system-level preparation; categorization of information
113 and information systems; control selection, tailoring, and implementation; assessment of
114 control effectiveness; information system and common control authorization; the ongoing
115 monitoring of controls; and maintaining awareness of the security and privacy posture of
116 information systems and the organization.

117 • [Supporting Appendices](#) provide information and guidance for the application of the RMF
118 including: references; glossary of terms; acronyms; roles and responsibilities; summary of
119 tasks; information system and common control authorizations; and SDLC considerations
120 affecting RMF implementation.

DRAFT

1 CHAPTER TWO

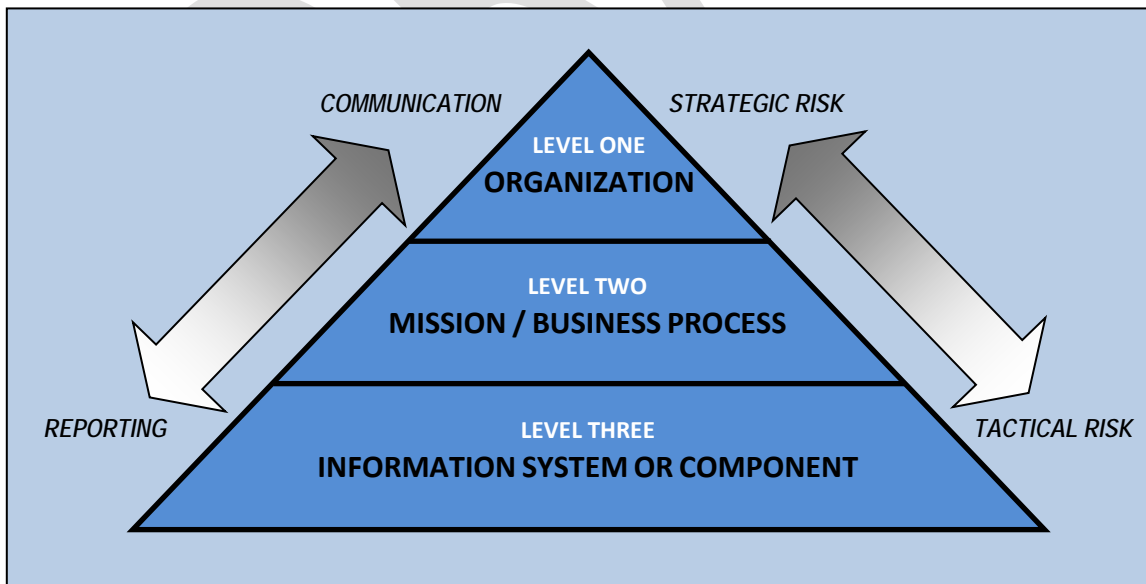
2 **THE FUNDAMENTALS**

3 MANAGING SYSTEM-RELATED SECURITY AND PRIVACY RISKS IN ORGANIZATIONS

4 **T**his chapter describes the basic concepts associated with managing information system-
 5 related security and privacy risks in organizations. These concepts include the system-of-
 6 interest, system elements, and how system boundaries are established; risk management
 7 principles and best practices employed in organization-wide strategic planning; security and
 8 privacy considerations in SDLC processes; and security and privacy risk management practices
 9 and considerations associated with the supply chain. Although the above concepts are discussed
 10 independently, there is a relationship among the concepts.

11 **2.1 ORGANIZATION-WIDE RISK MANAGEMENT**

12 Managing information system-related security and privacy risks is a complex undertaking that
 13 requires the involvement of the entire organization—from senior leaders providing the strategic
 14 vision and top-level goals and objectives for the organization, to mid-level leaders planning and
 15 managing projects, to individuals developing, implementing, operating, and maintaining the
 16 systems supporting the organization’s missions and business functions. Risk management is a
 17 holistic activity that is fully integrated into every aspect of the organization including the mission
 18 and business planning activities, the enterprise architecture, the SDLC processes, and the systems
 19 engineering activities that are integral to those system life cycle processes. Security and privacy
 20 requirements, key elements of risk management, are clearly articulated and communicated to each
 21 organizational entity to help ensure mission and business success. [Figure 1](#) illustrates a three-level
 22 (tiered) approach to risk management that addresses risk-related concerns at the *organization*
 23 level, the *mission/business process* level, and the *information system or system component* level.¹¹

34 **FIGURE 1: ORGANIZATION-WIDE RISK MANAGEMENT APPROACH**

¹¹ [NIST Special Publication 800-39](#) provides guidance on organization-wide risk management.

35 The activities conducted at Levels 1 and 2 are critical to preparing the organization to execute the
36 RMF. Such preparation involves a wide range of activities that go beyond managing the security
37 and privacy risks associated with operating or using specific systems and includes activities that
38 are essential to managing security and privacy risks appropriately throughout the organization.
39 Decisions about how to manage security and privacy risks at the system level cannot be made in
40 isolation. Such decisions are closely linked to decisions regarding the mission/business objectives
41 of the organization; the modernization of information systems, components, and services to adopt
42 new and innovative technologies; the enterprise architecture and the need to manage and reduce
43 the complexity of systems through consolidation, optimization, and standardization (i.e., reducing
44 the attack surface and technology footprint exploitable by adversaries);¹² and the allocation of
45 resources to ensure the organization can conduct its missions and business operations with a high
46 degree of effectiveness, efficiency, and cost-effectiveness.

47 Preparing the organization for a successful execution of the RMF can include assigning key roles
48 and responsibilities for risk management processes; establishing a risk management strategy and
49 organizational risk tolerance; identifying the missions, business functions, and mission/business
50 processes the information system is intended to support; identifying key stakeholders (internal
51 and external to the organization) that have an interest in the information system; identifying and
52 prioritizing assets (including information assets); understanding threats to information systems
53 organizations, and individuals; conducting risk assessments; identifying and prioritizing key
54 stakeholder protection needs and security and privacy requirements;¹³ determining systems-of-
55 interest (i.e., authorization boundaries); defining information systems in terms of the enterprise
56 architecture; developing the security and privacy architectures that include controls suitable for
57 inheritance by organizational systems; identifying, aligning, and deconflicting requirements; and
58 allocating both security and privacy requirements to information systems and environments in
59 which those systems operate.

60 In contrast to the Level 1 and 2 activities that prepare the organization for the execution of the
61 RMF, Level 3 addresses risk from an *information system* perspective and is guided and informed
62 by the risk decisions at the organization and mission/business process levels. The risk decisions at
63 Levels 1 and 2 impact the selection and implementation of controls at the system level. System
64 security and privacy requirements are satisfied by the selection and implementation of controls
65 from [NIST Special Publication 800-53](#). These controls are allocated to the system as system-
66 specific, hybrid, or common controls in accordance with the enterprise architecture, security or
67 privacy architecture, and any tailored control baselines or overlays that have been developed by
68 the organization.¹⁴ In certain cases, when appropriate, controls are allocated to individual system
69 elements. Controls are *traceable* to the security and privacy requirements established by the
70 organization to ensure that there is *transparency* in the development of security and privacy
71 solutions and that the requirements are fully addressed during system design, development,
72 implementation, and maintenance. Each level of the risk management hierarchy is a beneficiary
73 of a successful RMF execution—reinforcing the iterative nature of the risk management process
74 where risk is framed, assessed, responded to, and monitored at various levels of an organization.

¹² *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.

¹³ 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.

¹⁴ Controls can be allocated at all three levels in the risk management hierarchy. For example, common controls may be allocated at the organization, mission/business process, or information system level.

75 Without adequate risk management preparation at the organizational level, security and privacy
76 activities can become too costly, demand too many skilled security and privacy professionals, and
77 produce ineffective solutions. For example, organizations that fail to define and implement an
78 effective enterprise architecture strategy will not be able to consolidate, optimize, and standardize
79 the information technology infrastructure—resulting in unnecessary redundancy and inefficient
80 and costly systems, applications, and services. The effect of ill-conceived architectural and design
81 decisions can produce a cost-multiplier effect downstream that adversely impacts the ability of
82 the organization to implement effective security and privacy solutions.
83

84 **HOLISTIC APPLICATION OF RISK MANAGEMENT CONCEPTS**

85 Successful security, privacy, and risk management programs depend on a holistic application of
86 the concepts to help ensure that there is a high degree of transparency and traceability of every
87 programmatic element. Such transparency and traceability promote a level of trust needed by
88 senior leaders and executives to understand and accept the security and privacy risks to
89 organizational operations and assets, individuals, other organizations, and the Nation.
90
91

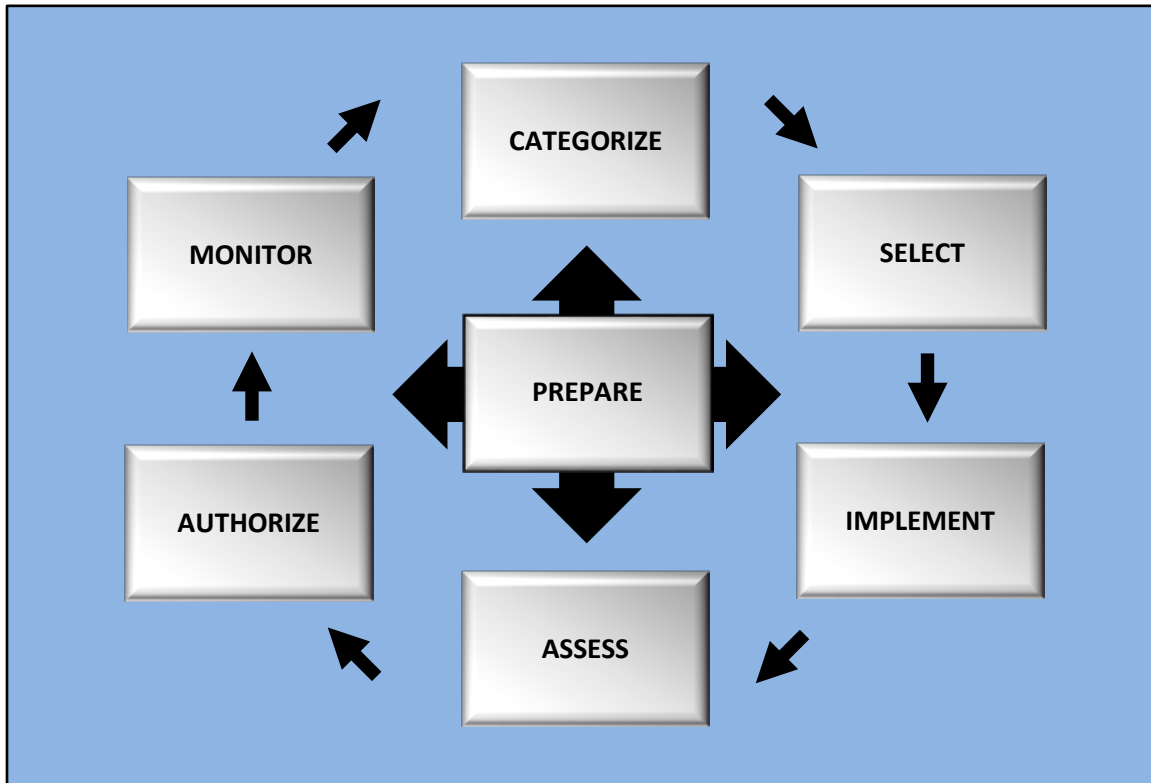
92 The RMF provides a structured and flexible process that integrates security and privacy activities
93 into the SDLC. The RMF operates at all levels in the risk management hierarchy illustrated in
94 [Figure 1](#). There are six main steps in the RMF and a preparatory step to ensure that organizations
95 are ready to execute the process. The steps are:

- 96 • **Prepare** to execute the RMF from an organization-level and a system-level perspective by
97 considering a variety of inputs and carrying out specific activities that establish the context
98 for managing security and privacy risk for the system-of-interest.
- 99 • **Categorize** the system and the information processed, stored, and transmitted by the system
100 based on a security impact analysis.
- 101 • **Select** an initial set of controls for the system and tailor the controls as needed based on an
102 organizational assessment of risk and local conditions.
- 103 • **Implement** the controls and describe how the controls are employed within the system and
104 its environment of operation.
- 105 • **Assess** the controls to determine the extent to which the controls are implemented correctly,
106 operating as intended, and producing the desired outcome with respect to meeting the security
107 and privacy requirements for the system and satisfying security and privacy policy.
- 108 • **Authorize** the system or common controls based on a determination that the risk to
109 organizational operations and assets, individuals, other organizations, and the Nation is
110 acceptable.
- 111 • **Monitor** the system and the associated controls on an ongoing basis to include assessing
112 control effectiveness, documenting changes to the system and environment of operation,
113 conducting risk assessments and impact analyses, and reporting the security and privacy
114 posture of the system.

115 [Figure 2](#) illustrates the steps in the RMF. [Chapter Three](#) provides a detailed description of each of
116 the tasks necessary to carry out the steps in the RMF. References to the [Cybersecurity Framework](#)

117 are indicated in the RMF tasks, where appropriate. The steps in the RMF can also be aligned with
118 the systems security engineering processes defined in [NIST Special Publication 800-160, Vol. 1](#).

119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135



136

FIGURE 2: RISK MANAGEMENT FRAMEWORK

137 While the RMF steps are listed in sequential order above, they can be carried out in any order.
138 Organizations executing the RMF for the first time will typically carry out the steps in sequential
139 order, although they may choose to revisit certain steps during initial execution. Once the system
140 is in the operations and maintenance phase of the SDLC as part of the continuous monitoring
141 step, events may dictate nonsequential execution.

142

143

FLEXIBILITY IN RMF IMPLEMENTATION

144

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.

145

146

147

148 Although the risk management approach in [Figure 1](#) is conveyed as hierarchical, project and
149 organization dynamics are typically more complex. The risk management approach selected by
150 an organization may vary on a continuum from top-down command to decentralized consensus
151 among peers. However, in all cases, organizations use a consistent approach that is applied to risk

152 management processes across the enterprise from the *organization* level to the *information system*
153 level. It is imperative that organizational officials identify and secure the needed resources to
154 complete the risk management tasks described in this publication and ensure that those resources
155 are made available to the appropriate personnel. Resource allocation includes funding to conduct
156 risk management tasks and assigning qualified personnel that will be needed to accomplish the
157 tasks.

158 Successful security, privacy, and risk management programs depend on a holistic application of
159 the concepts to help ensure that there is a high degree of transparency and traceability of every
160 programmatic element. Transparency and traceability promote a level of trust needed by senior
161 leaders and executives to understand and accept the security and privacy risks to organizational
162 operations and assets, individuals, other organizations, and the Nation.

163 2.2 INFORMATION SECURITY AND PRIVACY UNDER THE RMF

164

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

166 In 2016, OMB revised [Circular A-130](#), the circular establishing general policy for the planning,
167 budgeting, governance, acquisition, and management of federal information, personnel,
168 equipment, funds, information technology resources, and supporting infrastructure and
169 services. The circular addresses responsibilities for protecting federal information resources and
170 managing personally identifiable information (PII). In establishing requirements for information
171 security programs and privacy programs, the circular emphasizes the need for both programs to
172 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.*

171 [Circular A-130](#) requires organizations to implement the RMF that is described in this guideline.
172 With the 2016 revision to the circular, OMB also requires organizations to integrate privacy into
173 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.*

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

180

181 Executing the RMF requires close collaboration between information security programs and
182 privacy programs. While information security programs and privacy programs have different
183 objectives, those objectives are overlapping and complementary. Information security programs
184 are responsible for protecting information and information systems from unauthorized access,

185 use, disclosure, disruption, modification, or destruction (i.e., unauthorized system activity or
186 behavior) in order to provide confidentiality, integrity, and availability. Privacy programs are
187 responsible for ensuring compliance with applicable privacy requirements and for managing the
188 risks to individuals associated with the creation, collection, use, processing, storage, maintenance,
189 dissemination, disclosure, or disposal (collectively referred to as “processing”) of PII.¹⁵ When
190 preparing to execute the steps of the RMF, organizations consider how to best promote and
191 institutionalize collaboration between the two programs to ensure that the objectives of both
192 disciplines are met at every step of the process.

193
194 When an information system processes PII, the organizations’ information security program and
195 privacy program have a shared responsibility for managing the risks to individuals that may arise
196 from unauthorized system activity or behavior. This requires the two programs to collaborate
197 when selecting, implementing, assessing, and monitoring security controls. However, while
198 information security programs and privacy programs have complementary objectives with respect
199 to managing the confidentiality, integrity, and availability of PII, protecting individuals’ privacy
200 cannot be achieved solely by securing PII. Not all privacy risks arise from unauthorized system
201 activity or behavior, such as unauthorized access or disclosure of PII; some privacy risks may
202 result from authorized activity that is beyond the scope of information security. For example,
203 privacy programs are responsible for managing the risks to individuals that may result from the
204 creation, collection, use, and retention of PII; the inadequate quality or integrity of PII; and the
205 lack of appropriate notice, transparency, or participation. Therefore, to ensure compliance with
206 applicable privacy requirements and to manage privacy risks from authorized and unauthorized
207 processing of PII, organizations’ privacy programs also select, implement, assess, and monitor
208 privacy controls.

209
210 [OMB Circular A-130](#) defines a *privacy control* as an administrative, technical, or physical
211 safeguard employed within an agency to ensure compliance with applicable privacy requirements
212 and to manage privacy risks. A privacy control is different from a *security control*, which the
213 Circular defines as a safeguard or countermeasure prescribed for an information system or an
214 organization to protect the confidentiality, integrity, and availability of the system and its
215 information. Due to the shared responsibility that organizations’ information security programs
216 and privacy programs have to manage the risks to individuals arising from unauthorized system
217 activity or behavior, controls that achieve both security and privacy objectives are both privacy
218 and security controls. This guideline refers to controls that achieve both sets of objectives as
219 “controls.” Organizations’ information security programs and privacy programs are responsible
220 for control selection, implementation, and assessment. When this guideline uses the descriptors
221 “privacy” and “security” with the term *control*, it is referring to those controls in circumstances
222 where they are selected, implemented, and assessed for particular objectives.

223
224 [Figure 3](#) illustrates how organizations manage privacy risks under the RMF, including both the
225 risks that arise from authorized processing of PII and the risks that arise from unauthorized
226 system activity or behavior. The only step that does not consider the risks that arise from the
227 authorized processing of PII is the [Categorize](#) step (with the exception of the system description
228 task). Information and information systems are categorized based on a security risk assessment,
229 which informs whether the impact on organizational operations and assets, individuals, other
230 organizations, and the Nation from a loss of confidentiality, integrity, and availability is low,

¹⁵ 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.

231 moderate, or high. While the *Categorize* step only considers the risks that arise from unauthorized
 232 system activity and behavior, when an information system processes PII, this necessarily includes
 233 risks to individuals. As such, categorizing information and information systems is a collaborative
 234 effort between the organizations' information security program and privacy program.

235
 236
 237
 238
 239
 240
 241
 242
 243
 244
 245
 246
 247
 248
 249
 250
 251
 252
 253

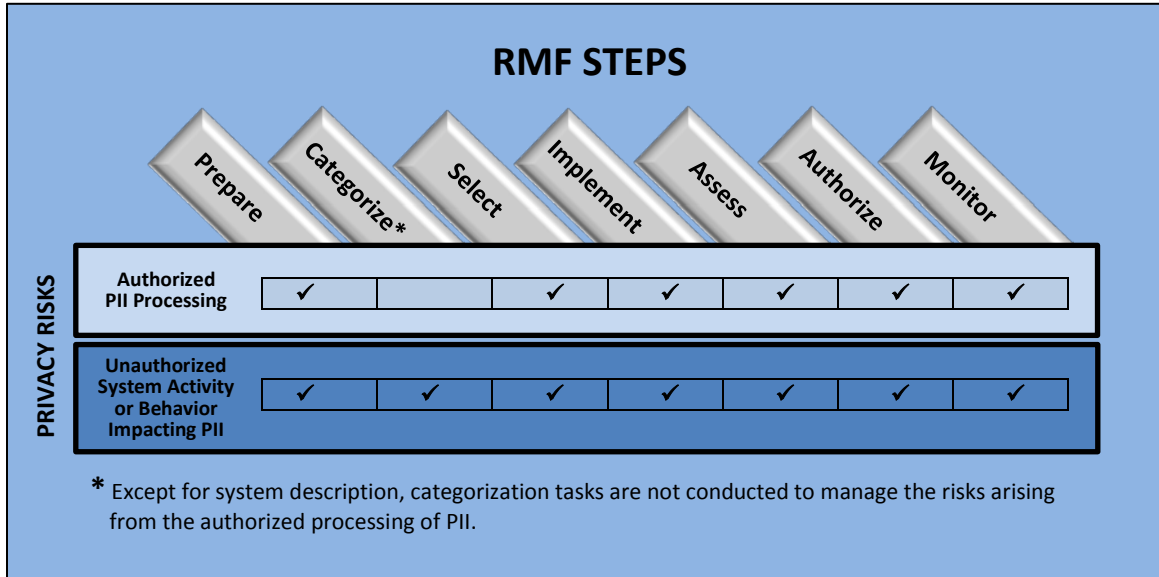


FIGURE 3: PRIVACY INTEGRATION INTO THE RISK MANAGEMENT FRAMEWORK

254 **2.3 SYSTEM AND SYSTEM ELEMENTS**

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

264 Similar to how federal law defines information system as a discrete set of information resources
 265 organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition
 266 of information, [ISO/IEC/IEEE 15288](#) defines a *system* as a set of interacting elements organized
 267 to achieve one or more stated purposes. And, just as the information resources that comprise an
 268 information system include resources such as personnel, equipment, funds, and information
 269 technology, system elements include technology or machine elements, human elements, and
 270 physical or environmental elements. Each of the *system elements*¹⁶ within the system fulfills
 271 specified requirements and may be implemented via hardware, software, or firmware;¹⁷ physical
 272 structures or devices; or people, processes, policies, and procedures. Individual system elements
 273 or a combination of system elements may satisfy stated system requirements. Interconnections

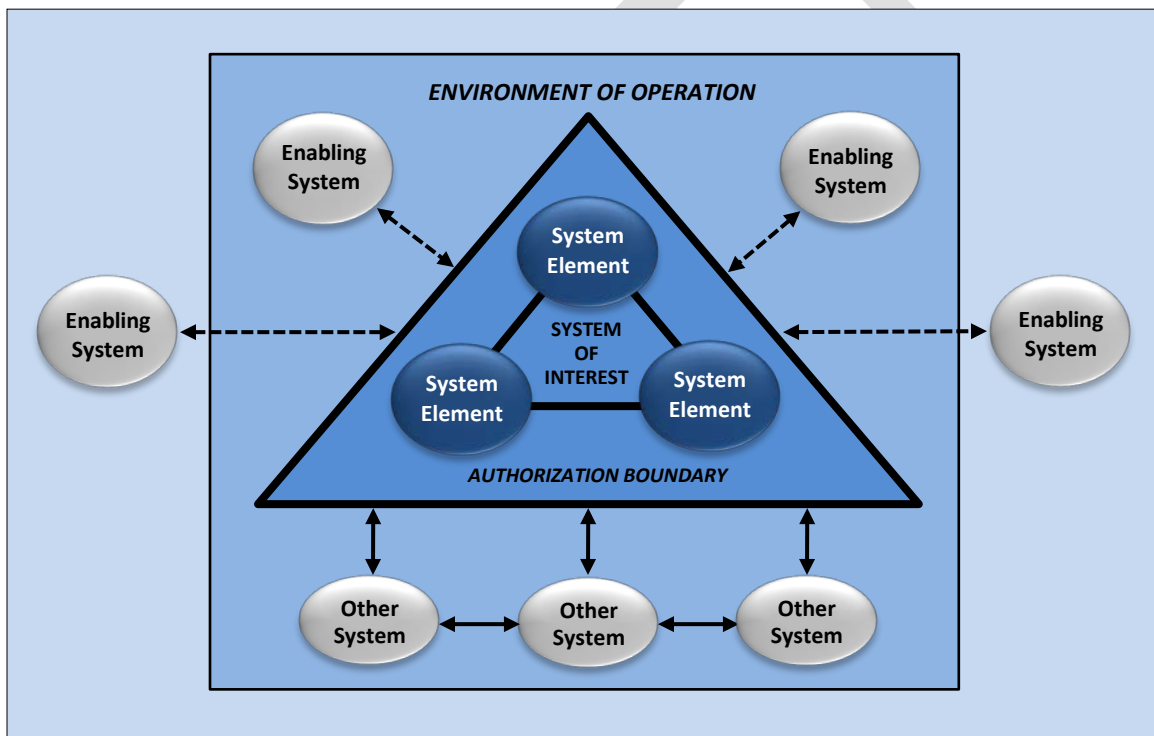
¹⁶ *System elements* are included in the set of information resources defined in 44 U.S.C. Sec. 3502 as information and related resources, such as personnel, equipment, funds, and information technology.

¹⁷ The term *system component* refers to a *system element* that is implemented via hardware, software, or firmware.

274 between system elements allow those elements to interact as necessary to produce a capability as
 275 specified by the system requirements. Finally, every system operates within an environment that
 276 influences the system and its operation.

277 The term *system-of-interest* defines the set of system elements, system element interconnections,
 278 and the environment in which the system operates. The system-of-interest also determines the
 279 authorization boundary¹⁸ for the execution of the RMF. The system-of-interest may be supported
 280 by one or more *enabling systems* that provide support during the system life cycle. The enabling
 281 systems are not within the authorization boundary of the system-of-interest and do not necessarily
 282 exist in the operational environment of the system-of-interest. Finally, there are *other systems* the
 283 system-of-interest interacts with in the operational environment. These systems are also outside
 284 of the authorization boundary and may be the beneficiaries of services provided by the system-of-
 285 interest or simply have some general interaction. [Figure 4](#) illustrates the conceptual view of the
 286 system-of-interest and the relationships among systems, systems elements, and the environment
 287 of operation.

288
 289
 290
 291
 292
 293
 294
 295
 296
 297
 298
 299
 300
 301
 302
 303
 304
 305
 306
 307
 308



309

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

310 The RMF, including the authorization process, is applied to an authorization boundary that can be
 311 conceptualized as a system-of-interest, not individual system elements. Organizations can employ
 312 “component-level” assessments for system elements¹⁹ and can take advantage of the assessment
 313 results generated during that process to support risk-based decision making for the system.

¹⁸ [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.

¹⁹ For example, the evaluation program established under [ISO/IEC 15408](#) (Common Criteria) provides independent component-level assessments for IT products.

314

315

316

RISK MANAGEMENT IN THE SYSTEM DEVELOPMENT LIFE CYCLE

317

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.

318

319

320

321

322

2.4 CONTROL ALLOCATION

323

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.²⁰ 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.²¹

334

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.

344

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.

348

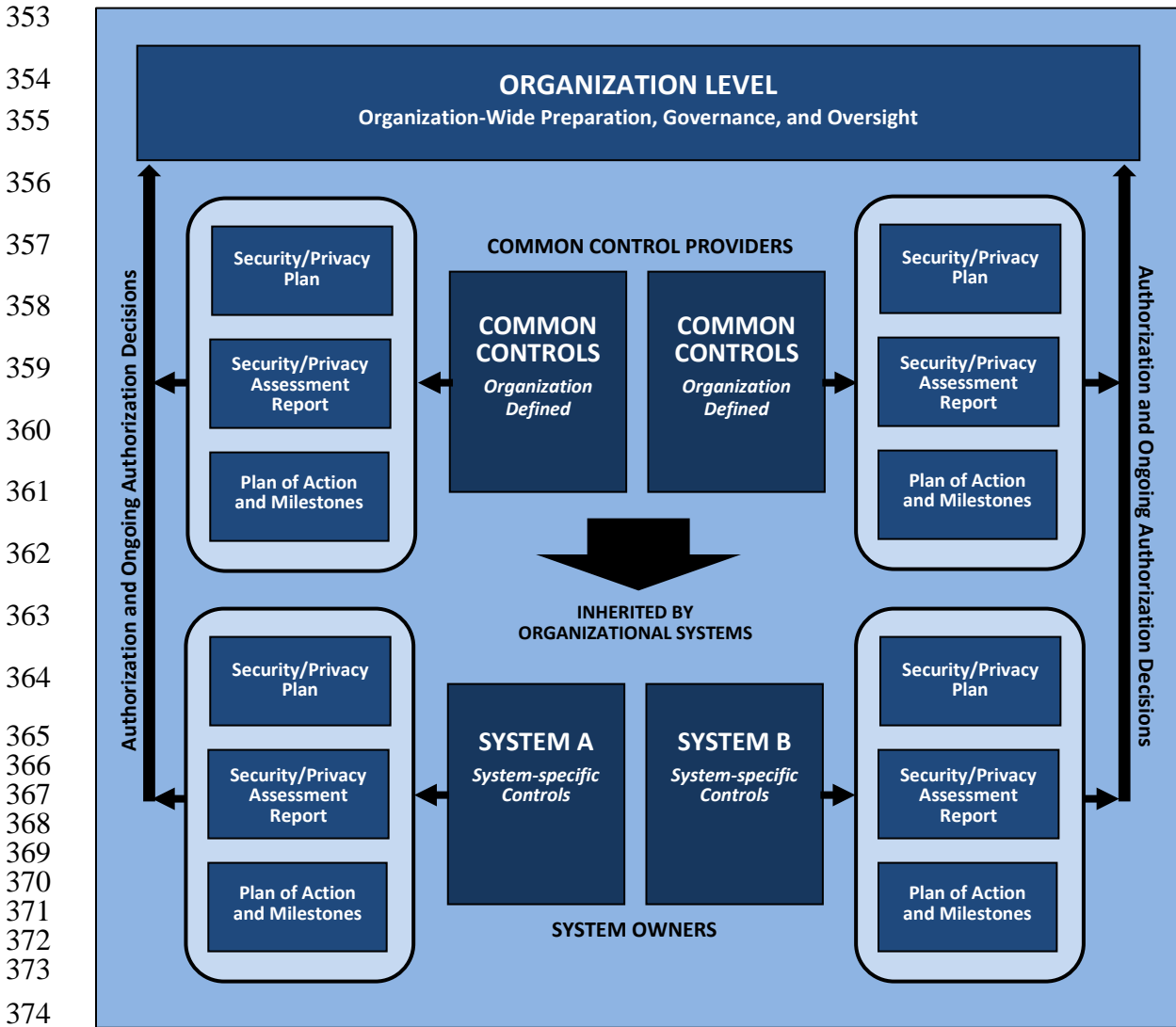
[Figure 5](#) illustrates control allocation using the RMF to produce risk-related information for the senior leaders and executives (including authorizing officials) in the organization on the security

350

²⁰ *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.

