NIST Special Publication 800
NIST SP 800-18r2

Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems

Jeremy Licata
Rebecca McWhite
Laura Calloway
Dylan Gilbert
Meghan Anderson
Julie Snyder
Jeremy Miller

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-18r2

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800
NIST SP 800-18r2

Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems

Jeremy Licata, Rebecca McWhite, Laura Calloway
Computer Security Division
Information Technology Laboratory

Dylan Gilbert[1], Meghan Anderson
Applied Cybersecurity Division
Information Technology Laboratory

Jeremy Miller[2], Julie Snyder
The MITRE Corporation

[1] *Former NIST employee; all work for this publication was done while at NIST.*
[2] *Former MITRE employee; all work for this publication was done while at MITRE.*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-18r2

June 2026

U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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 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 all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with 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, Director of the OMB, 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.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on 2026-05-26
Supersedes NIST SP 800-18r1 (February 2006) https://doi.org/10.