²¹ 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.

351 and privacy posture of organizational systems and the mission/business processes supported by
 352 those systems.²²



375 **FIGURE 5: ORGANIZATION-WIDE CONTROL ALLOCATION**

376 **2.5 SECURITY AND PRIVACY POSTURE**

377 The purpose of the RMF is to ensure that information systems, organizations, and individuals are
 378 adequately protected; and that authorizing officials have the information needed to make credible,
 379 risk-based decisions regarding the operation or use of those systems or the inheritance of common
 380 controls. A key aspect of risk-based decision making for authorizing officials is understanding the

²² 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.

381 security and privacy posture of organizational information systems and the common controls that
382 are designated for inheritance by those systems. The security and privacy posture represents the
383 status of the information systems and information resources (i.e., personnel, equipment, funds,
384 and information technology) within an organization based on information assurance resources
385 (e.g., people, hardware, software, policies, procedures) and the capabilities in place to manage the
386 defense of the organization; comply with applicable privacy requirements and manage privacy
387 risks; and react as the situation changes.

388 The security and privacy posture of the information systems and the organization is determined
389 on an ongoing basis by assessing and continuously monitoring system-specific, hybrid, and
390 common controls.²³ The control assessments and monitoring activities provide evidence that the
391 controls selected by the organization are implemented correctly, operating as intended, and
392 satisfying the security and privacy requirements in response to mission or business requirements,
393 laws, executive orders, regulations, directives, policies, or standards. Authorizing officials use the
394 security and privacy posture to determine if the risk to organizational operations and assets,
395 individuals, other organizations, or the Nation are acceptable based on the organization's risk
396 management strategy and organizational risk tolerance.²⁴

397 **2.6 SUPPLY CHAIN RISK MANAGEMENT**

398 Organizations are becoming increasingly reliant on component products, systems, and services
399 provided by external providers to carry out their important missions and business functions.
400 Organizations are responsible and accountable for the risk incurred when using such component
401 products, systems, and services.²⁵ Relationships with external providers can be established in a
402 variety of ways, for example, through joint ventures, business partnerships, various types of
403 formal agreements (e.g., contracts, interagency agreements, lines of business arrangements,
404 licensing agreements), or outsourcing arrangements.

405 The growing dependence on component products, systems, and services from external providers
406 and the relationships with the providers, present an increasing amount of risk to an organization.
407 Some of the risks associated with the global and distributed nature of product and service supply
408 chains include the insertion of counterfeits, unauthorized production, tampering, theft, insertion
409 of malicious software and hardware, as well as poor manufacturing and development practices in
410 the supply chain. These risks are associated with an organization's decreased visibility into, and
411 understanding of, how the technology that they acquire is developed, integrated, and deployed—
412 and the processes, procedures, and practices used to assure the integrity, security, resilience, and
413 quality of the products, systems, and services. Challenges to managing these risks include:

- 414 • Defining the types of component products, systems, and services provided to the organization
415 by external providers;
- 416 • Describing how component products, systems, and services provided by external providers
417 are protected in accordance with the security and privacy requirements of the organization;
418 and

²³ 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.

²⁴ See RMF *Prepare-Organization Level* step, [Task 2](#).

²⁵ [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.

- 419 • Obtaining the necessary assurances that the risk to organizational operations and assets,
420 individuals, other organizations, and the Nation arising from the use of component products,
421 systems, and services provided by external providers is avoided, mitigated, or accepted.

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

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

448 [FISMA](#) and [OMB Circular A-130](#) require external providers handling federal information or
449 operating systems on behalf of the federal government to meet the same security and privacy
450 requirements as federal agencies. Security and privacy requirements for external providers
451 including the controls for systems processing, storing, or transmitting federal information are
452 expressed in contracts or other formal agreements. The RMF can be effectively used to manage
453 supply chain security risk. The conceptual view of the system-of-interest in [Figure 4](#) can guide
454 and inform security and risk management activities for all elements of the supply chain. Every
455 step in the RMF can be executed by nonfederal entities except for the [Authorize](#) step—that is, the
456 acceptance of risk is an inherent federal responsibility for which senior leaders and executives are
457 held accountable.²⁶ The authorization decision is directly linked to the management of risk related
458 to the acquisition and use of component products, systems, and services from external providers.
459 [OMB Circular A-130](#) also requires organizations to develop and implement supply chain risk
460 management plans. Managing supply chain risks is a complex, multifaceted undertaking requiring
461 a coordinated effort across an organization—building trust relationships and communicating with
462 both internal and external stakeholders. This includes engaging multiple disciplines in identifying
463 priorities and developing solutions; ensuring that SCRM activities are performed throughout the

²⁶ 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.

464 SDLC; and incorporating SCRM into organizational risk management decisions. SCRM activities
465 involve identifying and assessing applicable risks, determining appropriate mitigating actions,
466 developing appropriate SCRM plans to document selected mitigating actions, and monitoring
467 performance against SCRM plans. Because supply chains differ across and within organizations,
468 SCRM plans are tailored to individual organizational, program, and operational contexts. Tailored
469 plans provide the basis for determining whether a system is “fit for purpose” and as such, the
470 controls need to be tailored accordingly. Tailored SCRM plans help organizations to focus their
471 resources on the most critical missions and business functions based on mission and business
472 requirements and their risk environment.

473 The determination that the risk from acquiring component products, systems, or services from
474 external providers is acceptable depends on the level of assurance²⁷ that the organization can gain
475 from the providers. The level of assurance is based on the degree of control the organization can
476 exert on the external provider regarding the controls needed for the protection of the component
477 product, system, or service and the evidence brought forth by the provider as to the effectiveness
478 of those controls. The degree of control is established by the specific terms and conditions of the
479 contract or service-level agreement. Some organizations have extensive control through contract
480 vehicles or other agreements that specify the security and privacy requirements for the external
481 provider. Other organizations, in contrast, have rather limited control because they are purchasing
482 commodity services or commercial off-the-shelf products. The level of assurance can also be
483 based on many other factors that convince the organization that the requisite controls have been
484 implemented and that a credible determination of control effectiveness exists. For example, an
485 authorized external cloud service provided to an organization through a well-established line of
486 business relationship may provide a level of trust in the service that is within the risk tolerance of
487 the organization.

488 Ultimately, the responsibility for responding to risks arising from the use of component products,
489 systems, and services from external providers remains with the organization and the authorizing
490 official. Organizations require that an appropriate *chain of trust* be established with external
491 providers when dealing with the many issues associated with system security or privacy risks. A
492 chain of trust requires that organizations establish and retain a certain level of trust such that each
493 participant in the consumer-provider relationship in the supply chain provides adequate protection
494 for component products, systems, and services provided to the organization. The chain of trust
495 can be complicated due to the number of entities participating and the types of relationships
496 between the parties. In certain situations, external providers may outsource the development of
497 component products, systems, and services to other external entities, making the chain of trust
498 difficult to manage. Depending on the type of component product, system, or service, it may not
499 be prudent for the organization to place significant trust in the external provider. This is not
500 necessarily due to any inherent untrustworthiness on the provider's part, but due to the intrinsic
501 level of risk in the component product, system, or service. Where sufficient degree of trust cannot
502 be established, the organization can implement mitigating controls, accept additional risk, or
503 forgo using the product, system, or service.²⁸
504

²⁷ The level of assurance provided by an external provider can vary, ranging from those who provide high assurance (e.g., business partners in a joint venture that share a common business model and goals) to those who provide less assurance and represent greater sources of risk (e.g., business partners in one endeavor who are also competitors in another market sector).

²⁸ [NIST Special Publication 800-161](#) provides guidance on supply chain risk management practices.

505
506**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.

1 CHAPTER THREE

2 THE PROCESS

3 EXECUTING THE RISK MANAGEMENT FRAMEWORK TASKS

4 **T**his chapter describes the process of applying the RMF to organizations and information
5 systems. The process includes a set of risk-based tasks that are to be carried out by selected
6 individuals or groups within defined organizational roles.²⁹ Many risk management roles
7 defined in this publication have counterpart roles defined in the SDLC process. Organizations
8 align their risk management roles with similar or complementary roles defined for the SDLC
9 whenever possible, and consistent with missions and business functions. RMF tasks are executed
10 concurrently with or as part of the SDLC processes in the organization. This helps to ensure that
11 organizations are effectively integrating the process of managing system-related security and
12 privacy risks with their life cycle processes.

13 Each step in the RMF has a purpose statement, a defined set of outcomes, and a set of tasks that
14 are carried out to achieve those outcomes.³⁰ Each task contains a set of potential inputs needed to
15 execute the task and a set of potential outputs generated from task execution.³¹ In addition, each
16 task describes the phase of the SDLC where task execution takes place and the risk management
17 roles and responsibilities associated with the task. Finally, there is a discussion section and
18 references to provide organizations with information on how to effectively execute each task.

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

28 There may be other opportunities to diverge from the sequential nature of the tasks when it is
29 more effective, efficient, or cost-effective to do so. For example, while the control assessment
30 tasks are listed after the control implementation tasks, organizations may choose to begin the
31 assessment of controls as soon as they are implemented but prior to the complete implementation
32 of all controls described in the security and privacy plans. This may result in some organizations
33 assessing the physical and environmental protection controls within a facility prior to assessing
34 the controls implemented in the hardware, firmware, or software components of the system
35 (which may be implemented later). Regardless of the task ordering, the final action before a
36 system is placed into operation is the explicit acceptance of risk by the authorizing official.
37 The RMF steps and associated tasks can be applied to new development systems and existing
38 systems. For new and existing systems, organizations ensure that the designated tasks have been

²⁹ [Appendix D](#) describes the roles and responsibilities of key participants involved in organizational risk management and the execution of the RMF.

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

³¹ 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.

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

43 Applying these steps to existing systems can serve as a gap analysis to determine if security and
44 privacy risks have been managed. Any deficiencies in controls can be addressed in the RMF steps
45 addressing implementation, assessment, authorization, and monitoring in the same manner as in
46 new development systems. If no deficiencies are discovered during the gap analysis and there is a
47 current authorization in effect, the organization can move directly to the last step in the RMF,
48 continuous monitoring. If a current authorization is not in place, the organization continues with
49 the assessment, authorization, and monitoring steps in the RMF.

50

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.

52 **3.1 PREPARE**³²

53
54
55
56
57
58
59
60
61

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*.

62 **PREPARE TASKS—ORGANIZATION LEVEL**³³

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

66 **TABLE 1: PREPARE TASKS AND OUTCOMES—ORGANIZATION LEVEL**

Tasks	Outcomes
TASK 1 RISK MANAGEMENT ROLES	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> Tailored control baselines for organization-wide use are established and made available. [Cybersecurity Framework: Profile]
TASK 5 COMMON CONTROL IDENTIFICATION	<ul style="list-style-type: none"> Common controls that are available for inheritance by organizational systems are identified, documented, and published.
TASK 6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	<ul style="list-style-type: none"> A prioritization of organizational systems with the same impact level is conducted. [Cybersecurity Framework: ID.AM-5]
TASK 7 CONTINUOUS MONITORING STRATEGY—ORGANIZATION	<ul style="list-style-type: none"> An organization-wide strategy for monitoring control effectiveness is developed and implemented. [Cybersecurity Framework: DE.CM]

67
68
69

[Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.](#)

³² 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.

³³ For ease of use, the preparatory activities are grouped into organization-level preparation and information system-level preparation.

70 RISK MANAGEMENT ROLES

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

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

74 **Potential Outputs:** Documented Risk Management Framework role assignments.

75 **Primary Responsibility:** [Head of Agency](#); [Chief Information Officer](#); [Senior Agency Official for Privacy](#).

76 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Senior](#)
77 [Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#); [Senior Agency Information](#)
78 [Security Officer](#).

79 **Discussion:** The roles and responsibilities of key participants in risk management processes are described
80 in [Appendix D](#). The roles and responsibilities may include personnel that are internal or external to the
81 organization, as appropriate. Since organizations have different missions, functions, and organizational
82 structures, there may be differences in naming conventions for risk management roles and how specific
83 responsibilities are allocated among organizational personnel including, for example, multiple individuals
84 filling a single role or one individual filling multiple roles. In either situation, the basic risk management
85 functions remain the same. Organizations ensure that there are no conflicts of interest when assigning the
86 same individual to multiple risk management roles. For example, authorizing officials cannot occupy the
87 role of system owner or common control provider for systems or common controls they are authorizing. In
88 addition, combining multiple roles for security and privacy requires care because the two disciplines may
89 require different expertise, and in some circumstances, the priorities may be competing.

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

92 RISK MANAGEMENT STRATEGY

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

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

97 **Potential Outputs:** Risk management strategy and statement of risk tolerance.

98 **Primary Responsibility:** [Head of Agency](#).

99 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#); [Chief](#)
100 [Information Officer](#); [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#).

101 **Discussion:** Risk tolerance is the level or degree of risk or uncertainty that is acceptable to an organization.
102 Risk tolerance affects all components of the risk management process, having a direct impact on the risk
103 management decisions made by senior leaders or executives throughout the organization and providing
104 important constraints on those decisions. The risk management strategy guides and informs risk-based
105 decisions including how security and privacy risk is framed, assessed, responded to, and monitored. The
106 risk management strategy makes explicit the threats, assumptions, constraints, priorities, trade-offs, and risk
107 tolerance used for making investment and operational decisions. This strategy includes the strategic-level
108 decisions and considerations for how senior leaders and executives are to manage security, privacy, and
109 supply chain risks to organizational operations and assets, individuals, other organizations, and the Nation.
110 The risk management strategy includes an expression of organizational risk tolerance; acceptable risk
111 assessment methodologies and risk response strategies; a process for consistently evaluating the security,
112 privacy, and supply chain risks across the organization with respect to risk tolerance; and approaches for
113 monitoring risk over time. As organizations define and implement risk management strategies, policies,
114 procedures, and processes, it is important that they include SCRM considerations. The risk management

115 strategy for security and privacy links security and privacy programs with the management control systems
116 established in the organization's Enterprise Risk Management strategy.³⁴

117 **References:** [NIST Special Publication 800-30](#); [NIST Special Publication 800-39](#) (Organization Level);
118 [NIST Special Publication 800-160, Volume 1](#) (Risk Management, Decision Management, Quality
119 Assurance, Quality Management, Project Assessment and Control Processes); [NIST Special Publication](#)
120 [800-161](#); [NIST Interagency Report 8062](#); [NIST Cybersecurity Framework](#) (Core [Identify Function]).

121 RISK ASSESSMENT—ORGANIZATION

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

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

125 **Potential Outputs:** Organization-level risk assessment results.

126 **Primary Responsibility:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#);
127 [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#).

128 **Supporting Roles:** [Chief Information Officer](#); [Authorizing Official](#) or [Authorizing Official Designated](#)
129 [Representative](#).

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

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

139 ORGANIZATION-WIDE TAILORED CONTROL BASELINES AND PROFILES (OPTIONAL)

140 **Task 4** Establish, document, and publish organization-wide tailored control baselines and/or profiles.

141 **Potential Inputs:** Documented stakeholder protection needs and security and privacy requirements;
142 applicable laws, executive orders, directives, regulations, policies, or standards requiring the use of specific
143 tailored control baselines; organization- and system-level risk assessment results; [NIST Special Publication](#)
144 [800-53](#) control baselines.

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

147 **Primary Responsibility:** [Mission or Business Owner](#); [Senior Accountable Official for Risk Management](#) or
148 [Risk Executive \(Function\)](#).

149 **Supporting Roles:** [Chief Information Officer](#); [Authorizing Official](#) or [Authorizing Official Designated](#)
150 [Representative](#); [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#).

151 **Discussion:** To address the organizational need for specialized sets of controls, tailored control baselines
152 may be developed for organization-wide use.³⁵ An organization-wide tailored baseline provides a fully
153 specified set of controls, control enhancements, and supplemental guidance derived from established

³⁴ [OMB Circular A-123](#), "Management's Responsibility for Enterprise Risk Management and Internal Control," (2016).

³⁵ 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.

154 control baselines described in [NIST Special Publication 800-53](#). The tailoring process can also be guided
155 and informed by the requirements engineering process described in [NIST Special Publication 800-160](#),
156 [Volume 1](#). Organizations can use the tailored control baseline concept when there is divergence from the
157 fundamental assumptions used to create the initial control baselines in NIST Special Publication 800-53.
158 This would include, for example, situations when the organization has specific security and privacy risks,
159 has specific mission or business needs, or plans to operate in environments that are not addressed in the
160 initial baselines.

161 Tailored baselines complement the initial NIST Special Publication 800-53 control baselines by providing
162 an opportunity to add or eliminate controls to accommodate organizational requirements while continuing
163 to protect information in a way that is commensurate with risk. Organizations can use tailored baselines to
164 customize control baselines by describing control applicability and providing interpretations for specific
165 technologies; types of missions, operations, systems, operating modes, or operating environments; and
166 statutory or regulatory requirements. Organization-wide tailored baselines can establish parameter values
167 for assignment or selection statements in controls and control enhancements that are agreeable to specific
168 communities of interest and can also extend the supplemental guidance where necessary. Organization-
169 wide tailored baselines may be more stringent or less stringent than the baselines identified in [NIST Special](#)
170 [Publication 800-53](#) and are applied to multiple systems. Tailored baselines may be mandated for use by
171 certain laws, executive orders, directives, regulations, policies, or standards. In some situations, tailoring
172 actions may be restricted or limited by the developer of the tailored baseline or by the issuing authority for
173 the tailored baseline. Tailored baselines (or overlays) have been developed by communities of interest for
174 cloud and shared systems, services, and applications; industrial control systems; national security systems;
175 weapons and space-based systems; high-value assets; mobile device management; federal public key
176 infrastructure; and privacy risks.

177 Organizations may also benefit from the creation of a Cybersecurity Framework *profile*. A profile is a
178 prioritization of the Framework Core Categories and/or Subcategory outcomes based on business/mission
179 functions, security requirements, and risk determinations. Many of the tasks in organizational preparation
180 provide an organization-level view of these considerations and can serve as inputs to a Framework profile.
181 The resulting prioritized list of cybersecurity outcomes developed at the organization and mission/business
182 process levels can be helpful in facilitating consistent, risk-based decisions at the system level during the
183 execution of the RMF steps. Profiles, the precursor to control selection in the Cybersecurity Framework,
184 can also be used to guide and inform the development of the tailored control baselines described above.

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

188 COMMON CONTROL IDENTIFICATION

189 **Task 5** Identify, document, and publish organization-wide common controls that are available for
190 inheritance by organizational systems.

191 **Potential Inputs:** Documented stakeholder protection needs and stakeholder security and privacy
192 requirements; existing common control providers and associated system security and privacy plans;
193 organizational information security and privacy program plans; organization- and system-level risk
194 assessment results.

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

198 **Primary Responsibility:** [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#).

199 **Supporting Roles:** [Mission or Business Owner](#); [Senior Accountable Official for Risk Management](#) or [Risk](#)
200 [Executive \(Function\)](#); [Chief Information Officer](#); [Authorizing Official](#) or [Authorizing Official Designated](#)
201 [Representative](#); [Common Control Provider](#); [System Owner](#).

202 **Discussion:** Common controls are controls that can be inherited by one or more information systems.
203 Common controls can include controls from any [NIST Special Publication 800-53](#) control family, for
204 example, physical and environmental protection controls, system boundary and monitoring controls,
205 personnel security controls, policies and procedures, acquisition controls, account and identity management
206 controls, audit log and accountability controls, or complaint management controls for receiving privacy-
207 related inquiries from the public. Organizations identify and select the set of common controls and allocate
208 those controls to the organizational entities designated as common control providers. Common controls
209 may differ based upon a variety of factors, such as hosting location, system architecture, and the structure
210 of the organization. The list of common controls should take these factors into account. Common controls
211 can also be identified at different levels of the organization, including, for example, corporate, department,
212 or agency level; bureau or subcomponent level; or individual program level. Organizations may establish
213 one or more lists of common controls that can be inherited by the systems in the organization.

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

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

230 Common control providers execute the steps in the RMF to implement, assess, and monitor the controls
231 designated as common controls. Common control providers may also be system owners when the common
232 controls are resident within an information system. Organizations select senior officials or executives to
233 serve as authorizing officials for common controls. The senior agency official for privacy is responsible for
234 designating common privacy controls and for documenting them in the organization's privacy program
235 plan. Authorizing officials are responsible for accepting security and privacy risk resulting from the use of
236 common controls inherited by organizational systems.

237 Common control providers are responsible for documenting common controls in security and privacy plans
238 (or equivalent documents prescribed by the organization); ensuring that the controls are implemented and
239 assessed for effectiveness by qualified assessors; ensuring that assessment findings are documented in
240 security and privacy assessment reports; producing a plan of action and milestones for common controls
241 determined to have unacceptable deficiencies and targeted for remediation; receiving authorization for the
242 common controls from the designated authorizing official; and monitoring control effectiveness on an
243 ongoing basis. Plans, assessment reports, and plans of action and milestones for common controls (or a
244 summary of such information) are made available to system owners and can be used by authorizing
245 officials to inform authorization decisions for systems inheriting common controls.

246 **References:** [NIST Special Publication 800-53](#).

247 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)

248 **Task 6** Prioritize organizational systems with the same impact level.

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

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

252 **Primary Responsibility:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#).
253 **Supporting Roles:** [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#);
254 [Mission or Business Owner](#); [System Owner](#); [Chief Information Officer](#); [Authorizing Official](#) or
255 [Authorizing Official Designated Representative](#).

256 **Discussion:** This task is carried out *only* after organizational systems have been categorized (see RMF
257 *Categorize* step, [Task 1](#)). This task requires organizations to apply the “high water mark” concept to each
258 of their information systems categorized in accordance with FIPS Publication 199. The application of the
259 high-water mark concept results in systems designated as low impact, moderate impact, or high impact.
260 Organizations desiring additional granularity in their impact designations for risk-based decision making
261 can use this task to prioritize their systems within each impact level. For example, an organization may
262 decide to prioritize its moderate-impact systems by assigning each moderate system to one of three new
263 subcategories: *low-moderate* systems, *moderate-moderate* systems, and *high-moderate* systems. This
264 prioritization of moderate systems gives organizations an opportunity to make more informed decisions
265 regarding control selection and the tailoring of control baselines when responding to identified risks.³⁶
266 Impact-level prioritization can also be used to determine those systems that are critical to organizational
267 missions and business operations (also known as high-value assets) and therefore, organizations can focus
268 on the important factors of complexity, aggregation, and system interconnections. Such systems can be
269 identified, for example, by prioritizing high-impact systems into *low-high* systems, *moderate-high* systems,
270 and *high-high* systems. Impact-level prioritizations can be conducted at any level of the organization and
271 are based on information system categorization data reported by individual system owners.

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

277 CONTINUOUS MONITORING STRATEGY—ORGANIZATION

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

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

282 **Potential Outputs:** An implemented organizational continuous monitoring strategy.

283 **Primary Responsibility:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#);
284 [Senior Agency Official for Privacy](#).

285 **Supporting Roles:** [Chief Information Officer](#); [Senior Agency Information Security Officer](#); [Mission or](#)
286 [Business Owner](#); [System Owner](#); [Authorizing Official](#) or [Authorizing Official Designated Representative](#).

287 **Discussion:** An important aspect of risk management is the ability to monitor the effectiveness of controls
288 implemented within or inherited by information systems on an ongoing basis. An effective organization-
289 wide continuous monitoring strategy is essential to efficiently and cost-effectively carrying out such
290 monitoring. Continuous monitoring strategies can also include supply chain risk considerations, for
291 example, requiring suppliers to be audited on an ongoing basis. The implementation of a robust and
292 comprehensive continuous monitoring program helps an organization to understand the security and
293 privacy postures of their information systems over time and to maintain the initial system or common
294 control authorizations. This includes the potential for changing missions/business functions, stakeholders,
295 technologies, vulnerabilities, threats, risks, and suppliers of systems, components, or services.

³⁶ 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.

296 The organizational continuous monitoring strategy addresses monitoring requirements at the organization,
 297 mission/business process, and information system levels. The continuous monitoring strategy also identifies
 298 the minimum frequency of monitoring for implemented controls across the organization and defines the
 299 organizational control assessment approach. The continuous monitoring strategy may also define security
 300 and privacy reporting requirements including recipients of the reports.³⁷ The criteria for determining the
 301 minimum frequency with which controls are to be monitored post implementation, is established in
 302 collaboration with selected organizational officials including, for example, the senior accountable official
 303 for risk management or risk executive (function); senior agency information security officer; senior agency
 304 official for privacy; chief information officer; system owners; common control providers; and authorizing
 305 officials or their designated representatives. An organizational risk assessment can be used to guide and
 306 inform the frequency of monitoring. The use of automation facilitates a greater frequency and volume of
 307 control assessments as part of the monitoring process. The ongoing monitoring of controls using automated
 308 tools and supporting databases facilitates near real-time risk management for information systems, and
 309 supports ongoing authorization and more efficient use of resources. The senior accountable official for risk
 310 management or the risk executive (function) approves the continuous monitoring strategy including the
 311 minimum frequency with which controls are to be monitored.

312 **References:** [NIST Special Publication 800-30](#); [NIST Special Publication 800-39](#) (Organization, Mission
 313 or Business Process, System Levels); [NIST Special Publication 800-53](#); [NIST Special Publication 800-
 314 53A](#); [NIST Special Publication 800-137](#); [NIST Special Publication 800-161](#); [NIST Interagency Report
 315 8062](#); [NIST Cybersecurity Framework](#) (Core [Detect Function]); [CNSS Instruction 1253](#).

316 **PREPARE TASKS—SYSTEM LEVEL**

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

320 **TABLE 2: PREPARE TASKS AND OUTCOMES—SYSTEM LEVEL**

Tasks	Outcomes
TASK 1 MISSION OR BUSINESS FOCUS	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> The stakeholders having an interest in the system are identified. [Cybersecurity Framework: ID.AM; ID.BE]
TASK 3 ASSET IDENTIFICATION	<ul style="list-style-type: none"> Stakeholder assets are identified and prioritized. [Cybersecurity Framework: ID.AM]
TASK 4 AUTHORIZATION BOUNDARY	<ul style="list-style-type: none"> The authorization boundary (i.e., system-of-interest) is determined.
TASK 5 INFORMATION TYPES	<ul style="list-style-type: none"> The types of information processed, stored, and transmitted by the system are identified. [Cybersecurity Framework: ID.AM-5]
TASK 6 INFORMATION LIFE CYCLE	<ul style="list-style-type: none"> For systems that process PII, the information life cycle is identified.
TASK 7 RISK ASSESSMENT—SYSTEM	<ul style="list-style-type: none"> A system-level risk assessment is completed or an existing risk assessment is updated. [Cybersecurity Framework: ID.RA]

³⁷ 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	<ul style="list-style-type: none"> Protection needs and security and privacy requirements are defined and prioritized. [Cybersecurity Framework: ID.GV; PR.IP]
TASK 9 ENTERPRISE ARCHITECTURE	<ul style="list-style-type: none"> The placement of the system within the enterprise architecture is determined.
TASK 10 SYSTEM REGISTRATION	<ul style="list-style-type: none"> The system is registered for purposes of management, accountability, coordination, and oversight. [Cybersecurity Framework: ID.GV]

321
322

[Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.](#)

323 MISSION OR BUSINESS FOCUS

324 [Task 1](#) Identify the missions, business functions, and mission/business processes that the system is
 325 intended to support.

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

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

330 **Primary Responsibility:** [Mission or Business Owner](#).

331 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [System Owner](#);
 332 [Information Owner or Steward](#); [Senior Agency Information Security Officer](#); [Senior Agency Official for](#)
 333 [Privacy](#).

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

336 **Discussion:** Organizational missions and business functions influence the design and development of the
 337 mission or business processes that are created to carry out those missions and business functions. The
 338 prioritization of missions and business functions drives investment strategies and funding decisions, and
 339 therefore, affects the development of the enterprise architecture and the associated security and privacy
 340 architectures. Information is elicited from stakeholders to acquire a thorough understanding of the missions,
 341 business functions, and mission/business processes of the organization from a system security and privacy
 342 perspective.

343 **References:** [NIST Special Publication 800-39](#) (Organization and Mission/Business Process Levels); [NIST](#)
 344 [Special Publication 800-64](#); [NIST Special Publication 800-160, Volume 1](#) (Business or Mission Analysis,
 345 Portfolio Management, and Project Planning Processes); [NIST Cybersecurity Framework](#) (Core [Identify
 346 Function]); [NIST Interagency Report 8179](#) (Criticality Analysis Process B).

347 ORGANIZATIONAL STAKEHOLDERS

348 [Task 2](#) Identify stakeholders who have an interest in the design, development, implementation,
 349 assessment, operation, maintenance, or disposal of the system.

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

- 355 **Potential Outputs:** List of system stakeholders.
- 356 **Primary Responsibility:** [System Owner](#).
- 357 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Mission or](#)
358 [Business Owner](#); [Information Owner or Steward](#); [Senior Agency Information Security Officer](#); [Senior](#)
359 [Agency Official for Privacy](#).
- 360 **System Development Life Cycle Phase:** New – Initiation (concept/requirements definition).
361 Existing – Operations/Maintenance.
- 362 **Discussion:** Stakeholders include individuals, organizations, or representatives that have an interest in the
363 system across the entire system life cycle—for design, development, implementation, delivery, operation,
364 and sustainment of the information system. It also includes all aspects of the supply chain. Stakeholders
365 may reside in the same organization or they may reside in different organizations in situations when there is
366 a common interest by those organizations in the information system. For example, this may occur during
367 the development, operation, and maintenance of cloud-based systems, shared service systems, or any
368 system where organizations may be adversely impacted by a breach or a compromise to the system or for a
369 variety of considerations related to the supply chain.
- 370 **References:** [NIST Special Publication 800-39](#) (Organization Level); [NIST Special Publication 800-64](#);
371 [NIST Special Publication 800-160, Volume 1](#) (Stakeholder Needs and Requirements Definition and
372 Portfolio Management Processes); [NIST Special Publication 800-161](#); [NIST Cybersecurity Framework](#)
373 (Core [Identify Function]).
- 374 ASSET IDENTIFICATION
- 375 **Task 3** Identify assets that require protection.
- 376 **Potential Inputs:** Information specifying the missions, business functions, and mission/business processes
377 the information system will support; business impact analyses; internal stakeholders; system stakeholder
378 information; system information; information about other systems that interact with the system.
- 379 **Potential Outputs:** Set of assets to be protected.
- 380 **Primary Responsibility:** [System Owner](#).
- 381 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Mission or](#)
382 [Business Owner](#); [Information Owner or Steward](#); [Senior Agency Information Security Officer](#); [Senior](#)
383 [Agency Official for Privacy](#).
- 384 **System Development Life Cycle Phase:** New – Initiation (concept/requirements definition).
385 Existing – Operations/Maintenance.
- 386 **Discussion:** Assets are the tangible and intangible items that are of value to achievement of organizational
387 mission or business objectives. Tangible assets are physical in nature and include the physical elements of
388 the system’s operational environment (e.g., structures, facilities) and hardware elements of components,
389 mechanisms, systems, and networks. In contrast, intangible assets are not physical in nature and include
390 mission and business processes, functions, information, data, firmware, software, personnel, and services.
391 Information assets include the information needed to carry out the missions or business functions, to deliver
392 services, and for system management and operation; classified information and controlled unclassified
393 information; and all forms of documentation associated with the information system. Intangible assets can
394 also include the image or reputation of an organization, as well as the privacy interests of the individuals
395 whose information will be processed by the system. The organization defines the scope of stakeholder
396 assets to be considered for protection. Assets that require protection are identified based on stakeholder
397 concerns and the contexts in which the assets are used. This includes the missions or business functions of
398 the organization; the other systems that interact with the system; and stakeholders whose assets are utilized
399 by the mission or business functions or by the system.
- 400 **References:** [NIST Special Publication 800-39](#) (Organization Level); [NIST Special Publication 800-64](#);
401 [NIST Special Publication 800-160, Volume 1](#) (Stakeholder Needs and Requirements Definition Process);

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

404 AUTHORIZATION BOUNDARY

405 **Task 4** Determine the authorization boundary of the system.

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

408 **Potential Outputs:** Documented authorization boundary.

409 **Primary Responsibility:** [System Owner](#).

410 **Supporting Roles:** [Chief Information Officer](#); [Authorizing Official](#) or [Authorizing Official Designated](#)
411 [Representative](#); [Mission or Business Owner](#); [Senior Agency Information Security Officer](#); [Senior Agency](#)
412 [Official for Privacy](#); [Enterprise Architect](#).

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

415 **Discussion:** Authorization boundaries establish the scope of protection for information systems (i.e., what
416 the organization agrees to protect under its management control or within the scope of its responsibilities).
417 Authorization boundaries are determined by authorizing officials with input from the system owner based
418 on mission, management, or budgetary responsibility. Clear delineation of authorization boundaries is
419 important for accountability and for security categorization, especially in situations where lower-impact
420 systems are connected to higher-impact systems. Each system consists of a set of interacting elements (i.e.,
421 information resources)³⁸ organized to achieve one or more stated purposes and to support the organization's
422 missions and business processes. Each system element is implemented to fulfill specified stakeholder
423 requirements including security and privacy requirements. System elements include human elements,
424 technology/machine elements, and physical/environmental elements.

425 The term system-of-interest is used to define the set of system elements, system element interconnections,
426 and the environment that is the focus of the RMF implementation (see [Figure 4](#)). For systems processing
427 PII, it is essential that privacy and security programs collaborate to develop a common understanding of the
428 authorization boundary. Privacy risks arise from the processing of PII, which may occur outside of what the
429 security program typically considers the authorization boundary. Privacy programs cannot effectively
430 conduct the privacy risk assessment that underpins the selection of controls if the privacy and security
431 programs have a materially different understanding of what constitutes the authorization boundary.

432 **References:** [NIST Special Publication 800-18](#); [NIST Special Publication 800-39](#) (System Level); NIST
433 [Special Publication 800-47](#); [NIST Special Publication 800-64](#); [NIST Special Publication 800-160, Volume](#)
434 [1](#) (System Requirements Definition Process); [NIST Cybersecurity Framework](#) (Core [Identify Function]).

435 INFORMATION TYPES

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

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

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

439 **Primary Responsibility:** [System Owner](#); [Information Owner or Steward](#).

440 **Supporting Role:** [Mission or Business Owner](#); [System Security or Privacy Officer](#).

441

³⁸ *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.

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

444 **Discussion:** Identifying the types of information needed to support organizational missions, business
445 functions, and mission/business processes is an important step in developing comprehensive security and
446 privacy plans for the information system and a precondition for determining the security categorization.
447 The National Archives and Records Administration (NARA) has defined a set of information types as part
448 of its Controlled Unclassified Information (CUI) program. Organizations may define additional information
449 types needed to support organizational missions, business functions, and mission/business processes that
450 are not defined in the CUI Registry or in [NIST Special Publication 800-60, Volume 2](#).

451 **References:** [NIST Special Publication 800-39](#) (System Level); [NIST Special Publication 800-60, Volume](#)
452 [1](#); [NIST Special Publication 800-60, Volume 2](#); [NIST Special Publication 800-122](#); [NIST Cybersecurity](#)
453 [Framework](#) (Core [Identify Function]); [NARA CUI Registry](#).

454 INFORMATION LIFE CYCLE

455 **Task 6** For systems that process PII, identify and understand all parts of the information life cycle.

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

459 **Potential Outputs:** Data map illustrating how PII is being processed throughout its life cycle by the
460 system.

461 **Primary Responsibility:** [Senior Agency Official for Privacy](#); [System Owner](#); [Information Owner or](#)
462 [Steward](#).

463 **Supporting Roles:** [Chief Information Officer](#); [Mission or Business Owner](#).

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

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

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

477 **References:** [NIST Interagency Report 8062](#).

478 RISK ASSESSMENT (SYSTEM)

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

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

485 **Potential Outputs:** Risk assessment report.

486 **Primary Responsibility:** [System Owner](#); [System Privacy Officer](#).

487 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#);
488 [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Mission or Business Owner](#);
489 [Information Owner or Steward](#); [System Security Officer](#).

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

492 **Discussion:** Assessment of security risk includes identification of threat sources³⁹ and threat events
493 affecting assets, whether and how the assets are vulnerable to the threats, the likelihood that an asset
494 vulnerability will be exploited by a threat, and the impact (or consequence) of loss of the assets. As a key
495 part of the risk assessment, assets are prioritized based on the adverse impact or consequence of asset loss.
496 The meaning of loss is defined for each asset type to enable a determination of loss consequence (i.e., the
497 adverse impact of the loss). Loss consequences constitute a continuum that spans from partial loss to total
498 loss relative to the asset. Interpretations of information loss may include loss of possession, destruction, or
499 loss of precision or accuracy. The loss of a function or service may be interpreted as a loss of control, loss
500 of accessibility, loss of the ability to deliver normal function, performance, or behavior, or a limited loss of
501 capability resulting in a level of degradation of function, performance, or behavior. Prioritization of assets
502 is based on asset value, criticality, cost of replacement, impact on image or reputation, or trust by users, by
503 mission or business partners, or by collaborating organizations. The asset priority translates to precedence
504 in allocating resources, determining strength of mechanisms, and defining levels of assurance. Asset
505 valuation is a precondition for defining protection needs and security requirements.

506 Privacy risk assessments are conducted to determine the likelihood that a given operation the system is
507 taking when processing PII could create an adverse effect on individuals—and the potential impact on
508 individuals.⁴⁰ Privacy risk assessments are influenced by contextual factors. Contextual factors can include,
509 but are not limited to, the sensitivity level of the PII, including specific elements or in aggregate; the types
510 of organizations using or interacting with the system and individuals’ perceptions about the organizations
511 with respect to privacy; individuals’ understanding about the nature and purpose of the processing; and
512 individuals’ privacy interests, technological expertise or demographic characteristics that influence their
513 understanding or behavior. The privacy risks to individuals may affect individuals’ decisions to engage
514 with the system thereby impacting mission or business objectives, or may create legal liability, reputational
515 risks, or other types of risks for the organization. Impacts to the organization are not privacy risks.
516 However, these impacts can guide and inform organizational decision-making and influence prioritization
517 and resource allocation for risk response. [Section 2.2](#) provides information on the overlapping areas in
518 security and privacy risk assessments, which may present opportunities for collaboration.

519 Risk assessments are conducted throughout the SDLC and support various RMF steps. Risk assessment
520 results are used to inform potential courses of action for risk responses. Organizations determine the form
521 of risk assessment conducted (including the scope, rigor, and formality of such assessments) and method of
522 reporting results.

523 **References:** [FIPS Publication 199](#); [FIPS Publication 200](#); [NIST Special Publication 800-30](#); [NIST Special](#)
524 [Publication 800-39](#) (Organization Level); [NIST Special Publication 800-59](#); [NIST Special Publication 800-](#)
525 [60, Volume 1](#); [NIST Special Publication 800-60, Volume 2](#); [NIST Special Publication 800-64](#); [NIST](#)
526 [Special Publication 800-160, Volume 1](#) (Stakeholder Needs and Requirements Definition and Risk
527 Management Processes); [NIST Special Publication 800-161](#) (Assess); [NIST Interagency Report 8062](#);
528 [NIST Interagency Report 8179](#); [NIST Cybersecurity Framework](#) (Core [Identify Function]); [CNSS](#)
529 [Instruction 1253](#).

³⁹ 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.

⁴⁰ [NIST Interagency Report 8062](#) introduces privacy risk management and a privacy risk model for conducting privacy risk assessments.

530 PROTECTION NEEDS—SECURITY AND PRIVACY AND REQUIREMENTS

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

532 **Potential Inputs:** System design documentation; organization- and system-level risk assessment results;
533 known set of stakeholder assets to be protected; information specifying the missions, business functions,
534 and mission/business processes the system will support; business impact analyses or criticality analyses;
535 information about system stakeholders; data map of the information life cycle for PII; information about
536 other systems that interact with the system; supply chain information; threat information; laws, regulations,
537 or policies that apply to the system; risk management strategy.

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

539 **Primary Responsibility:** [Mission or Business Owner](#); [System Owner](#); [System Privacy Officer](#); [Information](#)
540 [Owner or Steward](#).

541 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [System](#)
542 [Security Officer](#); [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#).

543
544 **System Development Life Cycle Phase:** New – Initiation (concept/requirements definition).
545 Existing – Operations/Maintenance.

546 **Discussion:** The protection needs are an expression of the protection capability required in the system.
547 Protection needs include the security characteristics⁴¹ of the system and the security behavior of the system
548 in its intended operational environment and across all system life cycle phases. The protection needs reflect
549 the relative priorities of stakeholders, results of negotiations among stakeholders in response to conflicts,
550 opposing priorities, contradictions, and stated objectives, and thus, are inherently subjective. The protection
551 needs are documented to ensure that the reasoning, assumptions, and constraints associated with those
552 needs are available for future reference. The protection needs are subsequently transformed into security
553 and privacy requirements and associated constraints on system requirements, and the measures needed to
554 validate that all requirements have been met.

555 Security and privacy requirements⁴² constitute a formal, more granular expression of protection needs
556 across all SDLC phases, the associated life cycle processes, and protections for the assets associated with
557 the system. Security and privacy requirements may be obtained from a variety of sources including, for
558 example, laws, executive orders, directives, regulations, policies, standards, mission and business needs, or
559 risk assessments. These requirements are a part of the formal expression of required characteristics of the
560 system—encompassing security, privacy, and assurance.⁴³ The security and privacy requirements guide and
561 inform the selection of controls for a system and the tailoring activities associated with those controls.

562 Organizations can use the Cybersecurity Framework to manage security requirements and express
563 those requirements in Framework Profiles defined for the organization. For instance, multiple requirements
564 can be aligned and even deconflicted using the *Function-Category-Subcategory* structure of the Framework
565 Core. The Framework *profiles* can then be used to inform the development of tailored security control
566 baselines described in the RMF *Prepare-Organization Level* step, [Task 4](#).

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

⁴¹ For example, a fundamental security characteristic is that the system-of-interest exhibits only specified behaviors, interactions, and outcomes.

⁴² 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.

⁴³ *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.

569 [NIST Special Publication 800-161](#) (Multi-Tiered Risk Management); [NIST Interagency Report 8179](#); [NIST](#)
570 [Cybersecurity Framework](#) (Core [Protect, Detect, Respond, Recover Functions]; Profiles).

571 ENTERPRISE ARCHITECTURE

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

573 **Potential Inputs:** Security and privacy requirements; organization- and system-level risk assessment
574 results; enterprise architecture information; security architecture information; privacy architecture
575 information; asset information.

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

578 **Primary Responsibility:** [Mission or Business Owner](#); [Enterprise Architect](#); [Security or Privacy Architect](#).

579 **Supporting Roles:** [Chief Information Officer](#); [Authorizing Official](#) or [Authorizing Official Designated](#)
580 [Representative](#); [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#); [System](#)
581 [Owner](#); [Information Owner](#) or [Steward](#).

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

584 **Discussion:** System complexity can impact the risk and the ability of organizations to successfully carry
585 out their missions and business functions. An enterprise architecture can help provide greater understanding
586 of information and operational technologies included in the initial design and development of information
587 systems and should be considered a prerequisite for achieving resilience and survivability of those systems
588 in the face of increasingly sophisticated threats. Enterprise architecture is a management practice used by
589 organizations to maximize the effectiveness of mission/business processes and information resources and to
590 achieve mission and business success. Enterprise architecture provides an opportunity for organizations to
591 consolidate, standardize, and optimize information and technology assets. An effectively implemented
592 enterprise architecture produces systems that are more transparent and therefore, easier to understand and
593 protect. Enterprise architecture also establishes a clear and unambiguous connection from investments to
594 measurable performance improvements. The placement of a system within the enterprise architecture is
595 important as it provides greater visibility and understanding about the other organizational systems that will
596 be connected to the system and can also be effectively used to establish security domains for increased
597 levels of protection for the system.

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

606 **References:** [NIST Special Publication 800-39](#) (Mission/Business Process Level); [NIST Special Publication](#)
607 [800-64](#); [NIST Special Publication 800-160, Volume 1](#) (System Requirements Definition Process); [NIST](#)
608 [Cybersecurity Framework](#) (Core [Identify Function]; Profiles); [Common Approach to Federal Enterprise](#)
609 [Architecture](#); [Federal Enterprise Architecture Framework](#).

610 SYSTEM REGISTRATION

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

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

613 **Potential Outputs:** Registered system in accordance with organizational policy.

614 **Primary Responsibility:** [System Owner](#).

615 **Supporting Role:** [Mission or Business Owner](#); [Chief Information Officer](#); [System Security or Privacy](#)
616 [Officer](#).

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

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

629 **References:** [NIST Cybersecurity Framework](#) (Core [Identify Function]).
630

631 **3.2 CATEGORIZE**⁴⁴

632
633
634
635
636
637
638
639
640

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.

641
642

CATEGORIZE TASKS

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

645

TABLE 3: CATEGORIZE TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 SECURITY CATEGORIZATION	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.
TASK 3 SYSTEM DESCRIPTION	<ul style="list-style-type: none"> The characteristics of the system are described and documented. [Cybersecurity Framework: Profile]

646
647

[Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.](#)

648 SECURITY CATEGORIZATION

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

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

⁴⁴ 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](#).

653 specific system elements; list of security requirements allocated to the environment of operation; business
654 impact analyses or criticality analyses.

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

658 **Primary Responsibility:** [System Owner](#); [Information Owner or Steward](#).

659 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#); [Chief](#)
660 [Information Officer](#); [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#);
661 [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [System Security or Privacy](#)
662 [Officer](#).

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

665 **Discussion:** Security categorization determinations consider potential adverse impacts to organizational
666 operations, organizational assets, individuals, other organizations, and the Nation. The categorization
667 process is carried out by the system owner and the information owner or steward in cooperation and
668 collaboration with senior leaders and executives with mission, business function, or risk management
669 responsibilities. This ensures that individual systems are categorized based on the mission and business
670 objectives of the organization. The system owner and information owner or steward consider the results
671 from the risk assessment as a part of the security categorization decision. The decision is consistent with
672 the risk management strategy and identifies the potential adverse impact to organizational missions or
673 business functions resulting from the loss of confidentiality, integrity, or availability of information. The
674 results of the security categorization process influence the selection of security controls for the system.
675 Security categorization information is documented in the security plan or included as an attachment to the
676 plan and can be cross-referenced in a privacy plan when the system processes PII.

677 The security categorization results for the system can be further refined by the organization to facilitate an
678 impact-level prioritization of systems with the same impact level (see RMF *Prepare-Organization Level*
679 *step, Task 6*). Results from the impact-level prioritization conducted by the organization can be used to
680 help system owners in control selection and tailoring decisions.

681 **References:** [FIPS Publication 199](#); [NIST Special Publication 800-30](#); [NIST Special Publication 800-39](#)
682 (System Level); [NIST Special Publication 800-59](#); [NIST Special Publication 800-60, Volume 1](#); [NIST](#)
683 [Special Publication 800-60, Volume 2](#); [NIST Special Publication 800-160, Volume 1](#) (Stakeholder Needs
684 and Requirements Definition and System Requirements Definition Processes); [NIST Interagency Report](#)
685 [8179](#); [CNSS Instruction 1253](#); [NIST Cybersecurity Framework](#) (Core [Identify Function]).

686 SECURITY CATEGORIZATION REVIEW AND APPROVAL

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

688 **Potential Inputs:** Impact levels determined for each information type and for each security objective
689 (confidentiality, integrity, availability); system categorization based on high water mark of information
690 type impact levels; list of high-value assets for the organization.

691 **Potential Outputs:** Approval of security categorization for the system.

692 **Primary Responsibility:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Senior](#)
693 [Agency Official for Privacy](#).⁴⁵

694 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#); [Chief](#)
695 [Information Officer](#); [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#).

696

⁴⁵ This role is active for information systems processing PII.

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

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

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

718 SYSTEM DESCRIPTION

719 **Task 3** Document the characteristics of the system.

720 **Potential Inputs:** System design and requirements documentation; authorization boundary information; list
721 of security and privacy requirements allocated to the system and to specific system elements; list of
722 security and privacy requirements allocated to the environment of operation; system element information or
723 system component inventory; system categorization; information on system use, users, and roles; data map
724 of the information life cycle for PII.

725 **Potential Outputs:** Documented system description.

726 **Primary Responsibility:** [System Owner](#).

727 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Information](#)
728 [Owner or Steward](#); [System Security or Privacy Officer](#).

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

731 **Discussion:** A description of the characteristics of the system is documented in the security and privacy
732 plans, included in attachments to the plans, or referenced in other standard sources for the information
733 generated as part of the SDLC. Duplication of information is avoided, whenever possible. The level of
734 detail in the security and privacy plans is determined by the organization and is commensurate with the
735 security categorization and the privacy risk assessment of the system. Information may be added to the
736 system description as it becomes available during the system life cycle and execution of the RMF steps.

737 Examples of different types of descriptive information that organizations can include in security and
738 privacy plans include: descriptive name of the system and system identifier; system version or release
739 number; individual responsible for the system and contact information; organization that manages, owns, or
740 controls the system; system location; purpose of the system and missions/business processes supported;
741 how the system is integrated into the enterprise architecture; SDLC phase; results of the categorization
742 process and privacy risk assessment; authorization boundary; laws, directives, policies, regulations, or
743 standards affecting individuals’ privacy and the security of the system; architectural description of the
744 system including network topology; information types; hardware, firmware, and software components that

745 are part of the system; hardware, software, and system interfaces (internal and external); information flows
746 within the system; network connection rules for communicating with external systems; interconnected
747 systems and identifiers for those systems; system users (including affiliations, access rights, privileges,
748 citizenship); system provenance in the supply chain; maintenance or other relevant agreements;
749 ownership/operation of system (government-owned, government-operated; government-owned, contractor-
750 operated; contractor-owned, contractor-operated; nonfederal [state and local governments, grantees]);
751 authorization date and authorization termination date; ongoing authorization status; and incident response
752 points of contact. System registration information is updated with the system characterization information
753 (see RMF *Prepare-System Level* step, [Task 10](#)).

754 **References:** [NIST Special Publication 800-18](#); [NIST Cybersecurity Framework](#) (Core [Identify Function]).
755

DRAFT

756 **3.3 SELECT**

757
758
759
760
761
762
763
764
765
766

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

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

769

TABLE 4: SELECT TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 SECURITY AND PRIVACY REQUIREMENTS ALLOCATION	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Controls are tailored producing tailored control baselines. [Cybersecurity Framework: Profile]
TASK 4 SECURITY AND PRIVACY PLANS	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.

770
771

[Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.](#)

772 SECURITY AND PRIVACY REQUIREMENTS ALLOCATION

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

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

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

782 **Primary Responsibility:** [Security Architect](#); [Privacy Architect](#) or [System Privacy Officer](#).

783 **Supporting Roles:** [Chief Information Officer](#); [Authorizing Official](#) or [Authorizing Official Designated](#)
784 [Representative](#); [Mission or Business Owner](#); [Senior Agency Information Security Officer](#); [Senior Agency](#)
785 [Official for Privacy](#); [System Owner](#).

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

788 **Discussion:** Organizations allocate security and privacy requirements to facilitate the control selection and
789 implementation processes at the organization, information system, and system element (i.e., component)
790 levels. The allocation of security and privacy requirements to the system and to the environment⁴⁶ in which
791 the system operates, determines which controls are designated as system-specific, common, and hybrid
792 during the control selection process. Requirements allocation also identifies the specific system elements
793 (i.e., components) to which controls are assigned. The allocation of security and privacy requirements saves
794 resources and facilitates streamlining of the risk management process by ensuring that requirements are not
795 implemented on multiple systems or multiple components within a system when implementation of a
796 common control or a system-level control on a specific component provides the needed protection
797 capability. Common controls satisfy security and privacy requirements allocated to the organization and
798 provide a security and privacy protection capability that is inherited by one or more systems (common
799 controls are identified as part of the RMF *Prepare-Organization Level* step, [Task 5](#)). Hybrid controls
800 satisfy security and privacy requirements allocated to the system and to the organization and provide a
801 security and privacy protection capability that is partially inherited by one or more systems. And finally,
802 system-specific controls satisfy security and privacy requirements allocated to the system and provide a
803 security and privacy protection capability only for that system. Security and privacy protection capabilities
804 may also be allocated to specific system components rather than to every component within a system. For
805 example, system-specific controls associated with management of audit logs may be allocated to a log
806 management server and thus need not be implemented on every system component.

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

811 CONTROL SELECTION

812 [Task 2](#) Select the controls for the system.

813 **Potential Inputs:** System categorization information; organization- and system-level risk assessment
814 results; system element information/system component inventory; list of security and privacy requirements
815 allocated to the system and to system elements; list of security and privacy requirements allocated to the
816 environment of operation; business impact analysis or criticality analysis; risk management strategy;
817 organizational security and privacy policy; federal or organization-approved or mandated baselines or
818 overlays; Cybersecurity Framework profiles.

819 **Potential Outputs:** Controls selected for the system.

820 **Primary Responsibility:** [System Owner](#); [Common Control Provider](#).

821 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Information](#)
822 [Owner or Steward](#); [Systems Security or Privacy Engineer](#); [System Security or Privacy Officer](#).

⁴⁶ 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](#).

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

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

838 The organization-generated control selection approach differs from the baseline control selection approach
839 because the organization does not start with a pre-defined set of controls. Rather, the organization develops
840 a set of security requirements using a life cycle-based systems engineering process (e.g., [ISO/IEC/IEEE](#)
841 [15288](#) and [NIST Special Publication 800-160, Volume 1](#)) as described in the RMF *Prepare-System Level*
842 step, [Task 8](#). The *requirements engineering* process generates a specific set of security requirements that
843 can subsequently be used to guide and inform the selection of a set of controls to satisfy the requirements.
844 Similarly, organizations can use the Cybersecurity Framework to develop *framework profiles* as a set of
845 organization-specific security requirements—guiding and informing control selection from [NIST Special](#)
846 [Publication 800-53](#). Tailoring at the system level may be required after the organization-generated control
847 selection (see RMF *Select* step, [Task 3](#)). In instances where organizations do not use a baseline approach
848 for selecting an initial set of privacy controls, the organizations can select privacy controls as part of an
849 organization-generated control selection approach.

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

855 CONTROL TAILORING

856 **Task 3** Tailor the controls selected for the system.

857 **Potential Inputs:** Initial control baselines; organization- and system-level risk assessment results; system
858 element information/system component inventory; list of security and privacy requirements allocated to the
859 system and to system elements; list of security and privacy requirements allocated to the environment of
860 operation; business impact analysis or criticality analysis; risk management strategy; organizational
861 security and privacy policy; federal or organization-approved or mandated overlays.

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

863 **Primary Responsibility:** [System Owner](#); [Common Control Provider](#).

864 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Information](#)
865 [Owner or Steward](#); [Systems Security or Privacy Engineer](#); [System Security or Privacy Officer](#).

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

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

871 which the system operates. The tailoring process includes identifying and designating common controls in
872 the control baselines (see RMF *Prepare-Organization Level* step, [Task 5](#)); applying scoping considerations
873 to the remaining baseline controls; selecting compensating controls, if needed; assigning specific values to
874 organization-defined control parameters through either assignment or selection statements; supplementing
875 baselines with additional controls; and providing specification information for control implementation.⁴⁷
876 Organizations have flexibility to determine the amount of detail to include in justifications or supporting
877 rationale required for tailoring decisions. For example, the justification or supporting rationale for scoping
878 decisions related to a high-impact system (or high value asset) may necessitate greater specificity than
879 similar decisions for a low-impact system. Such determinations are consistent with organizational missions
880 and business functions; stakeholder needs; and any relevant laws, executive orders, regulations, directives,
881 or policies.

882 Organizations use risk assessments to inform and guide the tailoring process. Threat information from
883 security risk assessments provides information on adversary capabilities, intent, and targeting that may
884 affect organizational decisions regarding the selection of security controls, including the associated costs
885 and benefits. Privacy risk assessments, including the contextual factors therein, will also influence tailoring
886 when an information system processes PII.⁴⁸ Risk assessment results are also leveraged when identifying
887 common controls to determine if the controls available for inheritance meet the security and privacy
888 requirements for the system and its environment of operation. When common controls provided by the
889 organization are not sufficient for systems inheriting the controls, system owners either supplement the
890 common controls with system-specific or hybrid controls to achieve the required protection for the system
891 or accept greater risk with the acknowledgement and approval of the organization. Organizations may also
892 consider federally or organizationally mandated or approved overlays, tailored baselines, or Cybersecurity
893 Framework Profiles when conducting tailoring (see RMF *Prepare-Organization Level* step, [Task 4](#)).

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

899 SECURITY AND PRIVACY PLANS

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

901 **Potential Inputs:** System categorization information; organization- and system-level risk assessment
902 results; system element information/system component inventory; list of security and privacy requirements
903 allocated to the system and to system elements; list of security and privacy requirements allocated to the
904 environment of operation; business impact analysis or criticality analysis; risk management strategy;
905 organizational security and privacy policy; list of selected controls for the system.

906 **Potential Outputs:** Security and privacy plans for the system.

907 **Primary Responsibility:** [System Owner](#); [Common Control Provider](#).

908 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Information](#)
909 [Owner or Steward](#); [Systems Security or Privacy Engineer](#); [System Security or Privacy Officer](#).

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

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

⁴⁷ The tailoring process is fully described in [NIST Special Publication 800-53](#).

⁴⁸ [NIST Interagency Report 8062](#) provides a discussion of context and its function in a privacy risk model.

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

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

936 Documentation of planned control implementations allows for traceability of decisions prior to and after
937 the deployment of the system. To the extent possible, organizations reference existing documentation
938 (either by vendors or other organizations that have employed the same or similar systems or system
939 elements), use automated support tools, and coordinate across the organization to reduce redundancy and
940 increase the efficiency and cost-effectiveness of control documentation. The documentation also addresses
941 platform dependencies and includes any additional information necessary to describe how the capability
942 required is to be achieved at the level of detail sufficient to support control implementation and assessment.
943 Documentation for control implementations follows best practices for hardware and software development
944 and for systems security and privacy engineering disciplines and is also consistent with established policies
945 and procedures for documenting SDLC activities. In certain situations, security controls can be
946 implemented in ways that create privacy risks. The privacy program supports documentation of privacy risk
947 considerations and the specific implementations intended to mitigate them.

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

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

962 CONTINUOUS MONITORING STRATEGY—SYSTEM

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

965 **Potential Inputs:** Organizational risk management strategy; organizational continuous monitoring strategy;
966 organization- and system-level risk assessment results; system security and privacy plans; organizational
967 security and privacy policies.

968 **Potential Outputs:** Continuous monitoring strategy for the system.

969 **Primary Responsibility:** [System Owner](#); [Common Control Provider](#).

970 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#); [Chief](#)
971 [Information Officer](#); [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#);
972 [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Information Owner or Steward](#);
973 [Security or Privacy Architect](#); [Systems Security or Privacy Engineer](#); [System Security or Privacy Officer](#).

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

976 **Discussion:** An important aspect of risk management is the ongoing monitoring of controls implemented
977 within or inherited by an information system. An effective continuous monitoring strategy at the system
978 level is developed and implemented in coordination with the organizational continuous monitoring strategy
979 early in the SDLC (i.e., during initial system design or procurement decision). The system-level continuous
980 monitoring strategy supplements the organizational continuous monitoring strategy—that is, the system-
981 level strategy addresses monitoring those controls for which monitoring is not provided as part of the
982 organizational continuous monitoring strategy and implementation for the organization.⁴⁹ The system-level
983 continuous monitoring strategy identifies the frequency of monitoring for controls not addressed by the
984 organizational strategy and defines the approach to be employed for assessing those controls. The system-
985 level continuous monitoring strategy, consistent with the organizational strategy, may define how changes
986 to the system are to be monitored; how security and privacy risk assessments are to be conducted; and the
987 security and privacy posture reporting requirements including recipients of the reports. The system-level
988 continuous monitoring strategy can be included in security and privacy plans.

989 For controls that are not addressed by the organizational continuous monitoring strategy, the criteria for
990 determining the frequency with which controls are monitored post-implementation, is established by the
991 system owner or common control provider in collaboration with organizational officials including, for
992 example, the authorizing official or designated representative; chief information officer; senior agency
993 information security officer; senior agency official for privacy; and senior accountable official for risk
994 management or risk executive (function). The frequency criteria at the system level reflect the priorities and
995 the importance of the system to organizational operations and assets, individuals, other organizations, and
996 the Nation. Controls that are volatile (i.e., where the control or the control implementation is most likely to
997 change over time),⁵⁰ critical to certain aspects of the protection needs for the organization, or identified in
998 plans of action and milestones, may require more frequent assessment. The approach to control assessments
999 during continuous monitoring may include for example, the detection of the status of system components;
1000 analysis of historical and operational data; and the reuse of assessment procedures and assessment results
1001 that supported the initial authorization decision.

1002 The authorizing official or designated representative approves the continuous monitoring strategy including
1003 the minimum frequency with which each control is to be monitored. The approval of the strategy can be

⁴⁹ 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.

⁵⁰ 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.

- 1004 obtained in conjunction with the security and privacy plan approval. The monitoring of controls begins at
1005 the start of the operational phase of the SDLC and continues through the disposal phase.
- 1006 **References:** [NIST Special Publication 800-30](#); [NIST Special Publication 800-39](#) (Organization, Mission or
1007 Business Process, System Levels); [NIST Special Publication 800-53](#); [NIST Special Publication 800-53A](#);
1008 [NIST Special Publication 800-137](#); [NIST Special Publication 800-161](#); [NIST Cybersecurity Framework](#)
1009 (Core [Detect Function]); [CNSS Instruction 1253](#).
- 1010 SECURITY AND PRIVACY PLAN REVIEW AND APPROVAL
- 1011 **Task 6** Review and approve the security and privacy plans for the system.
- 1012 **Potential Inputs:** Completed system security and privacy plans; organization- and system-level risk
1013 assessment results.
- 1014 **Potential Outputs:** System security and privacy plans approved by the authorizing official.
- 1015 **Primary Responsibility:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#).
- 1016 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#); [Chief](#)
1017 [Information Officer](#); [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#).
- 1018 **System Development Life Cycle Phase:** New – Development/Acquisition.
1019 Existing – Operations/Maintenance.
- 1020 **Discussion:** The review of the security and privacy plans by the authorizing official or designated
1021 representative with support from the senior accountable official for risk management or risk executive
1022 (function), chief information officer, senior agency information security officer, and senior agency official
1023 for privacy helps determine if the plans are complete, consistent, and satisfy the stated security and privacy
1024 requirements for the system. Based on the results of this review and analysis, the authorizing official or
1025 designated representative may recommend changes to the security and privacy plans. If the security or
1026 privacy plans are unacceptable, the system owner or common control provider makes appropriate changes
1027 to the plans. If the plans are acceptable, the authorizing official or designated representative approves the
1028 plans. The acceptance of the security and privacy plans represents an important milestone in the SDLC and
1029 risk management process. The authorizing official or designated representative, by approving the security
1030 and privacy plans, agrees to the set of controls (i.e., system-specific, hybrid, or common controls) and the
1031 description of the proposed implementation of the controls to meet the security and privacy requirements
1032 for the system and the environment in which the system operates. The approval of the security and privacy
1033 plans allows the risk management process to proceed to the next step in the RMF (i.e., the implementation
1034 of selected controls). The approval of the security and privacy plans also establishes the appropriate level of
1035 effort required to successfully complete the remainder of the RMF steps and provides the basis of the
1036 security and privacy specifications for the acquisition of the system or system components.
- 1037 **References:** [NIST Special Publication 800-30](#); [NIST Special Publication 800-53](#); [NIST Special](#)
1038 [Publication 800-160, Volume 1](#) (System Requirements Definition, Architecture Definition, and Design
1039 Definition Processes); [CNSS Instruction 1253](#).

1040 **3.4 IMPLEMENT**

1041
 1042
 1043
 1044
 1045
 1046
 1047
 1048
 1049
 1050

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

1051 Table 5 provides a summary of tasks and expected outcomes for the RMF *Implement* step. A
 1052 mapping of Cybersecurity Framework categories, subcategories, and constructs is also provided.

1053

TABLE 5: IMPLEMENT TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 CONTROL IMPLEMENTATION	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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]

1054
 1055

[Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.](#)

1056

CONTROL IMPLEMENTATION

1057

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

1058

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.

1064

Potential Outputs: Implemented controls.

1065

Primary Responsibility: [System Owner](#); [Common Control Provider](#).

1066

Supporting Roles: [Information Owner or Steward](#); [Security or Privacy Architect](#); [Systems Security or Privacy Engineer](#); [System Security or Privacy Officer](#); [Enterprise Architect](#); [System Administrator](#).

1067

1068

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

1069

Existing – Operations/Maintenance.

1070 **Discussion:** Organizations implement the controls listed in the security and privacy plans. The control
1071 implementation is consistent with the organization’s enterprise architecture and the associated security and
1072 privacy architectures. The security and privacy architectures serve as a resource to guide and inform the
1073 allocation of controls to a system or system component. Not all controls need to be allocated to every
1074 system component. Controls providing a specific security or privacy capability are only allocated to those
1075 system components that require the specific security or privacy capability. The security categorization, the
1076 privacy risk assessment, the security and privacy architectures, and the allocation of controls work together
1077 to help achieve a suitable balance between security and privacy protections and the mission-based function
1078 of the system.

1079 Organizations use best practices when implementing controls, including systems security and privacy
1080 engineering methodologies, concepts, and principles. Risk assessments guide and inform decisions
1081 regarding the cost, benefit, and risk trade-offs in using different technologies or policies for control
1082 implementation. Organizations also ensure that mandatory configuration settings are established and
1083 implemented on system components in accordance with federal and organizational policies. When
1084 organizations have no direct control over what controls are implemented in a system component, for
1085 example, in commercial off-the-shelf products, organizations consider the use of system components that
1086 have been tested, evaluated, or validated by approved, independent, third-party assessment facilities (e.g.,
1087 NIST Cryptographic Module Validation Program Testing Laboratories, National Information Assurance
1088 Partnership Common Criteria Testing Laboratories). In addition, organizations address, where applicable,
1089 assurance requirements when implementing controls. Assurance requirements are directed at the activities
1090 that control developers and implementers carry out to increase the level of confidence that the controls are
1091 implemented correctly, operating as intended, and producing the desired outcome with respect to meeting
1092 the security and privacy requirements for the system. The assurance requirements address quality of the
1093 design, development, and implementation of the controls.⁵¹

1094 For the common controls inherited by the system, systems security and privacy engineers with support
1095 from system security and privacy officers, coordinate with the common control provider to determine the
1096 most appropriate way to implement common controls. System owners can refer to the authorization
1097 packages prepared by common control providers when making determinations regarding the adequacy of
1098 common controls inherited by their systems. During implementation, it may be determined that common
1099 controls previously selected to be inherited by the system do not meet the protection needs of the system.
1100 For common controls that do not meet the protection needs of the systems inheriting the controls or when
1101 common controls are found to have unacceptable deficiencies, the system owners identify compensating or
1102 supplementary controls to be implemented. System owners can supplement the common controls with
1103 system-specific or hybrid controls to achieve the required protection for their systems or accept greater risk
1104 with the acknowledgement and approval of the organization. Risk assessments may determine how gaps in
1105 protection needs between systems and common controls affect the overall risk associated with the system,
1106 and how to prioritize the need for compensating or supplementary controls to mitigate specific risks.

1107 Consistent with the flexibility allowed in applying the tasks in the RMF, organizations conduct initial
1108 control assessments during system development and implementation. Conducting such assessments in
1109 parallel with the development and implementation phases of the SDLC facilitates early identification of
1110 deficiencies and provides a cost-effective method for initiating corrective actions. Issues discovered during
1111 these assessments can be referred to authorizing officials for resolution. The results of the initial control
1112 assessments can also be used during the authorize step to avoid delays or costly repetition of assessments.
1113 Assessment results that are subsequently reused in other phases of the SDLC meet the reuse requirements
1114 established by the organization.⁵²

1115 **References:** [FIPS Publication 200](#); [NIST Special Publication 800-30](#); [NIST Special Publication 800-53](#);
1116 [NIST Special Publication 800-53A](#); [NIST Special Publication 800-160, Volume 1](#) (Implementation,
1117 Integration, Verification, and Transition Processes); [NIST Special Publication 800-161](#); [NIST Interagency](#)
1118 [Report 8062](#); [NIST Interagency Report 8179](#); [CNSS Instruction 1253](#).

⁵¹ [NIST Special Publication 800-53](#) provides a list of assurance-related security and privacy controls.

⁵² See the RMF *Assess* step and [NIST Special Publication 800-53A](#) for information on assessments and reuse of assessment results.

- 1119 BASELINE CONFIGURATION
- 1120 **Task 2** Establish the initial configuration baseline for the system by documenting changes to planned
1121 control implementation.
- 1122 **Potential Inputs:** System security and privacy plans; information from control implementation efforts.
- 1123 **Potential Outputs:** System security and privacy plans updated with implementation detail sufficient for
1124 use by assessors; system configuration baseline.
- 1125 **Primary Responsibility:** [System Owner](#); [Common Control Provider](#).
- 1126 **Supporting Roles:** [Information Owner or Steward](#); [Security or Privacy Architect](#); [Systems Security or](#)
1127 [Privacy Engineer](#); [System Security or Privacy Officer](#); [Enterprise Architect](#); [System Administrator](#).
- 1128 **System Development Life Cycle Phase:** New – Development/Acquisition; Implementation/Assessment.
1129 Existing – Operations/Maintenance.
- 1130 **Discussion:** Despite the specific control implementation details in the security and privacy plans and the
1131 system design documents, it is not always possible to implement controls as planned. Therefore, as control
1132 implementations are carried out, the security and privacy plans are updated with as-implemented control
1133 implementation details. The updates include revised descriptions of implemented controls including any
1134 changes to planned inputs, expected behavior, and expected outputs with sufficient detail to support control
1135 assessments. Configuration baselines are established for all aspects of the information system including any
1136 information technology component (i.e., hardware, software, and firmware) configurations and include
1137 configuration settings and other technical implementation details. The configuration baselines are essential
1138 to providing the capability to determine when there are changes to the system, whether those changes are
1139 authorized, and the impact of the changes on the security and privacy posture of the organization and the
1140 system.
- 1141 **References:** [NIST Special Publication 800-53](#); [NIST Special Publication 800-128](#); [NIST Special](#)
1142 [Publication 800-160, Volume 1](#) (Implementation, Integration, Verification, and Transition, Configuration
1143 Management Processes); [CNSS Instruction 1253](#).

1144 **3.5 ASSESS**

1145
 1146
 1147
 1148
 1149
 1150
 1151
 1152
 1153
 1154

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

1155 Table 6 provides a summary of tasks and expected outcomes for the RMF *Assess* step. A mapping
 1156 of Cybersecurity Framework categories, subcategories, and constructs is also provided.

1157

TABLE 6: ASSESS TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 ASSESSOR SELECTION	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Security and privacy assessment reports that provide findings and recommendations are completed.
TASK 5 REMEDIATION ACTIONS	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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]

1158 [Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.](#)

1159 ASSESSOR SELECTION

1160 **Task 1** Select the appropriate assessor or assessment team for the type of assessment to be conducted.

1161 **Potential Inputs:** System security and privacy plans; program management control information; common
1162 control documentation; organizational security and privacy program plans; supply chain risk management
1163 plan; system design documentation; enterprise, security, and privacy architecture information; policies and
1164 procedures applicable to the system.

1165 **Potential Outputs:** Selection of assessor or assessment team responsible for conducting the control
1166 assessment.

1167 **Primary Responsibility:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Senior](#)
1168 [Agency Official for Privacy](#).

1169 **Supporting Roles:** [Senior Agency Information Security Officer](#).

1170 **System Development Life Cycle Phase:** New – Development/Acquisition; Implementation/Assessment.
1171 Existing – Operations/Maintenance.

1172 **Discussion:** Organizations consider both the technical expertise and level of independence required in
1173 selecting control assessors.⁵³ Organizations ensure that control assessors possess the required skills and
1174 technical expertise to develop the assessment plans and to conduct assessments of program management,
1175 system-specific, hybrid, and common controls, as appropriate. This includes general knowledge of risk
1176 management concepts as well as comprehensive knowledge of and experience with the specific hardware,
1177 software, and firmware components implemented. Security control assessments in support of initial and
1178 subsequent system, common, and program management authorizations are conducted by independent
1179 assessors if the system is categorized as moderate or high impact. An independent assessor is an individual
1180 or group capable of conducting an impartial assessment. Impartiality implies that assessors are free from
1181 any perceived or actual conflicts of interest with respect to the determination of control effectiveness or the
1182 development, operation, or management of the system, common controls, or program management
1183 controls.

1184 Independent assessment services can be obtained from within the organization or can be contracted to a
1185 public or private sector entity outside of the organization. Contracted assessment services are considered
1186 independent if the system owner or common control provider is not directly involved in the contracting
1187 process or cannot influence the independence of the assessors conducting the assessment. The authorizing
1188 official or designated representative determines the required level of independence for control assessors
1189 based on the results of the security categorization process and the risk to organizational operations and
1190 assets, individuals, other organizations, and the Nation. In special situations, for example, when the
1191 organization that owns the system is small or the organizational structure requires that the control
1192 assessments be accomplished by individuals that are in the developmental, operational, or management
1193 chain of the system owner, independence in the assessment process can be achieved by ensuring that the
1194 assessment results are carefully reviewed and analyzed by an independent team of experts to validate the
1195 completeness, consistency, and veracity of the results. The authorizing official consults with the Office of
1196 the Inspector General, chief information officer, and senior agency information security officer, to guide
1197 and inform the decisions regarding assessor independence in the types of special circumstances described
1198 above. For assessment of program management controls, the assessor is independent of the entity that
1199 manages and implements the program management controls.

1200 The senior agency official for privacy is responsible for identifying assessment methodologies and metrics
1201 to determine if privacy controls are implemented correctly, operating as intended, and sufficient to ensure
1202 compliance with applicable privacy requirements and manage privacy risks. The senior agency official for
1203 privacy is also responsible for conducting assessments of privacy controls and documenting the results of
1204 the assessments. At the discretion of the organization, privacy controls may be assessed by an independent
1205 assessor. In all cases, however, the senior agency official for privacy is responsible and accountable for the

⁵³ 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.

1206 organization's privacy program, including any privacy functions performed by independent assessors. The
1207 senior agency official for privacy is also responsible for providing privacy-related information to the
1208 authorizing official.

1209 **References:** [FIPS Publication 199](#); [NIST Special Publication 800-30](#); [NIST Special Publication 800-53A](#).

1210 ASSESSMENT PLAN

1211 **Task 2** Develop, review, and approve plans to assess implemented controls.

1212 **Potential Inputs:** System security and privacy plans; program management control information; common
1213 control documentation; organizational security and privacy program plans; supply chain risk management
1214 plan; system design documentation; enterprise, security, and privacy architecture information; policies and
1215 procedures applicable to the system.

1216 **Potential Outputs:** Security and privacy assessment plans approved by the authorizing official.

1217 **Primary Responsibility:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Control](#)
1218 [Assessor](#).

1219 **Supporting Roles:** [Senior Agency Information Security Officer](#); [Senior Agency Official for Privacy](#);
1220 [System Owner](#); [Common Control Provider](#); [Information Owner or Steward](#); [System Security or Privacy](#)
1221 [Officer](#).

1222 **System Development Life Cycle Phase:** New – Development/Acquisition; Implementation/Assessment.
1223 Existing – Operations/Maintenance.

1224 **Discussion:** Security and privacy assessment plans are developed by control assessors based on the
1225 implementation information contained in system security and privacy plans, program management control
1226 documentation, and common control documentation. Organizations may choose to develop a single,
1227 integrated security and privacy assessment plan for the system. An integrated assessment plan clearly
1228 delineates roles and responsibilities for control assessment. Assessment plans provide the objectives for
1229 control assessments and specific assessment procedures for each control. Assessment plans also reflect the
1230 type of assessment the organization is conducting, for example, developmental testing and evaluation;
1231 independent verification and validation; audits, including supply chain; assessments supporting system and
1232 common control authorization or reauthorization; program management control assessments; continuous
1233 monitoring; and assessments conducted after remediation actions.

1234 Assessment plans are reviewed and approved by the authorizing official or the designated representative of
1235 the authorizing official to ensure that the plans are consistent with the security and privacy objectives of the
1236 organization; employ procedures, techniques, tools, and automation to support continuous monitoring and
1237 near real-time risk management; and are cost-effective. Approved assessment plans establish expectations
1238 for the control assessments and the level of effort for the assessment. Approved assessment plans help to
1239 ensure that an appropriate level of resources is applied toward determining control effectiveness while
1240 providing the necessary level of assurance in making such determinations. When controls are provided by
1241 an external provider through contracts, interagency agreements, lines of business arrangements, licensing
1242 agreements, or supply chain arrangements, the organization can request security and privacy assessment
1243 plans and/or assessments results/evidence from the provider.

1244 **References:** [NIST Special Publication 800-53A](#); [NIST Special Publication 800-160, Volume 1](#)
1245 (Verification and Validation Processes); [NIST Special Publication 800-161](#).

1246 CONTROL ASSESSMENTS

1247 **Task 3** Assess the controls in accordance with the assessment procedures described in the security and
1248 privacy assessment plans.

1249 **Potential Inputs:** Security and privacy assessment plans; system security and privacy plans; external
1250 assessment or audit results (if applicable).

- 1251 **Potential Outputs:** Completed control assessments and associated assessment evidence.
- 1252 **Primary Responsibility:** [Control Assessor](#).
- 1253 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [System Owner](#);
1254 [Common Control Provider](#); [Information Owner or Steward](#); [Senior Agency Information Security Officer](#);
1255 [Senior Agency Official for Privacy](#); [System Security or Privacy Officer](#).
- 1256 **System Development Life Cycle Phase:** New – Development/Acquisition; Implementation/Assessment.
1257 Existing – Operations/Maintenance.
- 1258 **Discussion:** Control assessments determine the extent to which the selected controls are implemented
1259 correctly, operating as intended, and producing the desired outcome with respect to meeting the security
1260 and privacy requirements for the system and the organization. The system owner, common control
1261 provider, and/or organization rely on the technical skills and expertise of assessors to assess implemented
1262 controls using the assessment procedures specified in assessment plans and provide recommendations on
1263 how to respond to control deficiencies to reduce or eliminate identified vulnerabilities or unacceptable
1264 risks. The senior agency official for privacy serves as the control assessor for the privacy controls and is
1265 responsible for conducting an initial assessment of the privacy controls prior to operation, and for assessing
1266 the controls periodically thereafter at a frequency sufficient to ensure compliance with applicable privacy
1267 requirements and to manage privacy risks.⁵⁴ The assessor findings are a factual reporting of whether the
1268 controls are operating as intended and whether any deficiencies⁵⁵ in the controls are discovered during the
1269 assessment.
- 1270 Control assessments occur as early as practicable in the SDLC, preferably during the development phase.
1271 These types of assessments are referred to as developmental testing and evaluation and validate that the
1272 controls are implemented correctly and are consistent with the established information security and privacy
1273 architectures. Developmental testing and evaluation activities include, for example, design and code
1274 reviews, regression testing, and application scanning. Security and privacy deficiencies identified early in
1275 the SDLC can be resolved more quickly and in a more cost-effective manner. Assessments may be needed
1276 prior to source selection during the procurement process to assess potential suppliers or providers before
1277 the organization enters into agreements or contracts to begin the development phase. The results of control
1278 assessments during the SDLC can also be used (consistent with reuse criteria) during the authorization
1279 process to avoid unnecessary delays or costly repetition of assessments. Organizations can maximize the
1280 use of automation to conduct control assessments to increase the speed, effectiveness, and efficiency of the
1281 assessments, and to support continuous monitoring of the security and privacy posture of organizational
1282 systems.
- 1283 Applying and assessing controls throughout the development process may be appropriate for iterative
1284 development processes. When iterative development processes such as agile development are employed, an
1285 iterative assessment may be conducted as each cycle is completed. A similar process is used for assessing
1286 controls in commercial information technology products that are used within the system. Organizations
1287 may choose to begin assessing controls prior to the complete implementation of all controls in the security
1288 and privacy plans. This type of incremental assessment is appropriate if it is more efficient or cost-effective
1289 to do so. Common controls (i.e., controls that are inherited by the system) are assessed separately (by
1290 assessors chosen by common control providers or the organization) and need not be assessed as part of a
1291 system-level assessment.
- 1292 Organizations ensure that assessors have access to the information system and environment of operation
1293 where the controls are implemented and to the appropriate documentation, records, artifacts, test results,
1294 and other materials needed to assess the controls. This includes situations when the controls are provided
1295 by external providers through contracts, interagency agreements, lines of business arrangements, licensing
1296 agreements, or supply chain arrangements. In addition, assessors have the required degree of independence

⁵⁴ The senior agency official for privacy can delegate the assessment functions, consistent with applicable policies.

⁵⁵ Only deficiencies in controls that can be exploited by threat agents are considered vulnerabilities.

1297 as determined by the authorizing official.⁵⁶ Security control assessments in support of system and common
1298 control authorizations are conducted by independent assessors if the system is categorized as moderate or
1299 high impact. Assessor independence during continuous monitoring, although not mandated, facilitates reuse
1300 of assessment results to support ongoing authorization and reauthorization, if required.

1301 To make the risk management process more efficient and cost-effective, organizations may choose to
1302 establish reasonable and appropriate criteria for reusing assessment results as part of organization-wide
1303 assessment policy or in the security and privacy program plans. For example, a recent audit of a system
1304 may have produced information about the effectiveness of selected controls. Another opportunity to reuse
1305 previous assessment results may come from external programs that test and evaluate security and privacy
1306 features of commercial information technology products (e.g., NIST Cryptographic Module Validation
1307 Program, Common Criteria Evaluation and Validation Program). If prior assessment results from the
1308 system developer are available, the control assessor, under appropriate circumstances, may incorporate
1309 those results into the assessment. And finally, assessment results can be reused to support reciprocity, for
1310 example, assessment results supporting an authorization to use (see [Appendix F](#)). Additional information
1311 on assessment result reuse is available in [NIST Special Publication 800-53A](#).

1312 **References:** [NIST Special Publication 800-53A](#); [NIST Special Publication 800-160, Volume 1](#)
1313 (Verification and Validation Processes).

1314 SECURITY AND PRIVACY ASSESSMENT REPORTS

1315 **Task 4** Prepare the security and privacy assessment reports documenting the findings and
1316 recommendations from the control assessments.

1317 **Potential Inputs:** Completed control assessments⁵⁷ and associated assessment evidence.

1318 **Potential Outputs:** Completed security and privacy assessment reports detailing the assessor findings and
1319 recommendations.

1320 **Primary Responsibility:** [Control Assessor](#).

1321 **Supporting Roles:** [System Owner](#); [Common Control Provider](#); [System Security or Privacy Officer](#).

1322 **System Development Life Cycle Phase:** New – Development/Acquisition; Implementation/Assessment.
1323 Existing – Operations/Maintenance.

1324 **Discussion:** The results of the security and privacy control assessments, including recommendations for
1325 correcting deficiencies in the implemented controls, are documented in the assessment reports⁵⁸ by control
1326 assessors. Organizations may choose to develop a single, integrated security and privacy assessment report.
1327 Assessment reports are key documents in the system or common control authorization package developed
1328 for authorizing officials. The assessment reports include information based on assessor findings, necessary
1329 to determine the effectiveness of the controls implemented within or inherited by the information system.
1330 Assessment reports are an important factor in a determination of risk to organizational operations and
1331 assets, individuals, other organizations, and the Nation by the authorizing official. The format and level of
1332 detail provided in assessment reports are appropriate for the type of control assessment conducted, for
1333 example, developmental testing and evaluation; independent verification and validation; independent
1334 assessments supporting information system or common control authorizations or reauthorizations; self-
1335 assessments; assessments after remediation actions; assessments during continuous monitoring; and
1336 independent audits or evaluations. The reporting format may also be prescribed by the organization.

⁵⁶ 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.

⁵⁷ 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.

⁵⁸ 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.

1337 Control assessment results obtained during the system development lifecycle are documented in an interim
1338 report, and included in the final security and privacy assessment reports. Development of interim reports
1339 that document assessment results from relevant phases of the SDLC reinforces the concept that assessment
1340 reports are evolving documents. Interim reports are used, as appropriate, to inform the final assessment
1341 report. Organizations may choose to develop an executive summary from the control assessment findings.
1342 The executive summary provides authorizing officials and other interested individuals in the organization
1343 with an abbreviated version of the assessment reports that includes a synopsis of the assessment, findings,
1344 and the recommendations for addressing deficiencies in the controls.

1345 **References:** [NIST Special Publication 800-53A](#); [NIST Special Publication 800-160, Volume 1](#)
1346 (Verification and Validation Processes).

1347 REMEDIATION ACTIONS

1348 **Task 5** Conduct initial remediation actions on the controls based on the findings and recommendations
1349 of the security and privacy assessment reports; reassess remediated controls.

1350 **Potential Inputs:** Completed security and privacy assessment reports with findings and recommendations;
1351 system security and privacy plans; security and privacy assessment plans; organization- and system-level
1352 risk assessment results.

1353 **Potential Outputs:** Completed initial remediation actions based on the security and privacy assessment
1354 reports; changes to implementations reassessed by the assessment team; updated security and privacy
1355 assessment reports; updated system security and privacy plans including any changes to the control
1356 implementations.

1357 **Primary Responsibility:** [System Owner](#); [Common Control Provider](#); [Control Assessor](#).

1358 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Senior Agency](#)
1359 [Information Security Officer](#); [Senior Agency Official for Privacy](#); [System Owner](#); [Information Owner or](#)
1360 [Steward](#); [Systems Security or Privacy Engineer](#); [System Security or Privacy Officer](#).

1361 **System Development Life Cycle Phase:** New – Development/Acquisition; Implementation/Assessment.
1362 Existing – Operations/Maintenance.

1363 **Discussion:** The security and privacy assessment reports describe deficiencies in the controls implemented
1364 within the system or the common controls available for inheritance that could not be resolved during the
1365 development of the system or that are discovered post-development. Such control deficiencies may result in
1366 security and privacy risks. The findings generated during assessments provide information that facilitates a
1367 disciplined and structured approach to responding to those risks in accordance with the organizational risk
1368 tolerance and priorities. Findings from a system-level control assessment may necessitate an update to both
1369 the system risk assessment and the organizational risk assessment.⁵⁹ The updated risk assessment and any
1370 inputs from the senior accountable official for risk management or risk executive (function) determines the
1371 initial remediation actions and the prioritization of those actions. System owners and common control
1372 providers may decide, based on a risk assessment, that certain findings are inconsequential and present no
1373 significant security or privacy risk. Such findings are retained in the security and privacy assessment
1374 reports and monitored during the monitoring step. The authorizing official is responsible for reviewing and
1375 understanding the assessor findings and for accepting the security and privacy risks from operating an
1376 information system or the use of common controls. The authorizing official, in consultation with system
1377 owners and other organizational officials, may decide that certain findings do, in fact, represent significant,
1378 unacceptable risk and require immediate remediation actions.

1379 In all cases, organizations review assessor findings to determine the significance of the findings (i.e., the
1380 potential adverse impact on organizational operations and assets, individuals, other organizations, or the
1381 Nation) and whether the findings warrant any further investigation or remediation. Senior leadership

⁵⁹ 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](#).

1382 involvement in the mitigation process may be necessary to ensure that the organization's resources are
1383 effectively allocated in accordance with organizational priorities, providing resources to the systems that
1384 are supporting the most critical and sensitive missions and business functions or correcting the deficiencies
1385 that pose the greatest risk. If deficiencies in controls are corrected, the assessors reassess the remediated
1386 controls. Control reassessments determine the extent to which the remediated controls are implemented
1387 correctly, operating as intended, and producing the desired outcome with respect to meeting the security
1388 and privacy requirements for the system and the organization. The assessors update the security and
1389 privacy assessment reports with the findings from the reassessment, but do not change the original
1390 assessment results. The security and privacy plans are updated based on the findings of the control
1391 assessments and any remediation actions taken. The updated security and privacy plans reflect the state of
1392 the controls after the initial assessment and any modifications by the system owner or common control
1393 provider in addressing recommendations for corrective actions. At the completion of the control
1394 assessments, the security and privacy plans contain an accurate description of implemented controls,
1395 including compensating controls.

1396 Organizations can prepare an addendum to the security and privacy assessment reports that provides system
1397 owners and common control providers an opportunity to respond to the initial assessment findings. The
1398 addendum may include, for example, information regarding initial remediation actions taken by system
1399 owners or common control providers in response to assessor findings. The addendum can also provide the
1400 system owner's or common control provider's perspective on the findings, including additional explanatory
1401 material, rebutting certain findings, and correcting the record. The addendum does not change or influence
1402 the initial assessor findings provided in the reports. Information provided in the addendum is considered by
1403 authorizing officials when making risk-based authorization decisions. Organizations implement a process
1404 to determine the actions to take regarding the control deficiencies identified during the assessment. This
1405 process can help address the vulnerabilities and risks, false positives, and any other factors that provide
1406 useful information to authorizing officials regarding the security and privacy posture of the system and
1407 organization including the ongoing effectiveness of system-specific, hybrid, and common controls. The
1408 issue resolution process can also ensure that only substantive items are identified and transferred to the plan
1409 of actions and milestones.

1410 **References:** [NIST Special Publication 800-53A](#); [NIST Special Publication 800-160, Volume 1](#)
1411 (Verification and Validation Processes).

1412 PLAN OF ACTION AND MILESTONES

1413 **Task 6** Prepare the plan of action and milestones based on the findings and recommendations of the
1414 security and privacy assessment reports excluding any initial remediation actions taken.

1415 **Potential Inputs:** Updated security and privacy assessment reports; updated system security and privacy
1416 plans; organization- and system-level risk assessment results; organizational risk management strategy and
1417 risk tolerance.

1418 **Potential Outputs:** A plan of action and milestones detailing the findings from the security and privacy
1419 assessment reports that are to be remediated.

1420 **Primary Responsibility:** [System Owner](#); [Common Control Provider](#).

1421 **Supporting Roles:** [Information Owner or Steward](#); [System Security or Privacy Officer](#); [Senior Agency](#)
1422 [Information Security Officer](#); [Senior Agency Official for Privacy](#).

1423 **System Development Life Cycle Phase:** New – Implementation/Assessment.
1424 Existing – Operations/Maintenance.

1425 **Discussion:** The plan of action and milestones, prepared for the authorizing official by the system owner or
1426 the common control provider, is included as part of the authorization package. It describes the actions that
1427 are planned to correct deficiencies in the controls identified during the assessment of the controls and
1428 during continuous monitoring. The plan of action and milestones identifies the tasks to be accomplished
1429 with a recommendation for completion before or after system authorization; resources required to
1430 accomplish the tasks; milestones established to meet the tasks; and the scheduled completion dates for the

1431 milestones and tasks. The plan of action and milestones is reviewed by the authorizing official to ensure
1432 there is agreement with the remediation actions planned to correct the identified deficiencies. It is
1433 subsequently used to monitor progress in completing the actions. Deficiencies are accepted by the
1434 authorizing official as residual risk, or are remediated during the assessment or prior to the submission of
1435 the authorization package to the authorizing official. Plan of action and milestones entries are not necessary
1436 when deficiencies are accepted by the authorizing official as residual risk. However, security and privacy
1437 deficiencies identified during assessment and monitoring are documented in the assessment reports, which
1438 can be retained within an automated security/privacy management and reporting tool to maintain an
1439 effective audit trail. Organizations develop plans of action and milestones based on the results obtained
1440 from control assessments, audits, and continuous monitoring and in accordance with applicable laws,
1441 executive orders, directives, policies, regulations, standards, or guidance.

1442 Organizations implement a consistent process for developing plans of action and milestones that facilitates
1443 a prioritized approach to risk mitigation that is uniform across the organization. A risk assessment guides
1444 the prioritization process for items included in the plan of action and milestones. The process ensures that
1445 plans of action and milestones are informed by the security categorization of the system and privacy risk
1446 assessments; the specific deficiencies in the controls; the criticality of the identified control deficiencies
1447 (i.e., the direct or indirect effect that the deficiencies may have on the security and privacy posture of the
1448 system, and therefore, on the risk exposure of the organization; or the ability of the organization to perform
1449 its mission or business functions); and the organization's proposed risk mitigation approach to address the
1450 identified deficiencies in the controls, including, for example, prioritization of risk mitigation actions and
1451 allocation of risk mitigation resources.

1452 **References:** [NIST Special Publication 800-30](#); [NIST Special Publication 800-53A](#); [NIST Special](#)
1453 [Publication 800-160, Volume 1](#) (Verification and Validation Processes); [NIST Interagency Report 8062](#).

1454 **3.6 AUTHORIZE**

1455
 1456
 1457
 1458
 1459
 1460
 1461
 1462
 1463
 1464
 1465

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

1466 Table 7 provides a summary of tasks and expected outcomes for the RMF *Authorize* step. A
 1467 mapping of Cybersecurity Framework categories, subcategories, and constructs is also provided.

1468

TABLE 7: AUTHORIZE TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 AUTHORIZATION PACKAGE	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> A risk determination by the authorizing official that reflects the risk management strategy including risk tolerance, is rendered.
TASK 3 RISK RESPONSE	<ul style="list-style-type: none"> Risk responses for determined risks are provided. [Cybersecurity Framework: ID.RA-6]
TASK 4 AUTHORIZATION DECISION	<ul style="list-style-type: none"> The authorization for the system or the common controls is approved or denied.
TASK 5 AUTHORIZATION REPORTING	<ul style="list-style-type: none"> Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.

1469
 1470

[Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.](#)

1471 AUTHORIZATION PACKAGE

1472 **Task 1** Assemble the authorization package and submit the package to the authorizing official for an
 1473 authorization decision.

1474 **Potential Inputs:** System security, privacy, and supply chain risk management plans; security and privacy
 1475 assessment reports; plan of action and milestones; supporting assessment evidence or other documentation,
 1476 as required.

1477 **Potential Outputs:** Authorization package (with an executive summary), which may be generated from a
 1478 security or privacy management tool⁶⁰ for submission to the authorizing official.

⁶⁰ 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.

1479 **Primary Responsibility:** [System Owner](#); [Common Control Provider](#); [Senior Agency Official for Privacy](#).⁶¹

1480 **Supporting Roles:** [System Security or Privacy Officer](#); [Senior Agency Information Security Officer](#);

1481 [Control Assessor](#).

1482 **System Development Life Cycle Phase:** New – Implementation/Assessment.

1483 Existing – Operations/Maintenance.

1484 **Discussion:** Authorization packages⁶² include the security and privacy plans, along with the supply chain

1485 risk management plan, security and privacy assessment reports, plans of action and milestones, and an

1486 executive summary. Additional information can be included in the authorization package at the request of

1487 the authorizing official. Organizations maintain version and change control as the information in the

1488 authorization package is updated. Providing timely updates to the security and privacy plans, security and

1489 privacy assessment reports, and plans of action and milestones on an ongoing basis supports the concept of

1490 near real-time risk management and ongoing authorization, and can be used for reauthorization actions, if

1491 required.

1492 The senior agency official for privacy reviews the authorization package for systems that process PII to

1493 ensure compliance with applicable privacy requirements and to manage privacy risks, prior to authorizing

1494 officials making risk determination and acceptance decisions.

1495 The information in the authorization package is used by authorizing officials to make informed, risk-based

1496 decisions. When controls are provided to an organization by an external provider through contracts,

1497 interagency agreements, lines of business arrangements, licensing agreements, or supply chain

1498 arrangements, the organization ensures that the information needed to make risk-based decisions is made

1499 available by the provider.

1500 The authorization package may be provided to the authorizing official in hard copy or electronically, or

1501 may be generated using an automated security/privacy management and reporting tool. Organizations can

1502 use automated support tools in preparing and managing the content of the authorization package. Such tools

1503 provide an effective vehicle for maintaining and updating information for authorizing officials regarding

1504 the ongoing security and privacy posture of information systems within the organization.

1505 When an information system is under ongoing authorization, the authorization package is presented to the

1506 authorizing official via automated reports in order to provide information to the authorizing official in the

1507 most efficient and timely manner possible.⁶³ Information to be presented to the authorizing official in

1508 security and privacy assessment reports is generated in the format and with the frequency determined by

1509 the organization using security and privacy information from the information security and privacy

1510 continuous monitoring programs.

1511 The security and privacy assessment reports presented to the authorizing official includes security and

1512 privacy information regarding implemented system-specific, hybrid, and common controls. The authorizing

1513 official uses, whenever practicable, automated security/privacy management and reporting tools or other

1514 automated methods to access the security and privacy plans and the plans of action and milestones. The

1515 frequency at which the authorization documents are updated is in accordance with the risk management

1516 objectives of the organization using automated or manual update processes.⁶⁴

⁶¹ This role is active for information systems processing PII.

⁶² 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.

⁶³ 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.

⁶⁴ 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.

1517 **References:** [NIST Special Publication 800-18](#); [NIST Special Publication 800-160, Volume 1](#) (Risk
1518 Management Process); [NIST Special Publication 800-161](#) (SCRM Plans).

1519 RISK ANALYSIS AND DETERMINATION

1520 **Task 2** Analyze and determine the risk from the operation or use of the system or the provision of
1521 common controls.

1522 **Potential Inputs:** Authorization package; supporting assessment evidence or other documentation as
1523 required; information provided by the senior accountable official for risk management or risk executive
1524 (function); organizational risk management strategy and risk tolerance; organization- and system-level risk
1525 assessment results.

1526 **Potential Outputs:** Risk determination.

1527 **Primary Responsibility:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#).

1528 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#); [Senior](#)
1529 [Agency Information Security Officer](#); [Senior Agency Official for Privacy](#).

1530 **System Development Life Cycle Phase:** New – Implementation/Assessment.
1531 Existing – Operations/Maintenance.

1532 **Discussion:** The authorizing official or designated representative, in collaboration with the senior agency
1533 information security officer and the senior agency official for privacy (for information systems processing
1534 PII), analyzes the information in the authorization package to verify agreement with and understanding of
1535 risk determinations made by the control assessor, system owner, or common control provider, and finalizes
1536 the determination of risk. Further discussion with the control assessor, system owner, or common control
1537 provider may be necessary to help ensure a thorough understanding of risk by the authorizing official.

1538 Risk assessments are employed, if needed, to provide information⁶⁵ that may influence the risk analysis and
1539 determination. The senior accountable official for risk management or risk executive (function) may
1540 provide information to the authorizing official that is considered in the final determination of risk to
1541 organizational operations and assets, individuals, other organizations, and the Nation resulting from either
1542 the operation or use of the system or the provision of common controls. Such information may include, for
1543 example, organizational risk tolerance, dependencies among systems and controls, mission and business
1544 requirements, the criticality of the missions or business functions supported by the system, or the risk
1545 management strategy.

1546 The authorizing official analyzes the information provided by the senior accountable official for risk
1547 management or risk executive (function) and information provided by the system owner or common control
1548 provider in the authorization package when making a risk determination. The information provided by the
1549 senior accountable official for risk management or risk executive (function) is documented and included, to
1550 the extent it is relevant, as part of the authorization decision (see RMF *Authorize* step, [Task 4](#)). The
1551 authorizing official may also use an automated security management and reporting tool to annotate senior
1552 accountable official for risk management or risk executive (function) input.

1553 When the system is operating under an ongoing authorization, the risk determination task is effectively
1554 unchanged. The authorizing official analyzes the relevant security and privacy information provided by the
1555 automated security/privacy management and reporting tool to determine the current security and privacy
1556 posture of the system.

1557 **References:** [NIST Special Publication 800-30](#); [NIST Special Publication 800-39](#) (Organization,
1558 Mission/Business Process, and System Levels); [NIST Special Publication 800-137](#); [NIST Special](#)
1559 [Publication 800-160, Volume 1](#) (Risk Management Process); [NIST Interagency Report 8062](#).

⁶⁵ [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.

1560 RISK RESPONSE

1561 **Task 3** Identify and implement a preferred course of action in response to the risk determined.

1562 **Potential Inputs:** Authorization package; risk determination; organization- and system-level risk
1563 assessment results.

1564 **Potential Outputs:** Risk responses for determined risks.

1565 **Primary Responsibility:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#).

1566 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#); [Senior](#)
1567 [Agency Information Security Officer](#); [Senior Agency Official for Privacy](#); [System Owner](#) or [Common](#)
1568 [Control Provider](#); [Information Owner or Steward](#); [Systems Security or Privacy Engineer](#); [System Security](#)
1569 [or Privacy Officer](#).

1570 **System Development Life Cycle Phase:** New – Implementation/Assessment.
1571 Existing – Operations/Maintenance.

1572 **Discussion:** After risk is analyzed and determined, organizations can respond to risk in a variety of ways,
1573 including acceptance of risk and mitigation of risk. Existing risk assessment results and risk assessment
1574 techniques may be used to help determine the preferred course of action for the risk response.⁶⁶ When the
1575 response to risk is mitigation, the planned mitigation actions are included in and tracked using the plan of
1576 action and milestones. When the response to risk is acceptance, the deficiency found during the assessment
1577 process remains documented in the security and privacy assessment reports and is monitored for changes to
1578 the risk factors.⁶⁷ Because the authorizing official is the only person who can accept risk, the authorizing
1579 official is responsible for reviewing the assessment reports and the plans of action and milestones and
1580 determining whether identified risks need to be mitigated prior to authorization. Decisions on the most
1581 appropriate course of action for responding to risk may include some form of prioritization. Some risks
1582 may be of greater concern to organizations than other risks. In that case, more resources may need to be
1583 directed at addressing higher-priority risks versus lower-priority risks. This does not necessarily mean that
1584 the lower-priority risks are ignored. Rather, it could mean that fewer resources are directed at addressing
1585 the lower-priority risks, or that the lower-priority risks are addressed later. A key part of the risk-based
1586 decision process is the recognition that regardless of the risk response decisions, there remains a degree of
1587 residual risk. Organizations determine acceptable degrees of residual risk based on organizational risk
1588 tolerance.

1589 **References:** [NIST Special Publication 800-30](#); [NIST Special Publication 800-39](#) (Organization,
1590 Mission/Business Process, and System Levels); [NIST Special Publication 800-160, Volume 1](#) (Risk
1591 Management Process); [NIST Interagency Report 8062](#); [NIST Interagency Report 8179](#); [NIST](#)
1592 [Cybersecurity Framework](#) (Core [Identify Function]).

1593 AUTHORIZATION DECISION

1594 **Task 4** Determine if the risk from the operation or use of the information system or the provision or use
1595 of common controls is acceptable.

1596 **Potential Inputs:** Risk responses for determined risks.

1597 **Potential Outputs:** Authorization to operate, authorization to use, common control authorization; denial of
1598 authorization to operate, denial of authorization to use, denial of common control authorization.

1599 **Primary Responsibility:** [Authorizing Official](#).

⁶⁶ [NIST Special Publication 800-39](#) provides additional information on risk response.

⁶⁷ 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.

1600 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#); [Senior](#)
1601 [Agency Information Security Officer](#); [Senior Agency Official for Privacy](#); [Authorizing Official Designated](#)
1602 [Representative](#).

1603 **System Development Life Cycle Phase:** New – Implementation/Assessment.
1604 Existing – Operations/Maintenance.

1605 **Discussion:** The explicit acceptance of risk is the responsibility of the authorizing official and cannot be
1606 delegated to other officials within the organization. The authorizing official considers many factors when
1607 deciding if the risk to the organization’s operations (including mission, functions, image, and reputation)
1608 and assets, individuals, other organizations, or the Nation, is acceptable. Balancing security and privacy
1609 considerations with mission and business needs is paramount to achieving an acceptable risk-based
1610 authorization decision.⁶⁸ The authorizing official issues an authorization decision for the system or for
1611 organization-designated common controls after reviewing the information in the authorization package,
1612 input from other organizational officials (see RMF *Authorize* step, [Task 2](#)), and other relevant information
1613 that may affect the authorization decision. The authorization package provides the most current information
1614 on the security and privacy posture of the system or the common controls.

1615 The authorization decision is conveyed by the authorizing official to the system owner or common control
1616 provider, and other organizational officials, as appropriate.⁶⁹ The authorization decision also conveys the
1617 specific terms and conditions for the authorization to operate; the authorization termination date or time-
1618 driven authorization frequency; input from the senior accountable official for risk management or risk
1619 executive (function), if provided; and for common control authorizations, the system impact level
1620 supported by the common controls.

1621 For systems, the authorization decision indicates to the system owner whether the system is authorized to
1622 operate or authorized to use, or not authorized to operate or not authorized to use. For common controls, the
1623 authorization decision indicates to the common control provider and to the system owners of inheriting
1624 systems, whether the common controls are authorized to be provided or not authorized to be provided. The
1625 terms and conditions for the common control authorization provide a description of any specific limitations
1626 or restrictions placed on the operation of the system or the controls that must be followed by the system
1627 owner or common control provider.

1628 The authorization termination date is established by the authorizing official and indicates when the
1629 authorization expires. Organizations may eliminate the authorization termination date if the system is
1630 operating under an ongoing authorization—that is, the continuous monitoring program is sufficiently robust
1631 and mature to provide the authorizing official with the needed information to conduct ongoing risk
1632 determination and risk acceptance activities regarding the security and privacy posture of the system and
1633 the ongoing effectiveness of the controls employed within and inherited by the system.

1634 The authorization decision is included with the authorization package and is transmitted to the system
1635 owner or common control provider. Upon receipt of the authorization decision and the authorization
1636 package, the system owner or common control provider acknowledges and implements the terms and
1637 conditions of the authorization. The organization ensures that the authorization package, including the
1638 authorization decision for systems and common controls, is made available to organizational officials
1639 including, for example, system owners inheriting common controls; chief information officers; senior
1640 accountable officials for risk management or risk executive (function); senior agency information security
1641 officers; senior agency officials for privacy; and system security and privacy officers. The authorizing

⁶⁸ 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.

⁶⁹ 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.

1642 official verifies on an ongoing basis as part of continuous monitoring (see RMF *Monitor* step, [Task 2](#)) that
1643 the established terms and conditions for authorization are being followed by the system owner or common
1644 control provider.

1645 When the system is operating under an ongoing authorization, the authorizing official continues to be
1646 responsible and accountable for explicitly understanding and accepting the risk of continuing to operate or
1647 use the system or continuing to provide common controls. Under ongoing authorization, the authorization
1648 frequency is specified in lieu of an authorization termination date. The authorizing official reviews the
1649 information with the specific time-driven authorization frequency defined by the organization as part of the
1650 continuous monitoring strategy and determines if the risk of continued system operation or the provision of
1651 common controls remains acceptable. If the risk remains acceptable, the authorizing official acknowledges
1652 the acceptance in accordance with organizational processes. If not, the authorizing official indicates that the
1653 risk is no longer acceptable and requires further risk response or a full denial of the authorization.

1654 The organization determines the level of formality for the process of communicating and acknowledging
1655 continued risk acceptance by the authorizing official. The authorizing official may continue to establish and
1656 convey the specific terms and conditions to be followed by the system owner or common control provider
1657 for continued authorization to operate, continued common control authorization, or continued authorization
1658 to use. The terms and conditions of the authorization may be conveyed through an automated management
1659 and reporting tool as part of an automated authorization decision.

1660 If control assessments are conducted by qualified assessors with the level of independence⁷⁰ required based
1661 on federal or organizational policies and the requisite security and privacy standards and guidelines, the
1662 assessment results support ongoing authorization and may be applied to a reauthorization. Organizational
1663 policies regarding ongoing authorization and reauthorization are consistent with laws, executive orders,
1664 directives, regulations, and policies.

1665 The authorizing official consults with the Senior Accountable Official for Risk Management or the Risk
1666 Executive (Function) prior to making the final authorization decision for the information system or the
1667 common controls. Because there are potentially significant dependencies among organizational systems
1668 and with external systems, the authorization decisions of individual systems are carried out in consideration
1669 of the current residual risk and PO&AMs of the organization and the risk tolerance of the organization.

1670 [Appendix F](#) provides additional guidance on authorization decisions, the types of authorizations, and the
1671 preparation of the authorization packages.

1672 **References:** [NIST Special Publication 800-39](#) (Organization, Mission/Business Process, and System
1673 Levels); [NIST Special Publication 800-160, Volume 1](#) (Risk Management Process).

1674 AUTHORIZATION REPORTING

1675 **Task 5** Report the authorization decision and any deficiencies in controls that represent significant
1676 security or privacy risk.

1677 **Potential Inputs:** Authorization decision.

1678 **Potential Outputs:** A report indicating the authorization decision for a system or set of common controls;
1679 report containing deficiencies in systems or controls described in the Cybersecurity Framework functions,
1680 categories, and subcategories; annotation of authorization status in the organizational system registry.

1681 **Primary Responsibility:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#).

1682 **Supporting Roles:** [System Owner](#) or [Common Control Provider](#); [Information Owner or Steward](#); [System](#)
1683 [Security or Privacy Officer](#); [Senior Agency Information Security Officer](#); [Senior Agency Official for](#)
1684 [Privacy](#).

⁷⁰ 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.

1685 **System Development Life Cycle Phase:** New – Implementation/Assessment.
1686 Existing – Operations/Maintenance.

1687 **Discussion:** Authorizing officials report authorization decisions for systems and common controls to
1688 designated organizational officials so the individual risk decisions can be viewed in the context of
1689 organization-wide security and privacy risk to organizational operations and assets, individuals, other
1690 organizations, and the Nation. Reporting occurs only in situations where organizations have delegated the
1691 authorization functions to levels of the organization below the head of agency. Authorizing officials also
1692 report exploitable deficiencies (i.e., vulnerabilities) in the system or controls noted during the assessment
1693 and continuous monitoring that represent significant security or privacy risk. Organizations determine, and
1694 the organizational policy reflects, what constitutes a significant security or privacy risk for reporting.
1695 Deficiencies that represent significant vulnerabilities and security/privacy risk can be reported using the
1696 subcategories, categories, and functions described in the NIST Cybersecurity Framework. Authorization
1697 decisions may be tracked and reflected as part of the organization-wide system registration process at the
1698 organization’s discretion (see RMF *Prepare-System Level* step, [Task 10](#)).

1699 **References:** [NIST Special Publication 800-39](#) (Organization, Mission/Business Process, and System
1700 Levels); [NIST Special Publication 800-160, Volume 1](#) (Decision Management and Project Assessment and
1701 Control Processes); [NIST Cybersecurity Framework](#) (Core [Identify, Protect, Detect, Respond, Recover
1702 Functions]).
1703

1704 **3.7 MONITOR**

1705
 1706
 1707
 1708
 1709
 1710
 1711
 1712
 1713
 1714

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

1715 Table 8 provides a summary of tasks and expected outcomes for the RMF *Monitor* step. A
 1716 mapping of Cybersecurity Framework categories, subcategories, and constructs is also provided.

1717

TABLE 8: MONITOR TASKS AND OUTCOMES

Tasks	Outcomes
TASK 1 SYSTEM AND ENVIRONMENT CHANGES	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy.
TASK 3 ONGOING RISK RESPONSE	<ul style="list-style-type: none"> The output of continuous monitoring activities is analyzed and responded to appropriately. [Cybersecurity Framework: RS.AN]
TASK 4 AUTHORIZATION UPDATES	<ul style="list-style-type: none"> Risk management documents are updated based on continuous monitoring activities. [Cybersecurity Framework: RS.IM]
TASK 5 SECURITY AND PRIVACY REPORTING	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> A system disposal strategy is developed and implemented, as needed.

1718
 1719

[Quick link to Appendix E summary table for RMF tasks, responsibilities, and supporting roles.](#)

1720 SYSTEM AND ENVIRONMENT CHANGES

1721 **Task 1** Monitor the information system and its environment of operation for changes that impact the
 1722 security and privacy posture of the system.

1723 **Potential Inputs:** Organizational continuous monitoring strategy; organizational configuration
 1724 management policy and procedures; organizational policy and procedures for handling unauthorized system
 1725 changes; system security and privacy plans; configuration change requests/approvals; system design
 1726 documentation; security and privacy assessment reports; plans of action and milestones; information from
 1727 automated and manual monitoring tools.

1728 **Potential Outputs:** Updated system security and privacy plans; updated plans of action and milestones;
1729 updated security and privacy assessment reports.

1730 **Primary Responsibility:** [System Owner](#) or [Common Control Provider](#); [Senior Agency Information Security](#)
1731 [Officer](#); [Senior Agency Official for Privacy](#).

1732 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#);
1733 [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Information Owner or Steward](#);
1734 [System Security or Privacy Officer](#).

1735 **System Development Life Cycle Phase:** New – Operations/Maintenance.
1736 Existing – Operations/Maintenance.

1737 **Discussion:** Systems are in a constant state of change with changes occurring in the technology or machine
1738 elements, human elements, and physical or environmental elements. Changes to the technology or machine
1739 elements include for example, upgrades to hardware, software, or firmware; changes to the human elements
1740 include for example, staff turnover or a reduction in force; and modifications to the surrounding physical
1741 and environmental elements include for example, changes in the location of the facility or the physical
1742 access controls protecting the facility. A disciplined and structured approach to managing, controlling, and
1743 documenting changes to systems and environments of operation, and adherence with terms and conditions
1744 of the authorization, is an essential element of security and privacy programs. Organizations establish
1745 configuration management and control processes to support configuration and change management.⁷¹

1746 Common activities within organizations can cause changes to systems or the environments of operation and
1747 can have a significant impact on the security and privacy posture of systems. Examples include installing or
1748 disposing of hardware, making changes to configurations, and installing patches outside of the established
1749 configuration change control process. Unauthorized changes may occur because of purposeful attacks by
1750 adversaries or inadvertent errors by authorized personnel. Thus, in addition to adhering to the established
1751 configuration management process, organizations monitor for unauthorized changes to systems and analyze
1752 information about unauthorized changes that have occurred to determine the root cause of the unauthorized
1753 change. In addition to monitoring for unauthorized changes, organizations continuously monitor systems
1754 and environments of operation for any authorized changes that impact the privacy posture of systems.⁷²

1755 Once the root cause of an unauthorized change (or an authorized change that impacts the privacy posture of
1756 the system) has been determined, organizations respond accordingly (see RMF *Monitor* step, [Task 3](#)). For
1757 example, if the root cause of an unauthorized change is determined to be an adversarial attack, multiple
1758 actions could be taken such as invoking incident response processes, adjusting intrusion detection and
1759 prevention tools and firewall configurations, or implementing additional or stronger controls to reduce the
1760 risk of future attacks. If the root cause of an unauthorized change is determined to be a failure of staff to
1761 adhere to established configuration management processes, remedial training for certain individuals may be
1762 warranted.

1763 **References:** [NIST Special Publication 800-30](#); [NIST Special Publication 800-128](#); [NIST Interagency](#)
1764 [Report 8062](#).

1765 ONGOING ASSESSMENTS

1766 **Task 2** Assess the controls implemented within and inherited by the system in accordance with the
1767 continuous monitoring strategy.

1768 **Potential Inputs:** Organizational continuous monitoring strategy and system level continuous monitoring
1769 strategy (if applicable); system security and privacy plans; security and privacy assessment plans; security
1770 and privacy assessment reports; plans of action and milestones; organization- and system-level risk

⁷¹ [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.

⁷² For information about the distinction between authorized and unauthorized system behavior, see the discussion of security and privacy in [Section 2.2](#).

- 1771 assessment results; external assessment or audit results (if applicable); information from automated and
1772 manual monitoring tools.
- 1773 **Potential Outputs:** Updated security and privacy assessment reports.
- 1774 **Primary Responsibility:** [Control Assessor](#).
- 1775 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [System Owner](#)
1776 or [Common Control Provider](#); [Information Owner or Steward](#); [System Security or Privacy Officer](#); [Senior](#)
1777 [Agency Information Security Officer](#); [Senior Agency Official for Privacy](#).
- 1778 **System Development Life Cycle Phase:** New – Operations/Maintenance.
1779 Existing – Operations/Maintenance.
- 1780 **Discussion:** After the initial system or common control authorization, the organization assesses all controls
1781 implemented within and inherited by the system on an ongoing basis. The frequency of monitoring for
1782 control effectiveness is based on the organizational continuous monitoring strategy and can be
1783 supplemented by the system-level continuous monitoring strategy, as needed. Adherence to terms and
1784 conditions specified by the authorizing official as part of the authorization decision are also monitored (see
1785 RMF *Monitor* step, [Task 1](#)).
- 1786 For ongoing control assessments, control assessors have the required degree of independence as determined
1787 by the authorizing official.⁷³ The control assessments in support of the initial and subsequent authorizations
1788 are conducted by independent assessors. Assessor independence during continuous monitoring, although
1789 not mandated, introduces efficiencies into the process and may allow for reuse of assessment results in
1790 support of ongoing authorization and when reauthorization is required.
- 1791 To satisfy the annual FISMA security assessment requirement, organizations can draw upon the assessment
1792 results from any of the following sources, including, for example, security control assessments conducted
1793 as part of authorization, ongoing authorization, or reauthorization; continuous monitoring; or the testing
1794 and evaluation of systems as part of the SDLC or an audit (provided that the assessment results are current,
1795 relevant to the determination of control effectiveness, and obtained by assessors with the required degree of
1796 independence). Existing security assessment results are reused consistent with the reuse policy established
1797 for the organization and are supplemented with additional assessments as needed. The reuse of assessment
1798 results is critical in achieving a cost-effective, fully integrated security program capable of producing the
1799 evidence necessary to determine the security posture of information systems and the organization. The use
1800 of automation to support control assessments facilitates a greater frequency, volume, and coverage of
1801 assessments.
- 1802 **References:** [NIST Special Publication 800-53A](#); [NIST Special Publication 800-137](#); [NIST Special](#)
1803 [Publication 800-160, Volume 1](#) (Verification, Validation, Operation, and Maintenance Processes).
- 1804 **ONGOING RISK RESPONSE**
- 1805 **Task 3** Respond to risk based on the results of ongoing monitoring activities, risk assessments, and
1806 outstanding items in plans of action and milestones.
- 1807 **Potential Inputs:** Security and privacy assessment reports; organization- and system-level risk assessment
1808 results; system security and privacy plans; plans of action and milestones.
- 1809 **Potential Outputs:** Mitigation actions or risk acceptance decisions; updated security and privacy
1810 assessment reports.
- 1811 **Primary Responsibility:** [Authorizing Official](#); [System Owner](#); [Common Control Provider](#).

⁷³ 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.

1812 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#); [Senior](#)
1813 [Agency Official for Privacy](#); [Authorizing Official Designated Representative](#); [Information Owner or](#)
1814 [Steward](#); [System Security or Privacy Officer](#); [Systems Security or Privacy Engineer](#); [Security or Privacy](#)
1815 [Architect](#).

1816 **System Development Life Cycle Phase:** New – Operations/Maintenance.
1817 Existing – Operations/Maintenance.

1818 **Discussion:** Assessment information produced by an assessor during continuous monitoring is provided to
1819 the system owner and the common control provider in updated security and privacy assessment reports or
1820 via reports from automated security/privacy management and reporting tools. The authorizing official
1821 determines the appropriate risk response to the assessment findings or approves responses proposed by the
1822 system owner and common control provider. The system owner and common control provider subsequently
1823 implement the appropriate risk response. When the response to risk is acceptance, the findings remain
1824 documented in the security and privacy assessment reports and are monitored for changes to risk factors.
1825 When the response to risk is mitigation, the planned mitigation actions are included in and tracked using
1826 the plans of action and milestones. Control assessors may, if called upon, provide recommendations for
1827 remediation actions. Recommendations for remediation actions may also be provided by an automated
1828 security/privacy management and reporting tool. An organizational assessment of risk (RMF *Prepare-*
1829 *Organization Level* step, [Task 3](#)) and system-level risk assessment results (RMF *Prepare-System Level*
1830 step, [Task 7](#)) help inform the decisions regarding ongoing risk response. Controls that are modified,
1831 enhanced, or added as part of ongoing risk response are reassessed by assessors to ensure that the new,
1832 modified, or enhanced controls have been implemented correctly, are operating as intended, and producing
1833 the desired outcome with respect to meeting the security and privacy requirements of the system.

1834 **References:** [NIST Special Publication 800-30](#); [NIST Special Publication 800-53](#); [NIST Special](#)
1835 [Publication 800-53A](#); [NIST Special Publication 800-137](#); [NIST Special Publication 800-160, Volume 1](#)
1836 (Risk Management Process); [NIST Interagency Report 8062](#); [NIST Cybersecurity Framework](#) (Core
1837 [Respond Functions]); [CNSS Instruction 1253](#).

1838 AUTHORIZATION UPDATES

1839 **Task 4** Update security and privacy plans, security and privacy assessment reports, and plans of action
1840 and milestones based on the results of the continuous monitoring process.

1841 **Potential Inputs:** Security and privacy assessment reports; organization- and system-level risk assessment
1842 results; system security and privacy plans; plans of action and milestones.

1843 **Potential Outputs:** Updated security and privacy assessment reports;⁷⁴ updated plans of action and
1844 milestones; updated risk assessment results; updated system security and privacy plans.

1845 **Primary Responsibility:** [System Owner](#); [Common Control Provider](#).

1846 **Supporting Roles:** [Information Owner or Steward](#); [System Security or Privacy Officer](#); [Senior Agency](#)
1847 [Official for Privacy](#).

1848 **System Development Life Cycle Phase:** New – Operations/Maintenance.
1849 Existing – Operations/Maintenance.

1850 **Discussion:** To achieve near real-time risk management, the organization updates security and privacy
1851 plans, security and privacy assessment reports, and plans of action and milestones on an ongoing basis.
1852 Updates to the security and privacy plans reflect any modifications to controls based on risk mitigation
1853 activities carried out by system owners or common control providers. Updates to control assessment reports
1854 reflect the additional assessment activities carried out to determine control effectiveness based on
1855 implementation details in the security and privacy plans. Plans of action and milestones are updated based

⁷⁴ 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.

1856 on progress made on the current outstanding items listed in the plan; address security and privacy risks
1857 discovered as part of control effectiveness monitoring; and describe how the system owner or common
1858 control provider intends to address those security and privacy risks. The updated information raises
1859 awareness of the security and privacy posture of the system and the common controls inherited by the
1860 system, thereby, supporting near real-time risk management and the ongoing authorization process.

1861 The frequency of updates to risk management-related information is at the discretion of the system owner,
1862 common control provider, and authorizing officials in accordance with federal and organizational policies
1863 and is consistent with the organizational and system-level continuous monitoring strategies. The updates to
1864 information regarding the security and privacy posture of the system and the common controls inherited by
1865 the system are accurate and timely since the information provided influences ongoing security and privacy
1866 actions and decisions by authorizing officials and other senior leaders within the organization. The use of
1867 automated support tools and organization-wide security and privacy program management practices help
1868 ensure that authorizing officials can readily access the current security and privacy posture of the system.
1869 This provides essential information for continuous monitoring and ongoing authorization and promotes the
1870 near real-time management of risk to organizational operations and assets, individuals, other organizations,
1871 and the Nation.

1872 Organizations ensure that information needed for oversight, management, and auditing purposes is not
1873 modified or destroyed when updating security and privacy plans, security and privacy assessment reports,
1874 and plans of action and milestones. Providing an effective method of tracking changes to systems through
1875 configuration management procedures is necessary to achieve transparency and traceability in the security
1876 and privacy activities of the organization; to obtain individual accountability for any security- and privacy-
1877 related actions; and to understand emerging trends in the security and privacy programs of the organization.

1878 **References:** [NIST Special Publication 800-53A](#).

1879 SECURITY AND PRIVACY POSTURE REPORTING

1880 **Task 5** Report the security and privacy posture of the system to the authorizing official and other
1881 organizational officials on an ongoing basis in accordance with the organizational continuous
1882 monitoring strategy.

1883 **Potential Inputs:** Security and privacy assessment reports; plans of action and milestones; organization-
1884 and system-level risk assessment results; organization- and system-level continuous monitoring strategy;
1885 system security and privacy plans.

1886 **Potential Outputs:** Security and privacy posture reports.

1887 **Primary Responsibility:** [System Owner](#); [Common Control Provider](#); [Senior Agency Information Security](#)
1888 [Officer](#); [Senior Agency Official for Privacy](#).

1889 **Supporting Roles:** [System Security or Privacy Officer](#).

1890
1891 **System Development Life Cycle Phase:** New – Operations/Maintenance.
1892 Existing – Operations/Maintenance.

1893 **Discussion:** The results of monitoring activities are documented and reported to the authorizing official and
1894 other selected organizational officials on an ongoing basis in accordance with the organizational continuous
1895 monitoring strategy. Other organizational officials who may receive security and privacy posture reports
1896 include, for example, chief information officer, senior agency information security officer, senior agency
1897 official for privacy, senior agency official for risk management or risk executive (function), information
1898 owner or steward, incident response roles, and contingency planning roles. Security and privacy posture
1899 reporting can be event-driven, time-driven, or event- and time-driven.⁷⁵ The reports provide the authorizing
1900 official and other organizational officials with information regarding the security and privacy posture of the
1901 systems including the effectiveness of implemented controls. Security and privacy posture reports describe

⁷⁵ See [Appendix F](#) for more information about time- and event-driven authorizations and reporting.

1902 the ongoing monitoring activities employed by system owners or common control providers. The reports
1903 also include information about security and privacy risks in the systems and environments of operation
1904 discovered during control assessments, auditing, and continuous monitoring and how system owners or
1905 common control providers plan to address those risks.

1906 Organizations have flexibility in the breadth, depth, formality, form, and format of security and privacy
1907 posture reports. The goal is efficient ongoing communication with the authorizing official and other
1908 organizational officials as necessary, conveying the current security and privacy posture of systems and
1909 environments of operation and how the current posture affects individuals, organizational missions, and
1910 business functions. At a minimum, security and privacy posture reports summarize changes to the security
1911 and privacy plans, security and privacy assessment reports, and plans of action and milestones that have
1912 occurred since the last report. The use of automated security/privacy management and reporting tools by
1913 the organization facilitates the effectiveness and timeliness of security and privacy posture reporting.

1914 The frequency of security and privacy posture reports is at the discretion of the organization and in
1915 compliance with federal and organizational policies. Reports occur at appropriate intervals to transmit
1916 security- and privacy-related information about systems or common controls but not so frequently as to
1917 generate unnecessary work or expense. Authorizing officials use the security and privacy posture reports
1918 and consult with the senior accountable official for risk management or risk executive (function), senior
1919 agency information security officer, and senior agency official for privacy to determine if a reauthorization
1920 action is necessary. Security and privacy posture reports are marked, protected, and handled in accordance
1921 with federal and organizational policies. Security and privacy posture reports can be used to satisfy FISMA
1922 reporting requirements for documenting remediation actions for security- and privacy-related weaknesses
1923 or deficiencies. Such reporting is intended to be ongoing and should not be interpreted as requiring the
1924 time, expense, and formality associated with the information provided for the initial authorization. Rather,
1925 reporting is conducted in a cost-effective manner consistent with achieving the reporting objectives.

1926 **References:** [NIST Special Publication 800-53A](#); [NIST Special Publication 800-137](#); [NIST Cybersecurity](#)
1927 [Framework](#) (Core [Identify, Protect, Detect, Respond, Recover Functions]).

1928 ONGOING AUTHORIZATION

1929 **Task 6** Review the security and privacy posture of the system on an ongoing basis to determine whether
1930 the risk remains acceptable.

1931 **Potential Inputs:** Security and privacy posture reports;⁷⁶ plans of action and milestones; organization- and
1932 system-level risk assessment results; system security and privacy plans.

1933 **Potential Outputs:** A determination of risk; ongoing authorization to operate, ongoing authorization to use,
1934 ongoing common control authorization; denial of ongoing authorization to operate, denial of ongoing
1935 authorization to use, denial of ongoing common control authorization.

1936 **Primary Responsibility:** [Authorizing Official](#).

1937 **Supporting Roles:** [Senior Accountable Official for Risk Management](#) or [Risk Executive \(Function\)](#); [Senior](#)
1938 [Agency Information Security Officer](#); [Senior Agency Official for Privacy](#); [Authorizing Official Designated](#)
1939 [Representative](#).

1940 **System Development Life Cycle Phase:** New – Operations/Maintenance.
1941 Existing – Operations/Maintenance.

1942 **Task Discussion:** In accordance with the guidance in the RMF *Authorize* step, [Task 4](#), the authorizing
1943 official or designated representative reviews the security and privacy posture of the system (including the
1944 effectiveness of implemented controls) on an ongoing basis, to determine the current risk to organizational
1945 operations and assets, individuals, other organizations, or the Nation. The authorizing official determines

⁷⁶ 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.

- 1946 whether the current risk is acceptable and provides appropriate direction to the system owner or common
1947 control provider.
- 1948 The risks may change based on the information provided in the security and privacy posture reports
1949 because the reports may indicate changes to any of the security or privacy risk factors. Determining how
1950 changing conditions affect organizational mission or business risk is essential for managing privacy risk
1951 and maintaining adequate security. By carrying out ongoing risk determination and risk acceptance,
1952 authorizing officials can maintain system and common control authorizations over time and transition to
1953 ongoing authorization. Reauthorization actions occur only in accordance with federal or organizational
1954 policies. The authorizing official conveys updated risk determination and acceptance results to the senior
1955 accountable official for risk management or the risk executive (function).
- 1956 The use of automated support tools to capture, organize, quantify, visually display, and maintain security
1957 and privacy posture information promotes near real-time risk management regarding the risk posture of the
1958 organization. The use of metrics and dashboards increases an organization's capability to make risk-based
1959 decisions by consolidating data in an automated fashion and providing the data to decision makers at
1960 different levels within the organization in an easy-to-understand format.
- 1961 **References:** [NIST Special Publication 800-30](#); [NIST Special Publication 800-39](#) (Organization,
1962 Mission/Business Process, and System Levels), [NIST Special Publication 800-160, Volume 1](#) (Risk
1963 Management Process); [NIST Interagency Report 8062](#).
- 1964 SYSTEM DISPOSAL
- 1965 **Task 7** Implement a system disposal strategy and execute required actions when a system is removed
1966 from operation.
- 1967 **Potential Inputs:** System security and privacy plans; organization- and system-level risk assessment
1968 results; system component inventory.
- 1969 **Potential Outputs:** Disposal strategy; updated system component inventory; updated system security and
1970 privacy plans.
- 1971 **Primary Responsibility:** [System Owner](#).
- 1972 **Supporting Roles:** [Authorizing Official](#) or [Authorizing Official Designated Representative](#); [Information](#)
1973 [Owner or Steward](#); [System Security or Privacy Officer](#); [Senior Accountable Official for Risk Management](#)
1974 or [Risk Executive \(Function\)](#); [Senior Agency Information Security Officer](#); [Senior Agency Official for](#)
1975 [Privacy](#).
- 1976 **System Development Life Cycle Phase:** New – Not Applicable.
1977 Existing – Disposal.
- 1978 **Discussion:** When a system is removed from operation, several risk management-related actions are
1979 required. Organizations ensure that all controls addressing system disposal are implemented. Examples
1980 include media sanitization; configuration management and control; and record retention. Organizational
1981 tracking and management systems (including inventory systems) are updated to indicate the specific system
1982 that is being removed from service. Security and privacy posture reports reflect the security and privacy
1983 status of the system. Users and application owners hosted on the disposed system are notified as
1984 appropriate, and any control inheritance relationships are reviewed and assessed for impact. This task also
1985 applies to system components that are removed from operation. Organizations that remove a system from
1986 operation update the inventory of information systems to reflect the removal of the system.
- 1987 **References:** [NIST Special Publication 800-30](#); [NIST Special Publication 800-88](#); [NIST Interagency Report](#)
1988 [8062](#).
- 1989
- 1990

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

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/csrf/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

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 <i>Control Assessment</i> .
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. <i>Note 1:</i> 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. <i>Note 2:</i> 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 <i>authentication</i> .
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 <i>control baseline</i> .
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 <i>Senior Agency Information Security Officer</i> .
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 <i>system component</i> .

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. <i>Note:</i> 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 <i>assessor</i> .
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 <i>common control</i> .
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 <i>security controls</i> and <i>safeguards</i> .
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 <i>organization</i> .
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 <i>executive agency</i> .
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 <i>hardware</i> and <i>software</i> .
hardware [CNSSI 4009]	The material physical components of a system. See <i>software</i> and <i>firmware</i> .
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 <i>common control</i> and <i>system-specific control</i> .

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 <i>authorization boundary</i> .
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 <i>system component</i> .
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 [CNSI 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 <i>operational technology</i> .
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 <i>tailoring</i> and <i>tailored control baseline</i> .
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. <i>Note:</i> 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	<p>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.</p> <p><i>Note:</i> The term <i>privacy requirement</i> 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.</p>

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 [CNSI 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 <i>security category</i> .
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 <i>control baseline</i> .
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. <i>See system security plan.</i>
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 <i>security status</i> .
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. <i>Note:</i> 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 <i>information system</i> . <i>Note:</i> 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. <i>Note 1:</i> 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. <i>Note 2:</i> The interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities. <i>Note 3:</i> System of systems is included in the definition of system.
system boundary	See <i>authorization boundary</i> .
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 <i>security plan</i> .
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 <i>risk</i> .
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 <i>risk</i> .
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 <i>tailoring</i> and <i>overlay</i> .
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 <i>overlay</i> .

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 <i>threat agent</i> .
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. <i>Note:</i> The term <i>weakness</i> is synonymous for <i>deficiency</i> . 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

1 APPENDIX D

2 ROLES AND RESPONSIBILITIES

3 KEY PARTICIPANTS IN THE RISK MANAGEMENT PROCESS

4 The following sections describe the roles and responsibilities of key participants involved in
5 an organization's risk management process.⁷⁷ Recognizing that organizations have varying
6 missions, business functions, and organizational structures, there may be differences in
7 naming conventions for risk management roles and how risk management responsibilities are
8 allocated among organizational personnel. This includes, for example, multiple individuals filling
9 a single role or one individual filling multiple roles.⁷⁸ However, the basic functions remain the
10 same. The application of the RMF described in this publication is flexible, allowing organizations
11 to effectively accomplish the intent of the specific tasks within their respective organizational
12 structures to best manage security and privacy risks. Many risk management roles defined in this
13 publication have counterpart roles defined in the SDLC processes carried out by organizations.
14 Organizations align their risk management roles with similar (or complementary) roles defined
15 for the SDLC whenever possible.⁷⁹

16 AUTHORIZING OFFICIAL

17 The *authorizing official* is a senior official or executive with the authority to formally assume
18 responsibility and accountability for operating a system; providing common controls inherited by
19 organizational systems; or using a system, service, or application from an external provider—and
20 is the only organizational official who can accept the security and privacy risk to organizational
21 operations, organizational assets, and individuals.⁸⁰ Authorizing officials typically have budgetary
22 oversight for the system or are responsible for the mission and/or business operations supported
23 by the system. Accordingly, authorizing officials are in management positions with a level of
24 authority commensurate with understanding and accepting such security and privacy risks.
25 Authorizing officials approve plans, memorandums of agreement or understanding, plans of
26 action and milestones, and determine whether significant changes in the systems or environments
27 of operation require reauthorization.

28 Authorizing officials coordinate their activities with common control providers, system owners,
29 chief information officers, senior agency information security officers, senior agency officials for
30 privacy, system security and privacy officers, control assessors, senior accountable officials for
31 risk management/risk executive (function), and other interested parties during the authorization
32 process. With the increasing complexity of mission/business processes, partnership arrangements,
33 and the use of shared services, it is possible that a system may involve co-authorizing officials.⁸¹
34 If so, agreements are established between the co-authorizing officials and documented in the
35 security and privacy plans. Authorizing officials are responsible and accountable for ensuring that

⁷⁷ Organizations may define other roles to support the risk management process.

⁷⁸ 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](#).

⁷⁹ 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.

⁸⁰ 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.

⁸¹ [OMB Circular A-130](#) provides additional information about authorizing officials and co-authorizing officials.

36 activities and functions associated with authorization that are delegated to authorizing official
37 designated representatives are carried out as specified. The role of authorizing official is an
38 inherent U.S. Government function and is assigned to government personnel only.

39 **AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE**

40 The *authorizing official designated representative* is an organizational official designated by the
41 authorizing official who is empowered to act on behalf of the authorizing official to coordinate
42 and conduct the day-to-day activities associated with managing risk to information systems and
43 organizations. This includes carrying out many of the activities related to the execution of the
44 RMF. The only activity that cannot be delegated by the authorizing official to the designated
45 representative is the authorization decision and signing of the associated authorization decision
46 document (i.e., the acceptance of risk).

47 **CHIEF INFORMATION OFFICER**

48 The *chief information officer*⁸² is an organizational official responsible for designating a senior
49 agency information security officer; developing and maintaining security policies, procedures,
50 and control techniques to address applicable requirements; overseeing personnel with significant
51 responsibilities for security and ensuring that the personnel are adequately trained; assisting
52 senior organizational officials concerning their security responsibilities; and reporting to the head
53 of the agency on the effectiveness of the organization's security program, including progress of
54 remedial actions. The chief information officer, with the support of the risk executive (function)
55 and the senior agency information security officer, works closely with authorizing officials and
56 their designated representatives to help ensure that:

- 57 • An organization-wide security program is effectively implemented resulting in adequate
58 security for all organizational systems and environments of operation;
- 59 • Security and supply chain risk management considerations are integrated into
60 programming/planning/budgeting cycles, enterprise architectures, the SDLC, and
61 acquisitions;
- 62 • Organizational systems and common controls are covered by approved security plans and
63 possess current authorizations;
- 64 • Security-related activities required across the organization are accomplished in an efficient,
65 cost-effective, and timely manner; and
- 66 • There is centralized reporting of security-related activities.

67 The chief information officer and authorizing officials determine the allocation of resources
68 dedicated to the protection of systems supporting the organization's missions and business
69 functions based on organizational priorities. For information systems that process personally
70 identifiable information, the chief information officer and authorizing officials coordinate any
71 determination about the allocation of resources dedicated to the protection of those information
72 systems with the senior agency official for privacy. For selected systems, the chief information
73 officer may be designated as an authorizing official or a co-authorizing official with other senior
74 organizational officials. The role of chief information officer is an inherent U.S. Government
75 function and is assigned to government personnel only.

⁸² 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.

76 COMMON CONTROL PROVIDER

77 The *common control provider* is an individual, group, or organization that is responsible for the
78 implementation, assessment, and monitoring of common controls (i.e., controls inherited by
79 organizational systems).⁸³ Common control providers also are responsible for ensuring the
80 documentation of organization-defined common controls in security and privacy plans (or the
81 equivalent documents prescribed by the organization); ensuring that required assessments of the
82 common controls are conducted by qualified assessors with an appropriate level of independence;
83 documenting assessment findings in control assessment reports; and producing plans of action
84 and milestones for controls having deficiencies. Security and privacy plans, security and privacy
85 assessment reports, and plans of action and milestones for common controls (or summary of such
86 information) are made available to the system owners of systems inheriting common controls
87 after the information is reviewed and approved by the authorizing officials accountable for those
88 common controls.

89 The senior agency official for privacy is responsible for designating which privacy controls may
90 be treated as common controls. Privacy controls that are designated as common controls are
91 documented in the organization's privacy program plan.⁸⁴ The senior agency official for privacy
92 has oversight responsibility for common controls in place or planned for meeting applicable
93 privacy requirements and managing privacy risks and is responsible for assessing those controls.
94 At the discretion of the organization, privacy controls that are designated as common controls
95 may be assessed by an independent assessor. In all cases, however, the senior agency official for
96 privacy retains responsibility and accountability for the organization's privacy program, including
97 any privacy functions performed by independent assessors. Privacy plans and privacy control
98 assessment reports are made available to systems owners whose systems inherit privacy controls
99 that are designated as common controls.

100 CONTRACTING OFFICER REPRESENTATIVE

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

105 CONTROL ASSESSOR

106 The *control assessor* is an individual, group, or organization responsible for conducting a
107 comprehensive assessment of the controls and control enhancements implemented within or
108 inherited by a system to determine the effectiveness of the controls (i.e., the extent to which the
109 controls are implemented correctly, operating as intended, and producing the desired outcome
110 with respect to meeting the security and privacy requirements for the system). The system owner
111 and common control provider rely on the security and privacy expertise and judgment of the
112 assessor to assess the controls implemented within and inherited by the system using the

⁸³ 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.

⁸⁴ 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.

113 assessment procedures specified in the security and privacy assessment plans. Multiple control
114 assessors who are differentiated by their expertise in specific control requirements or technologies
115 may be required to accurately conduct the assessment. Prior to initiating the control assessment,
116 assessors review the security and privacy plans to facilitate development of the security
117 assessment plan. Control assessors provide an assessment of the severity of the deficiencies
118 discovered in the system and its environment of operation and can recommend corrective actions
119 to address identified vulnerabilities. Finally, control assessors prepare security and privacy
120 assessment reports containing the results and findings from the assessment.

121 The required level of assessor independence is determined by the conditions of the control
122 assessment. When a security control assessment is conducted in support of an authorization
123 decision or ongoing authorization, the authorizing official makes an explicit determination of the
124 degree of independence required in accordance with federal policies, directives, standards, and
125 guidelines. Assessor independence is an important factor in preserving an impartial and unbiased
126 assessment process; determining the credibility of the assessment results; and ensuring that the
127 authorizing official receives objective information to make an informed, risk-based authorization
128 decision.

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

135 **ENTERPRISE ARCHITECT**

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

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

154

155 HEAD OF AGENCY

156 The *head of agency* is the senior official in an organization with the responsibility for ensuring
157 that privacy interests are protected and that PII is managed responsibly within the organization.
158 The agency head is also responsible for providing security protections commensurate with the
159 risk to organizational operations, organizational assets, individuals, other organizations, and the
160 Nation—that is, risk resulting from unauthorized access, use, disclosure, disruption, modification,
161 or destruction of information collected or maintained by or on behalf of the agency; and the
162 information systems used or operated by an agency or by a contractor of an agency or other
163 organization on behalf of an agency. The heads of agencies ensure that:

- 164 • Information security and privacy management processes are integrated with strategic and
165 operational planning processes;
- 166 • Senior officials within the organization provide information security for the information and
167 systems that support the operations and assets under their control;
- 168 • Senior agency officials for privacy are designated who are responsible and accountable for
169 ensuring compliance with applicable privacy requirements, managing privacy risk, and the
170 organization’s privacy program; and
- 171 • The organization has adequately trained personnel to assist in complying with security and
172 privacy requirements in legislation, executive orders, policies, directives, instructions,
173 standards, and guidelines.

174 The head of agency establishes the organizational commitment to security and privacy and the
175 actions required to effectively manage security and privacy risk and protect the missions and
176 business functions being carried out by the organization. The head of agency or establishes
177 security and privacy accountability and provides active support and oversight of monitoring and
178 improvement for the security and privacy programs. Senior leadership commitment to security
179 and privacy establishes a level of due diligence within the organization that promotes a climate
180 for mission and business success.

181 INFORMATION OWNER OR STEWARD

182 The *information owner or steward* is an organizational official with statutory, management, or
183 operational authority for specified information and the responsibility for establishing the policies
184 and procedures governing its generation, collection, processing, dissemination, and disposal. In
185 information-sharing environments, the information owner/steward is responsible for establishing
186 the rules for appropriate use and protection of the information and retains that responsibility even
187 when the information is shared with or provided to other organizations. The owner/steward of the
188 information processed, stored, or transmitted by a system may or may not be the same individual
189 as the system owner. An individual system may contain information from multiple information
190 owners/stewards. Information owners/stewards provide input to system owners regarding the
191 security and privacy requirements and controls for the systems where the information is
192 processed, stored, or transmitted.

193 MISSION OR BUSINESS OWNER

194 The *mission or business owner* is the senior official or executive within an organization with
195 specific mission or line of business responsibilities and that has a security and privacy interest in
196 the organizational systems supporting those missions or lines of business. Mission or business
197 owners are key stakeholders that have a significant role in establishing organizational mission and

198 business processes and the protection needs and security and privacy requirements that ensure the
199 successful conduct of the organization's missions and business operations. Mission and business
200 owners provide essential inputs to the risk management strategy, play an active part in the SDLC,
201 and may also serve in the role of authorizing official.

202 **RISK EXECUTIVE (FUNCTION)**

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

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

216 The risk executive (function) coordinates with senior leaders and executives to:

- 217 • Establish risk management roles and responsibilities;
- 218 • Develop and implement an organization-wide *risk management strategy* that provides a
219 strategic view of security-related risks for the organization⁸⁵ and that guides and informs
220 organizational risk decisions (including how risk is framed, assessed, responded to, and
221 monitored over time);
- 222 • Provide a comprehensive, organization-wide, holistic approach for addressing risk—an
223 approach that provides a greater understanding of the integrated operations of the
224 organization;
- 225 • Manage threat, vulnerability, and security/privacy risk information for organizational systems
226 and the environments in which the systems operate;
- 227 • Establish organization-wide forums to consider all types and sources of risk (including
228 aggregated risk);
- 229 • Identify the organizational risk posture based on the aggregated risk from the operation and
230 use of systems and the respective environments of operation for which the organization is
231 responsible;
- 232 • Provide oversight for the risk management activities carried out by organizations to help
233 ensure consistent and effective risk-based decisions;
- 234 • Develop a broad-based understanding of risk regarding the strategic view of organizations
235 and their integrated operations;

⁸⁵ 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.

- 236 • Establish effective vehicles and serve as a focal point for communicating and sharing risk-
237 related information among key stakeholders (e.g., authorization officials and other senior
238 leaders) internally and externally to organizations;
- 239 • Specify the degree of autonomy for subordinate organizations permitted by parent
240 organizations regarding framing, assessing, responding to, and monitoring risk;
- 241 • Promote cooperation and collaboration among authorizing officials to include authorization
242 actions requiring shared responsibility (e.g., joint authorizations);
- 243 • Provide an organization-wide forum to consider all sources of risk (including aggregated risk)
244 to organizational operations and assets, individuals, other organizations, and the Nation;
- 245 • Ensure that authorization decisions consider all factors necessary for mission and business
246 success; and
- 247 • Ensure shared responsibility for supporting organizational missions and business functions
248 using external providers receives the needed visibility and is elevated to appropriate decision-
249 making authorities.

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

261 **SECURITY OR PRIVACY ARCHITECT**

262 The *security or privacy architect* is an individual, group, or organization responsible for ensuring
263 that the stakeholder security and privacy requirements necessary to protect the organization's
264 mission and business processes are adequately addressed in all aspects of enterprise architecture
265 including reference models, segment and solution architectures, and the systems supporting those
266 missions and business processes. The security or privacy architect serves as the primary liaison
267 between the enterprise architect and the systems security or privacy engineer and coordinates
268 with system owners, common control providers, and system security or privacy officers on the
269 allocation of controls. Security or privacy architects, in coordination with system security or
270 privacy officers, advise authorizing officials, chief information officers, senior accountable
271 officials for risk management or risk executive (function), senior agency information security
272 officers, and senior agency officials for privacy on a range of security and privacy issues.
273 Examples include establishing authorization boundaries; establishing security or privacy alerts;
274 assessing the severity of deficiencies in the system or controls; developing effective plans of
275 action and milestones; creating risk mitigation approaches; and potential adverse effects of
276 identified vulnerabilities or privacy risks.

277 **SENIOR ACCOUNTABLE OFFICIAL FOR RISK MANAGEMENT**

278 The *senior accountable official for risk management* is the individual that leads and manages the
279 risk executive (function) in an organization and is responsible for aligning information security

280 management processes with strategic, operational, and budgetary planning processes. This
281 official is the agency head or an individual designated by the agency head.

282 The senior accountable official for risk management determines the organizational structure and
283 responsibilities of the risk executive (function). The head of the agency, in coordination with the
284 senior accountable official for risk management, may retain the risk executive (function) or
285 delegate the function to another organizational official or group. The senior accountable official
286 for risk management and the risk executive (function) are inherent U.S. Government functions
287 and are assigned to government personnel only.

288 **SENIOR AGENCY INFORMATION SECURITY OFFICER**

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

304 **SENIOR AGENCY OFFICIAL FOR PRIVACY**

305 The *senior agency official for privacy* is the senior official or executive with agency-wide
306 responsibility and accountability for ensuring compliance with applicable privacy requirements
307 and managing privacy risk. Among other things, the senior agency official for privacy is
308 responsible for: coordinating with the senior agency information security officer to ensure
309 coordination of privacy and information security activities; reviewing and approving the
310 categorization of information systems that create, collect, use, process, store, maintain,
311 disseminate, disclose, or dispose of personally identifiable information; designating which
312 privacy controls will be treated as program management, common, system-specific, and hybrid
313 privacy controls; identifying assessment methodologies and metrics to determine whether privacy
314 controls are implemented correctly, operating as intended, and sufficient to ensure compliance
315 with applicable privacy requirements and manage privacy risks; reviewing and approving privacy
316 plans for information systems prior to authorization, reauthorization, or ongoing authorization;
317 reviewing authorization packages for information systems that create, collect, use, process, store,
318 maintain, disseminate, disclose, or dispose of personally identifiable information to ensure
319 compliance with privacy requirements and manage privacy risks; conducting and documenting
320 the results of privacy control assessments to verify the continued effectiveness of all privacy
321 controls selected and implemented at the agency; and establishing and maintaining a privacy
322 continuous monitoring program to maintain ongoing awareness of privacy risks and assess
323 privacy controls at a frequency sufficient to ensure compliance with privacy requirements and
324 manage privacy risks.

325

326 SYSTEM ADMINISTRATOR

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

332 SYSTEM OWNER

333 The *system owner* is an organizational official responsible for the procurement, development,
334 integration, modification, operation, maintenance, and disposal of a system.⁸⁶ The system owner
335 is responsible for addressing the operational interests of the user community (i.e., users who
336 require access to the system to satisfy mission, business, or operational requirements) and for
337 ensuring compliance with security requirements. In coordination with the system security and
338 privacy officers, the system owner is responsible for the development and maintenance of the
339 security and privacy plans and ensures that the system is deployed and operated in accordance
340 with the selected and implemented controls. In coordination with the information owner/steward,
341 the system owner is responsible for deciding who has access to the system (and with what types
342 of privileges or access rights)⁸⁷ and ensures that system users and support personnel receive the
343 requisite security and privacy training. Based on guidance from the authorizing official, the
344 system owner informs organizational officials of the need to conduct the authorization, ensures
345 that the necessary resources are available for the effort, and provides the required system access,
346 information, and documentation to control assessors. The system owner receives the security and
347 privacy assessment results from the control assessors. After taking appropriate steps to reduce or
348 eliminate vulnerabilities or privacy risks, the system owner assembles the authorization package
349 and submits the package to the authorizing official or the authorizing official designated
350 representative for adjudication.⁸⁸

351 SYSTEM SECURITY OR PRIVACY OFFICER

352 The *system security or privacy officer*⁸⁹ is an individual responsible for ensuring that the security
353 and privacy posture is maintained for an organizational system and works in close collaboration
354 with the system owner. The system security or privacy officer also serves as a principal advisor
355 on all matters, technical and otherwise, involving the controls for the system. The system security
356 or privacy officer has the knowledge and expertise to manage the security or privacy aspects of an
357 organizational system and, in many organizations, is assigned responsibility for the day-to-day
358 system security or privacy operations. This responsibility may also include, but is not limited to,
359 physical and environmental protection; personnel security; incident handling; and security and
360 privacy training and awareness. The system security or privacy officer may be called upon to
361 assist in the development of the system-level security or privacy policies and procedures and to

⁸⁶ Organizations may refer to system owners as program managers or business/asset owners.

⁸⁷ 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.

⁸⁸ 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.

⁸⁹ 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.

362 ensure compliance with those policies and procedures. In close coordination with the system
363 owner, the system security or privacy officer often plays an active role in the monitoring of a
364 system and its environment of operation to include developing and updating security and privacy
365 plans, managing and controlling changes to the system, and assessing the security or privacy
366 impact of those changes.

367 **SYSTEM USER**

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

373 **SYSTEMS SECURITY OR PRIVACY ENGINEER**

374 The *systems security or privacy engineer* is an individual, group, or organization responsible for
375 conducting systems security or privacy engineering activities as part of the SDLC. Systems
376 security and privacy engineering is a process that captures and refines security or privacy
377 requirements for systems and helps to ensure that the requirements are effectively integrated into
378 systems and system components through security or privacy architecting, design, development,
379 and configuration. Systems security or privacy engineers are an integral part of the development
380 team—designing and developing organizational systems or upgrading existing systems. Systems
381 security or privacy engineers employ best practices when implementing controls within a system
382 including software engineering methodologies; system and security or privacy engineering
383 principles; secure or privacy-enhancing design, secure or privacy-enhancing architecture, and
384 secure or privacy-enhancing coding techniques. Systems security or privacy engineers coordinate
385 security- and privacy-related activities with senior agency information security officers, senior
386 agency officials for privacy, security and privacy architects, system owners, common control
387 providers, and system security or privacy officers.

APPENDIX E

SUMMARY OF RMF TASKS

RMF TASKS, RESPONSIBILITIES, AND SUPPORTING ROLES

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

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
Organization Level		
<p><u>TASK 1</u> Risk Management Roles Identify and assign individuals to specific roles associated with security and privacy risk management.</p>	<ul style="list-style-type: none"> • Head of Agency • Chief Information Officer • Senior Agency Official for Privacy 	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative • Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer
<p><u>TASK 2</u> Risk Management Strategy Establish a risk management strategy for the organization that includes a determination of risk tolerance.</p>	<ul style="list-style-type: none"> • Head of Agency 	<ul style="list-style-type: none"> • Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
<p><u>TASK 3</u> Risk Assessment—Organization Assess organization-wide security and privacy risk and update the results on an ongoing basis.</p>	<ul style="list-style-type: none"> • Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy 	<ul style="list-style-type: none"> • Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative
<p><u>TASK 4</u> Organization-Wide Tailored Control Baselines and Profiles (Optional) Establish, document, and publish organization-wide tailored control baselines and/or profiles.</p>	<ul style="list-style-type: none"> • Mission or Business Owner • Senior Accountable Official for Risk Management or Risk Executive (Function) 	<ul style="list-style-type: none"> • Chief Information Officer • Authorizing Official or Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy
<p><u>TASK 5</u> Common Control Identification Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.</p>	<ul style="list-style-type: none"> • Senior Agency Information Security Officer • Senior Agency Official for Privacy 	<ul style="list-style-type: none"> • 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
<p>TASK 6 Impact-Level Prioritization (Optional) Prioritize organizational systems with the same impact level.</p>	<ul style="list-style-type: none"> • Senior Accountable Official for Risk Management or Risk Executive (Function) 	<ul style="list-style-type: none"> • 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
<p>TASK 7 Continuous Monitoring Strategy—Organization Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.</p>	<ul style="list-style-type: none"> • Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Official for Privacy 	<ul style="list-style-type: none"> • Chief Information Officer • Senior Agency Information Security Officer • Mission or Business Owner • System Owner • Authorizing Official or Authorizing Official Designated Representative
System Level		
<p>TASK 1 Mission or Business Focus Identify the missions, business functions, and mission/business processes that the system is intended to support.</p>	<ul style="list-style-type: none"> • Mission or Business Owner 	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative • System Owner • Information Owner or Steward • Senior Agency Information Security Officer • Senior Agency Official for Privacy
<p>TASK 2 Organizational Stakeholders Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.</p>	<ul style="list-style-type: none"> • System Owner 	<ul style="list-style-type: none"> • 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
<p>TASK 3 Asset Identification Identify assets that require protection.</p>	<ul style="list-style-type: none"> • System Owner 	<ul style="list-style-type: none"> • 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
<p>TASK 4 Authorization Boundary Determine the authorization boundary of the system.</p>	<ul style="list-style-type: none"> • System Owner 	<ul style="list-style-type: none"> • 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
<p><u>TASK 5</u> Information Types Identify the types of information to be processed, stored, and transmitted by the system.</p>	<ul style="list-style-type: none"> • System Owner • Information Owner or Steward 	<ul style="list-style-type: none"> • System Security or Privacy Officer • Mission or Business Owner
<p><u>TASK 6</u> Information Life Cycle For systems that process PII, identify and understand all parts of the information life cycle.</p>	<ul style="list-style-type: none"> • Senior Agency Official for Privacy • System Owner • Information Owner or Steward 	<ul style="list-style-type: none"> • Chief Information Officer • Mission or Business Owner
<p><u>TASK 7</u> Risk Assessment (System) Conduct a system-level risk assessment and update the risk assessment on an ongoing basis.</p>	<ul style="list-style-type: none"> • System Owner • System Security or Privacy Officer 	<ul style="list-style-type: none"> • 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
<p><u>TASK 8</u> Protection Needs—Security and Privacy Requirements Define the protection needs and security and privacy requirements for the system.</p>	<ul style="list-style-type: none"> • Mission or Business Owner • System Owner • Information Owner or Steward • System Security or Privacy Officer 	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative • Senior Agency Information Security Officer • Senior Agency Official for Privacy
<p><u>TASK 9</u> Enterprise Architecture Determine the placement of the system within the enterprise architecture.</p>	<ul style="list-style-type: none"> • Mission or Business Owner • Enterprise Architect • Security or Privacy Architect 	<ul style="list-style-type: none"> • 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
<p><u>TASK 10</u> System Registration Register the system with organizational program or management offices.</p>	<ul style="list-style-type: none"> • System Owner 	<ul style="list-style-type: none"> • 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
<p><u>TASK 1</u> Security Categorization Categorize the system and document the security categorization results.</p>	<ul style="list-style-type: none"> • System Owner • Information Owner or Steward 	<ul style="list-style-type: none"> • 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
<p><u>TASK 2</u> Security Categorization Review and Approval Review and approve the security categorization results and decision.</p>	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative • Senior Agency Official for Privacy (for systems processing PII) 	<ul style="list-style-type: none"> • Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy
<p><u>TASK 3</u> System Description Document the characteristics of the system.</p>	<ul style="list-style-type: none"> • System Owner 	<ul style="list-style-type: none"> • 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
<p><u>TASK 1</u> Security and Privacy Requirements Allocation Allocate security and privacy requirements to the information system and to the environment in which the system operates.</p>	<ul style="list-style-type: none"> • Security Architect • Privacy Architect or System Privacy Officer 	<ul style="list-style-type: none"> • 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
<p><u>TASK 2</u> Control Selection Select the controls for the system.</p>	<ul style="list-style-type: none"> • System Owner • Common Control Provider 	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Systems Security or Privacy Engineer • System Security or Privacy Officer
<p><u>TASK 3</u> Control Tailoring Tailor the controls selected for the system.</p>	<ul style="list-style-type: none"> • System Owner • Common Control Provider 	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Systems Security or Privacy Engineer • System Security or Privacy Officer
<p><u>TASK 4</u> Security and Privacy Plans Document the security and privacy controls for the system in security and privacy plans.</p>	<ul style="list-style-type: none"> • System Owner • Common Control Provider 	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative • Information Owner or Steward • Systems Security or Privacy Engineer • System Security or Privacy Officer
<p><u>TASK 5</u> Continuous Monitoring Strategy—System Develop and implement a system-level strategy for monitoring control effectiveness to supplement the organizational continuous monitoring strategy</p>	<ul style="list-style-type: none"> • System Owner • Common Control Provider 	<ul style="list-style-type: none"> • 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
<p><u>TASK 6</u> Security and Privacy Plan Review and Approval Review and approve the security and privacy plans for the system.</p>	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative 	<ul style="list-style-type: none"> • Senior Accountable Official for Risk Management or Risk Executive (Function) • Chief Information Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy.

DRAFT

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

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
<p><u>TASK 1</u> Control Implementation Implement the controls specified in the security and privacy plans.</p>	<ul style="list-style-type: none"> • System Owner • Common Control Provider 	<ul style="list-style-type: none"> • Information Owner or Steward • Security or Privacy Architect • Systems Security or Privacy Engineer • System Security or Privacy Officer • Enterprise Architect • System Administrator
<p><u>TASK 2</u> Baseline Configuration Establish the initial configuration baseline for the system by documenting changes to planned control implementation.</p>	<ul style="list-style-type: none"> • System Owner • Common Control Provider 	<ul style="list-style-type: none"> • Information Owner or Steward • Security or Privacy Architect • Systems Security or Privacy Engineer • System Security or Privacy Officer • Enterprise Architect • System Administrator

DRAFT

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

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
<p>TASK 1 Assessor Selection Select the appropriate assessor or assessment team for the type of assessment to be conducted.</p>	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative • Senior Agency Official for Privacy 	<ul style="list-style-type: none"> • Senior Agency Information Security Officer
<p>TASK 2 Assessment Plan Develop, review, and approve plans to assess implemented controls.</p>	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative • Control Assessor 	<ul style="list-style-type: none"> • Senior Agency Information Security Officer • Senior Agency Official for Privacy • System Owner • Common Control Provider • Information Owner or Steward • System Security or Privacy Officer
<p>TASK 3 Control Assessments Assess the security and privacy controls in accordance with the assessment procedures described in the security and privacy assessment plans.</p>	<ul style="list-style-type: none"> • Control Assessor 	<ul style="list-style-type: none"> • 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
<p>TASK 4 Security and Privacy Assessment Reports Prepare the security and privacy assessment reports documenting the findings and recommendations from the control assessments.</p>	<ul style="list-style-type: none"> • Control Assessor 	<ul style="list-style-type: none"> • System Owner • Common Control Provider • System Security or Privacy Officer
<p>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.</p>	<ul style="list-style-type: none"> • System Owner • Common Control Provider • Control Assessor 	<ul style="list-style-type: none"> • 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
<p><u>TASK 6</u></p> <p>Plan of Action and Milestones</p> <p>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.</p>	<ul style="list-style-type: none"> • System Owner • Common Control Provider 	<ul style="list-style-type: none"> • Information Owner or Steward • System Security or Privacy Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy

DRAFT

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

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
<p>TASK 1 Authorization Package Assemble the authorization package and submit the package to the authorizing official for an authorization decision.</p>	<ul style="list-style-type: none"> • System Owner • Common Control Provider 	<ul style="list-style-type: none"> • System Security or Privacy Officer • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Control Assessor
<p>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.</p>	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative 	<ul style="list-style-type: none"> • Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy
<p>TASK 3 Risk Response Identify and implement a preferred course of action in response to the risk determined.</p>	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative 	<ul style="list-style-type: none"> • 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
<p>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.</p>	<ul style="list-style-type: none"> • Authorizing Official 	<ul style="list-style-type: none"> • Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Authorizing Official Designated Representative
<p>TASK 5 Authorization Reporting Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.</p>	<ul style="list-style-type: none"> • Authorizing Official or Authorizing Official Designated Representative 	<ul style="list-style-type: none"> • 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
<p>TASK 1</p> <p>System and Environment Changes</p> <p>Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.</p>	<ul style="list-style-type: none"> • System Owner or Common Control Provider • Senior Agency Information Security Officer • Senior Agency Official for Privacy 	<ul style="list-style-type: none"> • 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
<p>TASK 2</p> <p>Ongoing Assessments</p> <p>Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy.</p>	<ul style="list-style-type: none"> • Control Assessor 	<ul style="list-style-type: none"> • 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
<p>TASK 3</p> <p>Ongoing Risk Response</p> <p>Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones.</p>	<ul style="list-style-type: none"> • Authorizing Official • System Owner • Common Control Provider 	<ul style="list-style-type: none"> • 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
<p>TASK 4</p> <p>Authorization Updates</p> <p>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.</p>	<ul style="list-style-type: none"> • System Owner • Common Control Provider 	<ul style="list-style-type: none"> • Information Owner or Steward • System Security or Privacy Officer • Senior Agency Official for Privacy
<p>TASK 5</p> <p>Security and Privacy Posture Reporting</p> <p>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.</p>	<ul style="list-style-type: none"> • System Owner • Common Control Provider • Senior Agency Information Security Officer • Senior Agency Official for Privacy 	<ul style="list-style-type: none"> • System Security or Privacy Officer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
<p><u>TASK 6</u></p> <p>Ongoing Authorization</p> <p>Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.</p>	<ul style="list-style-type: none"> • Authorizing Official 	<ul style="list-style-type: none"> • Senior Accountable Official for Risk Management or Risk Executive (Function) • Senior Agency Information Security Officer • Senior Agency Official for Privacy • Authorizing Official Designated Representative
<p><u>TASK 7</u></p> <p>System Disposal</p> <p>Implement a system disposal strategy and execute required actions when a system is removed from operation.</p>	<ul style="list-style-type: none"> • System Owner 	<ul style="list-style-type: none"> • 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

DRAFT

1 APPENDIX F

2 **SYSTEM AND COMMON CONTROL AUTHORIZATIONS**

3 AUTHORIZATION DECISIONS AND SUPPORTING EVIDENCE

4 **T**his appendix provides information on the system and common control authorization
5 processes to include: types of authorizations; content of authorization packages;
6 authorization decisions; authorization decision documents; ongoing authorization;
7 reauthorization; event-driven triggers and significant changes; type and facility authorizations;
8 and authorization approaches.

9 **TYPES OF AUTHORIZATIONS**

10 Authorization is the process by which a senior management official, the *authorizing official*,
11 reviews security- and privacy-related information describing the current security and privacy
12 posture of information systems or common controls that are inherited by systems. The authorizing
13 official uses this information to determine if the mission/business risk of operating a system or
14 providing common controls is acceptable—and if it is, explicitly accepts the risk. Security- and
15 privacy-related information is presented to the authorizing official in an authorization package,
16 which may consist of a report from an automated security/privacy management and reporting
17 tool.⁹⁰ System and common control authorization occurs as part of the RMF *Authorize* step. A
18 system authorization or a common control authorization can be an initial authorization, an
19 ongoing authorization, or a reauthorization as defined below:

- 20 • *Initial authorization* is defined as the initial (start-up) risk determination and risk acceptance
21 decision based on a complete, zero-base review of the system or of common controls. The
22 zero-base review of the system includes an assessment of all implemented system-level
23 controls (including the system-level portion of the hybrid controls) and a review of the
24 security status of inherited common controls as specified in security and privacy plans.⁹¹ The
25 zero-base review of common controls (other than common controls that are system-based)
26 includes an assessment of all applicable controls (e.g., policies, operating procedures,
27 implementation information) that contribute to the provision of a common control or set of
28 common controls.
- 29 • *Ongoing authorization* is defined as the subsequent (follow-on) risk determinations and risk
30 acceptance decisions taken at agreed-upon and documented frequencies in accordance with
31 the organization's mission/business requirements and organizational risk tolerance. Ongoing
32 authorization is a time-driven or event-driven authorization process whereby the authorizing
33 official is provided with the necessary and sufficient information regarding the near real-time
34 security and privacy posture of the system to determine whether the mission/business risk of
35 continued system operation or the provision of common controls is acceptable. Ongoing
36 authorization is fundamentally related to the ongoing understanding and ongoing acceptance
37 of security and privacy risk and is dependent on a robust continuous monitoring program.

⁹⁰ [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.

⁹¹ 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.

- 38 • *Reauthorization* is defined as the static, single point-in-time risk determination and risk
39 acceptance decision that occurs after initial authorization. In general, reauthorization actions
40 may be time-driven or event-driven. However, under ongoing authorization, reauthorization
41 is in most instances, an event-driven action initiated by the authorizing official or directed by
42 the senior accountable official for risk management or risk executive (function) in response to
43 an event that results in security and/or privacy risk above the level of risk previously accepted
44 by the authorizing official. Reauthorization consists of a review of the system or the common
45 controls similar to the review carried out during the initial authorization. The reauthorization
46 differs from the initial authorization because the authorizing official can choose to initiate a
47 complete zero-base review of the system or of the common controls or to initiate a targeted
48 review based on the type of event that triggered the reauthorization. Reauthorization is a
49 separate activity from the ongoing authorization process. However, security- and privacy-
50 related information generated from the organization's continuous monitoring program may be
51 leveraged to support reauthorization. Reauthorization actions may necessitate a review of and
52 changes to the organization's information security and privacy continuous monitoring
53 strategies which may in turn affect ongoing authorization.

54 **AUTHORIZATION PACKAGE**

55 The *authorization package* provides a record of the results of the control assessments and
56 provides the authorizing official with the information needed to make a risk-based decision on
57 whether to authorize the operation of a system or common controls.⁹² The system owner or
58 common control provider is responsible for the development, compilation, and submission of the
59 authorization package. This includes information available from reports generated by an
60 automated security/privacy management and reporting tool. The system owner or common
61 control provider receives inputs from many sources during the preparation of the authorization
62 package including, for example: senior agency information security officer; senior agency official
63 for privacy, senior accountable official for risk management or risk executive (function); control
64 assessors; system security or privacy officer; and the continuous monitoring program. The
65 authorization package⁹³ includes the following:

- 66 • Executive summary;
- 67 • Security and privacy plans;⁹⁴
- 68 • Security and privacy assessment reports;⁹⁵ and
- 69 • Plans of action and milestones.

70 The executive summary provides a consolidated view of the security- and privacy-related
71 information in the authorization package. The executive summary helps to identify and highlight
72 risk management issues associated with protecting organizational systems and the environments
73 in which the systems operate. It provides the necessary and sufficient information needed by the
74 authorization official to understand the security and privacy risks to the organization's operations

⁹² 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.

⁹³ The authorizing official determines what additional supporting information or references may be required to be included in the authorization package.

⁹⁴ [NIST Special Publication 800-18](#) provides guidance on security plans. Guidance on privacy plans will be addressed in future updates to this publication.

⁹⁵ [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.

75 and assets, individuals, other organizations, and the Nation—and to use that information to make
76 informed, risk-based decisions regarding the operation and use of the system or the provision of
77 common controls that can be inherited by organizational systems.

78 The security and privacy plans provide an overview of the security and privacy requirements and
79 describe the controls in place or planned for meeting those requirements. The plans provide
80 sufficient information to understand the intended or actual implementation of the controls
81 implemented within the system and indicate the controls that are implemented via inherited
82 common controls. Additionally, privacy plans specifically describe the methodologies and
83 metrics that will be used to assess the controls. The security and privacy plans may also include
84 as supporting appendices or as references, additional security- and privacy-related documents
85 such as a privacy impact assessment, interconnection security agreements, security and privacy
86 configurations, contingency plan, configuration management plan, incident response plan, and
87 system-level continuous monitoring strategy. The security and privacy plans are updated
88 whenever events dictate changes to the controls implemented within or inherited by the system.

89 The security and privacy assessment reports, prepared by the control assessor or generated by
90 automated security/privacy management and reporting tools, provide the findings and results of
91 assessing the implementation of the security and privacy controls identified in the security and
92 privacy plans to determine the extent to which the controls are implemented correctly, operating
93 as intended, and producing the desired outcome with respect to meeting the specified security and
94 privacy requirements. The security and privacy assessment reports may contain recommended
95 corrective actions for deficiencies identified in the security and privacy controls.⁹⁶

96 Supporting the near real-time risk management objectives of the authorization process, the
97 security and privacy assessment reports are updated on an ongoing basis whenever changes are
98 made to the security and privacy controls implemented within or inherited by the system.⁹⁷
99 Updates to the assessment reports help to ensure that system owners, common control providers,
100 and authorizing officials maintain an awareness of control effectiveness. The effectiveness of the
101 security and privacy controls directly affects the security and privacy posture of the system and
102 decisions regarding explicit acceptance of risk.

103 The plan of action and milestones, prepared by the system owner or common control provider,
104 describes the specific measures planned to correct deficiencies identified in the security and
105 privacy controls during the assessment; and to address known vulnerabilities or privacy risks in
106 the system.⁹⁸ The content and structure of plans of action and milestones are informed by the risk
107 management strategy developed as part of the risk executive (function) and are consistent with
108 the plans of action and milestones process established by the organization which include any
109 specific requirements defined in federal laws, executive orders, policies, directives, or standards.
110 If the systems and the environments in which those systems operate have more vulnerabilities
111 than available resources can realistically address, organizations develop and implement plans of

⁹⁶ 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.

⁹⁷ 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.

⁹⁸ Implementation information about mitigation actions from plans of actions and milestones is documented in the system security plan.

112 action and milestones that facilitate a prioritized approach to risk mitigation and that is consistent
113 across the organization. This ensures that plans of action and milestones are based on:

- 114 • The security categorization of the system and privacy risk assessment;
- 115 • The specific deficiencies in the controls;
- 116 • The criticality of the control deficiencies (i.e., the direct or indirect effect the deficiencies
117 may have on the overall security and privacy posture of the system and hence on the risk
118 exposure⁹⁹ of the organization);
- 119 • The risk mitigation approach of the organization to address the identified deficiencies in the
120 controls; and
- 121 • The rationale for accepting certain deficiencies in the controls.

122 Organizational strategies for plans of action and milestones are guided and informed by the
123 security categorization of the systems affected by the risk mitigation activities. Organizations
124 may decide, for example, to allocate their risk mitigation resources initially to the highest-impact
125 systems or other high-value assets because a failure to correct the known deficiencies in those
126 systems or assets could potentially have the most significant adverse effects on their missions or
127 business functions. Organizations prioritize deficiencies using information from risk assessments
128 and the risk management strategy developed as part of the risk executive (function). Therefore, a
129 high-impact system would have a prioritized list of deficiencies for that system, and similarly for
130 moderate-impact and low-impact systems.

131 **AUTHORIZATION DECISIONS**

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

- 134 • Authorization to Operate;
- 135 • Common Control Authorization;
- 136 • Authorization to Use; and
- 137 • Denial of Authorization.

138 ***Authorization to Operate***

139 If the authorizing official, after reviewing the authorization package, determines that the risk to
140 organizational operations, organizational assets, individuals, other organizations, and the Nation
141 is acceptable, an *authorization to operate* is issued for the information system. The system is
142 authorized to operate for a specified period in accordance with the terms and conditions
143 established by the authorizing official. An *authorization termination date* is established by the
144 authorizing official as a condition of the authorization. The authorization termination date can be
145 adjusted at any time by the authorizing official to reflect an increased level of concern regarding
146 the security and privacy posture of the system. For example, the authorizing official may choose
147 to authorize the system to operate only for a short time if it is necessary to test a system in the
148 operational environment before all controls are fully in place, (i.e., the authorization to operate is
149 strictly limited to the time needed to complete the testing objectives).¹⁰⁰ The authorizing official

⁹⁹ 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.

¹⁰⁰ Formerly referred to as an interim authority to test.

150 may choose to include operating restrictions such as limiting logical and physical access to a
151 minimum number of users; restricting system use time periods; employing enhanced or increased
152 audit logging, scanning, and monitoring; or restricting system functionality to include only the
153 functions that require live testing.

154 The authorizing official considers results from the assessment of controls that are fully or
155 partially implemented since if the system is ready to be tested in a live environment, many of the
156 controls should already be in place. If the system is under ongoing authorization, a time-driven
157 authorization frequency is specified. Additionally, within any authorization type, an adverse event
158 could occur that triggers the need to review the authorization to operate.¹⁰¹

159 **Common Control Authorization**

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

168 Common controls are authorized for a specific time period in accordance with the terms and
169 conditions established by the authorizing official and the organization. An *authorization*
170 *termination date* is established by the authorizing official as a condition of the initial common
171 control authorization. The termination date can be adjusted at any time to reflect the level of
172 concern by the authorizing official regarding the security and privacy posture of the common
173 controls that are available for inheritance. If the controls are under ongoing authorization, a time-
174 driven authorization frequency is specified. Within any authorization type, an adverse event could
175 occur that triggers the need to review the common control authorization. Common controls that
176 are implemented in a system do not require a separate common control authorization because they
177 receive an authorization to operate as part of the system authorization to operate.¹⁰²

178 **Authorization to Use**

179 An *authorization to use* applies to cloud and shared systems, services, and applications and is
180 employed when an organization (hereafter referred to as the customer organization) chooses to
181 accept the information in an existing authorization package generated by another organization
182 (hereafter referred to as the provider organization).¹⁰³ An authorization to use is issued by a
183 designated authorizing official from the customer organization in lieu of an authorization to
184 operate. The authorizing official issuing an authorization to use has the same level of risk

¹⁰¹ Additional information on event-driven triggers is provided below.

¹⁰² 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.

¹⁰³ 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.

185 management responsibility and authority as an authorizing official issuing an authorization to
186 operate or a common control authorization.¹⁰⁴

187 The acceptance of the information in the authorization package from the provider organization is
188 based on a need to use shared information technology resources, including for example, a system,
189 an application, or a service. A customer organization can issue an authorization to use only after a
190 valid authorization to operate has been issued by the provider organization.¹⁰⁵ The provider
191 organization's authorization (to operate) is a statement of the acceptance of risk for the system,
192 service, or application being provided. The customer organization's authorization (to use) is a
193 statement of the customer's acceptance of risk for the system, service, or application being used
194 with respect to the customer's information. An authorization to use provides opportunities for
195 significant cost savings and avoids a potentially costly and time-consuming authorization process
196 by the customer organization.

197 An authorization to use requires the customer organization to review the authorization package
198 from the provider organization as the fundamental basis for determining risk.¹⁰⁶ When reviewing
199 the authorization package, the customer organization considers various risk factors such as the
200 time elapsed since the authorization results were produced; the environment of operation (if
201 different from the environment reflected in the authorization package); the impact level of the
202 information to be processed, stored, or transmitted; and the overall risk tolerance of the customer
203 organization. If the customer organization plans to integrate the shared system, application, or
204 service with one or more of its systems, the customer organization considers the risk in doing so.

205 If the customer organization determines that there is insufficient information in the provider
206 authorization package or inadequate controls in place for establishing an acceptable level of risk,
207 the organization may negotiate with the provider organization and request additional controls or
208 security- and privacy-related information. This may include for example, supplementing controls
209 for risk reduction; implementing compensating controls; conducting additional or more rigorous
210 assessments; or establishing constraints on the use of the system, application, or service provided.
211 The request for additional security- and privacy-related information may include information the
212 provider organization produced or discovered in the use of the system that is not reflected in the
213 authorization package. When the provider organization does not provide the requested controls,
214 the customer organization may choose to implement additional controls to reduce risk to an
215 acceptable level.

216 Once the customer organization is satisfied with the security and privacy posture of the shared or
217 cloud system, application, or service (as reflected in the current authorization package) and the
218 risk of using the shared or cloud system, application, or service has been sufficiently mitigated,
219 the customer organization issues an authorization to use in which the customer organization
220 explicitly understands and accepts the security and privacy risk incurred by using the shared

¹⁰⁴ 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.

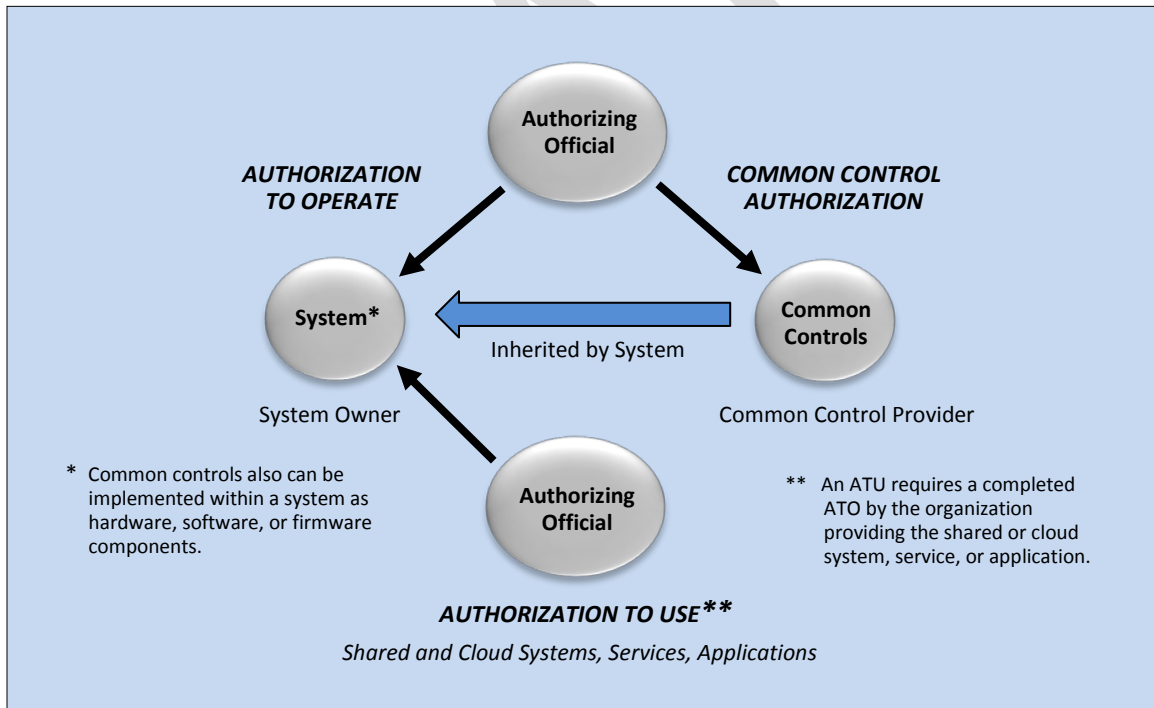
¹⁰⁵ A provisional authorization (to operate) issued by the General Services Administration (GSA) as part of the Federal Risk and Authorization Management Program (FedRAMP) is considered a valid authorization to operate for customer organizations desiring to issue an authorization to use for cloud-based systems, services, or applications.

¹⁰⁶ 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).

221 system, service, or application.¹⁰⁷ The customer organization is responsible and accountable for
 222 the security and privacy risks that may impact the customer organization’s operations and assets,
 223 individuals, other organizations, or the Nation.

224 The authorization to use does not require a termination date, but remains in effect while the
 225 customer organization continues to accept the security and privacy risk of using the shared or
 226 cloud system, application, or service; and the authorization to operate issued by the provider
 227 organization meets the requirements established by federal and organizational policies. It is
 228 incumbent on the customer organization to ensure that information from the monitoring activities
 229 conducted by the provider organization is shared on an ongoing basis and that the provider
 230 organization notifies the customer organization when there are significant changes to the system,
 231 application, or service that may affect the security and privacy posture of the provider. If desired,
 232 the authorization to use decision may specify time- or even-driven triggers for review of the
 233 security and privacy posture of the provider organization system, service, or application being
 234 used by the customer organization. It is incumbent on the provider organization to notify the
 235 customer organization if there is a significant event that compromises or adversely affects the
 236 customer organization’s information.

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



260 **FIGURE F-1: TYPES OF AUTHORIZATION DECISIONS**

¹⁰⁷ 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.

261 **Denial of Authorization**

262 If the authorizing official, after reviewing the authorization package, including any inputs
263 provided by the senior accountable official for risk management or risk executive (function),
264 determines that the risk to organizational operations and assets, individuals, other organizations,
265 and the Nation is unacceptable and immediate steps cannot be taken to reduce the risk to an
266 acceptable level, the authorization is not granted. A *denial of authorization* means that the
267 information system is not authorized to operate and not placed into operation; common controls
268 are not authorized to be provided to systems; or that the provider's system is not authorized for
269 use by the customer organization. If the system is currently in operation, all activity is halted.
270 Failure to receive an authorization means that there are significant deficiencies in the controls.
271 The authorizing official or designated representative works with the system owner or the common
272 control provider to revise the plan of action and milestones to help ensure that measures are taken
273 to correct the deficiencies. A special case of authorization denial is an *authorization rescission*.
274 Authorizing officials can rescind a previous authorization decision in situations where there is a
275 violation of federal or organizational policies, directives, regulations, standards, or guidance; or a
276 violation of the terms and conditions of the authorization. For example, failure to maintain an
277 effective continuous monitoring program may be grounds for rescinding an authorization
278 decision.

279 **AUTHORIZATION DECISION INFORMATION**

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

- 283 • Authorization decision;
- 284 • Terms and conditions for the authorization;
- 285 • Time-driven authorization frequency or authorization termination date;
- 286 • Events that may trigger a review of the authorization decision (if any); and
- 287 • For common controls, the FIPS Publication 199 impact level supported by those controls.

288 The authorization decision indicates if the system is authorized to operate or authorized to be
289 used; or if the common controls are authorized to be provided to system owners and inherited by
290 organizational systems. The terms and conditions for the authorization provide any limitations or
291 restrictions placed on the operation of the system that must be followed by the system owner or
292 alternatively, limitations or restrictions placed on the implementation of common controls that
293 must be followed by the common control provider. If the system or common controls are not
294 under ongoing authorization, the termination date for the authorization established by the
295 authorizing official indicates when the authorization expires and reauthorization is required. The
296 authorization decision document is transmitted with the original authorization package to the
297 system owner or common control provider.¹⁰⁸

298 Upon receipt of the authorization decision and authorization package, the system owner and
299 common control provider acknowledge, implement, and comply with the terms and conditions of
300 the authorization. The system owner and common control provider retain the authorization

¹⁰⁸ Authorization decision documents may be digitally signed to ensure authenticity.

301 decision and authorization package.¹⁰⁹ The organization ensures that authorization documents are
302 available to organizational officials when requested. The contents of authorization packages,
303 including sensitive information regarding system vulnerabilities, privacy risks, and control
304 deficiencies, are marked and protected in accordance with federal and organizational policy.
305 Authorization decision information is retained in accordance with the organization's record
306 retention policy. The authorizing official verifies on an ongoing basis, that the terms and
307 conditions established as part of the authorization are being followed by the system owner and
308 common control provider.

309 **Authorization to Use Decision**

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

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

314 An authorization to use is issued by an authorizing official from a customer organization in lieu
315 of an authorization to operate. The authorizing official has the same level of risk management
316 responsibility and authority as an authorizing official issuing an authorization to operate or a
317 common control authorization. The risk acceptance statement indicates the explicit acceptance of
318 the security and privacy risk incurred from the use of a shared system, service, or application with
319 respect to the customer organization information processed, stored, or transmitted by or through
320 the shared or cloud system, service, or application.

321 **ONGOING AUTHORIZATION**

322 Continuous monitoring strategies¹¹⁰ promote effective and efficient risk management on an
323 ongoing basis. Risk management can become *near real-time* by using automation and state-of-
324 the-practice tools, techniques, and procedures for the ongoing monitoring of controls and changes
325 to systems and the environments in which those systems operate. Continuous monitoring based
326 on the needs of the authorizing official, produces the necessary information to determine the
327 current security and privacy posture of the system.¹¹¹ It also highlights the risks to organizational
328 operations and assets, individuals, other organizations, and the Nation. Ultimately, continuous
329 monitoring guides and informs the authorizing official's decision whether to authorize the
330 continued operation of the system or the continued use of the common controls inherited by
331 organizational systems.

332 Continuous monitoring helps to achieve a state of *ongoing authorization* where the authorizing
333 official maintains sufficient knowledge of the current security and privacy posture of the system
334 to determine whether continued operation is acceptable based on ongoing risk determinations—
335 and if not, which steps in the RMF need to be revisited to effectively respond to the additional
336 risk. Reauthorizations are unnecessary in situations where the continuous monitoring program
337 provides authorizing officials with the information necessary to manage the risk arising from

¹⁰⁹ 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.

¹¹⁰ [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.

¹¹¹ 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.

338 changes to the system or the environment in which the system operates. If a reauthorization is
339 required, organizations maximize the use of status reports and relevant information about the
340 security and privacy posture of the system that is produced during the continuous monitoring
341 process to improve efficiency.

342 When a system or common controls are under ongoing authorization, the system or common
343 controls may be authorized on a time-driven and/or event-driven basis, leveraging the security-
344 and privacy-related information generated by the continuous monitoring program. The system
345 and common controls are authorized on a time-driven basis in accordance with the authorization
346 frequency determined as part of the organization- and system-level continuous monitoring
347 strategies. The system and common controls are authorized on an event-driven basis when
348 organizational-defined trigger events occur. Whether the authorization is time-driven or event-
349 driven, the authorizing official acknowledges the ongoing acceptance of identified risks. The
350 organization determines the level of formality required for such acknowledgement by the
351 authorizing official.

352 ***System and Organizational Conditions for Implementation of Ongoing Authorization***

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

- 357 • The system or common control being considered for ongoing authorization has received an
358 initial authorization based on a complete, zero-base review of the system or the common
359 controls.¹¹²
- 360 • An organizational continuous monitoring program is in place that monitors implemented
361 controls with the appropriate degree of rigor and at the required frequencies specified by the
362 organization in accordance with the continuous monitoring strategy and NIST standards and
363 guidelines.¹¹³

364 The organization establishes and implements a process to designate that the two conditions are
365 satisfied and the system or the common controls are transitioning to ongoing authorization. This
366 includes the authorizing official acknowledging that the system or common control are now being
367 managed by an ongoing authorization process and accepting the responsibility for performing all
368 activities associated with that process. The transition to ongoing authorization is documented by
369 the authorizing official by issuing a new authorization decision.¹¹⁴ The security- and privacy-
370 related information generated through the continuous monitoring process is provided to the
371 authorizing officials and other organizational officials in a timely manner through security and
372 privacy management and reporting tools. Such tools facilitate risk-based decision making for the
373 ongoing authorization for systems and common controls.

¹¹² System owners and authorizing officials leverage security- and privacy-related information about inherited common controls from assessments conducted by common control providers.

¹¹³ [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.

¹¹⁴ 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.

374 **Information Generation, Collection, and Independence Requirements**

375 To support ongoing authorization, security- and privacy-related information for controls is
376 generated and collected at the frequency specified in the organization's continuous monitoring
377 strategy. This information may be collected using automated tools or other methods of assessment
378 depending on the type and purpose of the control and desired rigor of the assessment. Automated
379 tools may not generate security- and privacy-related information that is sufficient to support the
380 authorizing official in making risk determinations. This may occur for various reasons, including
381 for example, the tools do not generate information for every control or every part of a control;
382 additional assurance is needed; or the tools do not generate information on specific technologies
383 or platforms. In such cases, manual control assessments are conducted at organizationally-
384 determined frequencies to cover any gaps in automated security- and privacy-related information
385 generation. The manually-generated assessment results are provided to the authorizing official in
386 the manner deemed appropriate by the organization.

387 To support ongoing authorizations for moderate-impact and high-impact systems, the security-
388 and privacy-related information provided to the authorizing official, whether generated manually
389 or in an automated fashion, is produced and analyzed by an entity that meets the independence
390 requirements established by the organization. The senior agency official for privacy is responsible
391 for assessing privacy controls and for providing privacy-related information to the authorizing
392 official. At the discretion of the organization, privacy controls may be assessed by an independent
393 assessor. The independent assessor is impartial and free from any perceived or actual conflicts of
394 interest regarding the development, implementation, assessment, operation, or management of the
395 organizational systems and common controls being monitored.

396 **Ongoing Authorization Frequency**

397 [NIST Special Publication 800-53](#), security control CA-6, Part c. specifies that the authorization
398 for a system and any common controls inherited by the system be updated at an organization-
399 established frequency. This reinforces the concept of ongoing authorization. In accordance with
400 CA-6 (along with the security and privacy assessment and monitoring frequency determinations
401 established as part of the continuous monitoring strategy), organizations determine a frequency
402 with which authorizing officials review security- and privacy-related information via the security
403 or privacy management and reporting tool or manual process.¹¹⁵ This near real-time information
404 is used to determine whether the mission or business risk of operating the system or providing the
405 common controls continues to be acceptable. [NIST Special Publication 800-137](#) provides criteria
406 for determining assessment and monitoring frequencies.

407 Under ongoing authorization, *time-driven* authorization triggers refer to the frequency with which
408 the organization determines that authorizing officials are to review security- and privacy-related
409 information and authorize the system (or common controls) for continued operation as described
410 above. Time-driven authorization triggers can be based on a variety of organization-defined
411 factors including, for example, the impact level of the system. When a time-driven trigger occurs,
412 authorizing officials review security- and privacy-related information on the systems for which
413 they are responsible and accountable to determine the ongoing organizational mission/business

¹¹⁵ *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.

414 risk, the acceptability of such risk in accordance with organizational risk tolerance, and whether
415 the approval for continued operation is justified. The organizational continuous monitoring
416 process, supported by the organization's security and privacy management and reporting tools,
417 provides the appropriate functionality to notify the responsible and accountable authorizing
418 official that it is time to review the security- and privacy-related information to support ongoing
419 authorization.

420 In contrast to time-driven authorization triggers, *event-driven* triggers necessitate an immediate
421 review of security- and privacy-related information by the authorizing official. Organizations may
422 define event-driven *triggers* (i.e., indicators or prompts that cause an organization to react in a
423 predefined manner) for ongoing authorization and reauthorization. When an event-driven trigger
424 occurs under ongoing authorization, the authorizing official is either notified by organizational
425 personnel (e.g., senior agency information security officer, senior agency official for privacy,
426 system owner, common control provider, or system security or privacy officer) or via automated
427 tools that defined trigger events have occurred requiring an immediate review of the system or
428 common controls. At any time, the authorizing official may also determine independently that an
429 immediate review is required. This review is conducted in addition to the time-driven frequency
430 review defined in the organizational continuous monitoring strategy and occurs during ongoing
431 authorization when the residual risk remains within the acceptable limits of organizational risk
432 tolerance.¹¹⁶

433 ***Transitioning from Static Authorization to Ongoing Authorization***

434 The intent of continuous monitoring is to monitor controls at a frequency that is sufficient to
435 provide authorizing officials with the information necessary to make effective, risk-based
436 decisions, whether by automated or manual means.¹¹⁷ However, if a substantial portion of
437 monitoring is not accomplished via automation, it will not be feasible or practical to move from
438 the current static authorization approach to an effective and efficient ongoing authorization
439 approach. A phased approach for the generation of security- and privacy-related information may
440 be necessary during the transition as automated tools become available and a greater number of
441 controls are monitored by automated techniques. Organizations may begin by generating security-
442 and privacy-related information from automated tools and fill in gaps by generating additional
443 information from manual assessments. As additional automated monitoring functionality is
444 added, processes can be adjusted.

445 Transitioning from a static authorization process to a dynamic, ongoing authorization process
446 requires considerable thought and preparation. One methodology that organizations may consider
447 is to take a phased approach to the migration based on the security categorization of the system.
448 Because risk tolerance levels for low-impact systems are likely to be greater than for moderate-
449 impact or high-impact systems, implementing continuous monitoring and ongoing authorization
450 for low-impact systems first may help ease the transition—allowing organizations to incorporate
451 lessons learned as continuous monitoring and ongoing authorization are implemented for the
452 moderate-impact and high-impact systems. This will facilitate the consistent progression of the
453 continuous monitoring and ongoing authorization implementation from the lowest to the highest

¹¹⁶ 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.

¹¹⁷ 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.

454 impact levels for the systems within the organization. Organizations may also consider employing
455 the phased implementation approach by partitioning their systems into well-defined subsystems
456 or system components and subsequently transitioning those subsystems or system components to
457 ongoing authorization one segment at a time until the entire system is ready for the full transition
458 (at which time the authorizing official acknowledges that the system is now being managed by an
459 ongoing authorization process).

460 REAUTHORIZATION

461 Reauthorization actions occur at the discretion of the authorizing official in accordance with
462 federal or organizational policy.¹¹⁸ If a reauthorization action is required, organizations maximize
463 the use of security and privacy risk-related information produced as part of the continuous
464 monitoring processes currently in effect. Reauthorization actions, if initiated, can be either time-
465 driven or event-driven. Time-driven reauthorizations occur when the authorization termination
466 date is reached (if one is specified). If the system is under ongoing authorization,¹¹⁹ a time-driven
467 reauthorization may not be necessary. However, if the continuous monitoring program is not yet
468 sufficiently comprehensive to fully support ongoing authorization, a maximum authorization
469 period can be specified by the authorizing official. Authorization termination dates are influenced
470 by federal and organizational policies and by the requirements of authorizing officials.

471 Under ongoing authorization, a reauthorization may be necessary if an event occurs that produces
472 risk above the acceptable organizational risk tolerance. This situation may occur, for example, if
473 there was a breach/incident or failure of or significant problems with the continuous monitoring
474 program. Reauthorization actions may necessitate a review of and changes to the continuous
475 monitoring strategy which may in turn, affect ongoing authorization.

476 For security and privacy assessments associated with reauthorization, organizations leverage
477 security- and privacy-related information generated by the continuous monitoring program and
478 fill in any gaps with manual assessments. Organizations may supplement automatically-generated
479 assessment information with manually-generated information in situations where an increased
480 level of assurance is needed. If security control assessments are conducted by qualified assessors
481 with the necessary independence, use appropriate security standards and guidelines, and are based
482 on the needs of the authorizing official, the assessment results can be cumulatively applied to the
483 reauthorization.¹²⁰

484 The senior agency official for privacy is responsible for assessing privacy controls and those
485 assessment results can be cumulatively applied to the reauthorization. Independent assessors may
486 assess privacy controls at the discretion of the organization. The senior agency official for privacy
487 reviews and approves the authorization packages for information systems that process PII prior to
488 the authorizing official making a reauthorization decision. The reauthorization action may be as
489 simple as updating the security and privacy plans, security and privacy assessment reports, and
490 plans of action and milestones—focused only on specific problems or ongoing issues, or as
491 comprehensive as the initial authorization.

492

¹¹⁸ 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).

¹¹⁹ 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.

¹²⁰ [NIST Special Publication 800-53A](#) describes the specific conditions when security-related information can be reused to support authorization actions.

493 The authorizing official signs an updated authorization decision document based on the current
494 risk determination and acceptance of risk to organizational operations and assets, individuals,
495 other organizations, and the Nation. In all situations where there is a decision to reauthorize a
496 system or the common controls inherited by organizational systems, the maximum reuse of
497 authorization information is encouraged to minimize the time and expense associated with the
498 reauthorization effort (subject to organizational reuse policy).

499 **EVENT-DRIVEN TRIGGERS AND SIGNIFICANT CHANGES**

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

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

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

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

- 525 • Installation of a new or upgraded operating system, middleware component, or application;
- 526 • Modifications to system ports, protocols, or services;
- 527 • Installation of a new or upgraded hardware platform;
- 528 • Modifications to how information, including PII, is processed;
- 529 • Modifications to cryptographic modules or services; or
- 530 • Modifications to security and privacy controls.

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

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

538 The examples of changes listed above are only significant when they represent a change that is
539 likely to affect the security and privacy posture of the system. Organizations establish criteria for
540 what constitutes significant change based on a variety of factors including, for example, mission
541 and business needs; threat and vulnerability information; environments of operation for systems;
542 privacy risks; and security categorization.

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

550 TYPE AND FACILITY AUTHORIZATIONS

551 A *type authorization*¹²¹ is an official authorization decision that allows for a single authorization
552 package to be developed for an archetype (i.e., common) version of a system. This includes, for
553 example hardware, software, or firmware components that are deployed to multiple locations for
554 use in specified environments of operation (e.g., installation and configuration requirements or
555 operational security and privacy needs to be assumed by the hosting organization at a specific
556 location). A type authorization is appropriate when the deployed system is comprised of identical
557 instances of software, identical information types, functionally identical hardware, information
558 that is processed in the same way, identical control implementations, or identical configurations.
559 A type authorization is used in conjunction with authorized site-specific controls¹²² or with a
560 facility authorization as described below. A type authorization is issued by the authorizing official
561 responsible for the development of the system¹²³ and represents an authorization to operate. At
562 the site or facility where the system is deployed, the authorizing official who is responsible for
563 the system at the site or facility accepts the risk of deploying the system and issues an
564 authorization to use. The authorization to use leverages the information in the authorization
565 packages for the archetype system and the facility common controls.

¹²¹ 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.

¹²² Site-specific controls are typically implemented by an organization as *common controls*. Examples include physical and environmental protection controls and personnel security controls.

¹²³ 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.

566 A *facility authorization* is an official authorization decision that is focused on specific controls
567 implemented in a defined environment of operation to support one or more systems residing
568 within that environment. This form of authorization addresses common controls within a facility
569 and allows systems residing in the defined environment to inherit the common controls and the
570 affected system security and privacy plans to reference the authorization package for the facility.
571 The common controls are provided at a specified impact level to facilitate risk decisions on
572 whether it is appropriate to locate a given system in the facility.¹²⁴ Physical and environmental
573 controls are addressed in a facility authorization but other controls may also be included, for
574 example, boundary protections; contingency plan and incident response plan for the facility; or
575 training and awareness and personnel screening for facility staff. The facility authorizing official
576 issues a common control authorization to describe the common controls available for inheritance
577 by systems residing within the facility.

578 **TRADITIONAL AND JOINT AUTHORIZATIONS**

579 Organizations can choose from two approaches when planning for and conducting authorizations.
580 These include an authorization with a *single* authorizing official or an authorization with *multiple*
581 authorizing officials.¹²⁵ The first approach is the traditional authorization process defined in this
582 appendix where a single organizational official in a senior leadership position is responsible and
583 accountable for a system or for common controls. The organizational official accepts the security-
584 and privacy-related risks that may adversely impact organizational operations, organizational
585 assets, individuals, other organizations, or the Nation.

586 The second approach, *joint authorization*, is employed when multiple organizational officials
587 either from the same organization or different organizations, have a shared interest in authorizing
588 a system. The organizational officials collectively are responsible and accountable for the system
589 and jointly accept the security- and privacy-related risks that may adversely impact organizational
590 operations and assets, individuals, other organizations, and the Nation. A similar authorization
591 process is followed as in the single authorization official approach with the essential difference
592 being the addition of multiple authorizing officials. Organizations choosing a joint authorization
593 approach are expected to work together on the planning and the execution of RMF tasks and to
594 document their agreement and progress in implementing the tasks. Collaborating on security
595 categorization, control selection and tailoring, a plan for assessing the controls to determine
596 effectiveness, a plan of action and milestones, and a system-level continuous monitoring strategy
597 is necessary for a successful joint authorization. The specific terms and conditions of the joint
598 authorization are established by the participating parties in the joint authorization including, for
599 example, the process for ongoing determination and acceptance of risk. The joint authorization
600 remains in effect only while there is agreement among authorizing officials and the authorization
601 meets the specific requirements established by federal and organizational policies. [NIST Special](#)
602 [Publication 800-53](#) controls CA-6 (1), *Joint Authorization – Same Organization* and CA-6 (2)
603 *Joint Authorization – Different Organizations*, describe the requirements for joint authorizations.

604

¹²⁴ 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.

¹²⁵ Authorization approaches can be applied to systems and to common controls inherited by organizational systems.

605

606

607

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.

DRAFT

1 APPENDIX G

2 LIFE CYCLE CONSIDERATIONS

3 OTHER FACTORS EFFECTING THE SUCCESSFUL EXECUTION OF THE RMF

4 All systems, including operational systems, systems under development, and systems that
5 are undergoing modification or upgrade, are in some phase of the SDLC.¹²⁶ Defining
6 requirements is a critical part of an SDLC process and begins in the *initiation* phase.¹²⁷
7 Security and privacy requirements are part of the functional and nonfunctional¹²⁸ requirements
8 allocated to a system. The security and privacy requirements are incorporated into the SDLC
9 simultaneously with the other requirements. Without the early integration of security and privacy
10 requirements, significant expense may be incurred by the organization later in the life cycle to
11 address security and privacy concerns that could have been included in the initial design. When
12 security and privacy requirements are defined early in the SDLC and integrated with other system
13 requirements, the resulting system has fewer deficiencies, and therefore, fewer privacy risks or
14 security vulnerabilities that can be exploited in the future.

15 Integrating security and privacy requirements into the SDLC is the most effective, efficient, and
16 cost-effective method to ensure that the organization's protection strategy is implemented. It also
17 ensures that security- and privacy-related processes are not isolated from the other processes used
18 by the organization to develop, implement, operate, and maintain the systems supporting ongoing
19 missions and business functions. In addition to incorporating security and privacy requirements
20 into the SDLC, the requirements are integrated into the organization's program, planning, and
21 budgeting activities to help ensure that resources are available when needed and program and
22 project milestones are completed. The enterprise architecture provides a central record of this
23 integration within an organization.

24 Ensuring that security and privacy requirements are integrated into the SDLC helps facilitate the
25 development and implementation of more resilient systems to reduce the security and privacy risk
26 to organizational operations and assets, individuals, other organizations, and the Nation. This can
27 be accomplished by using the concept of integrated project teams.¹²⁹ Organizational officials
28 ensure that security and privacy professionals are part of the SDLC activities. Such consideration
29 fosters an increased level of cooperation among personnel responsible for the development,
30 implementation, assessment, operation, maintenance, and disposition of systems and the security
31 and privacy professionals advising the senior leadership on the controls needed to adequately
32 mitigate security and privacy risks and protect organizational missions and business functions.

33 Finally, organizations maximize the use of security- and privacy-relevant information generated
34 during the SDLC process to satisfy requirements for similar information needed for other security
35 and privacy purposes. The reuse of such information is an effective method to reduce or eliminate
36 duplication of effort, reduce documentation, promote reciprocity, and avoid unnecessary costs
37 that may result when security and privacy activities are conducted independently of the SDLC
38 processes. Reuse promotes consistency of information used in the development, implementation,

¹²⁶ 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.

¹²⁷ Organizations may employ a variety of development processes including, for example, waterfall, spiral, or agile.

¹²⁸ Nonfunctional requirements include, for example, quality and assurance requirements.

¹²⁹ 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.

39 assessment, operation, maintenance, and disposition of systems including security- and privacy-
40 related considerations.

41

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.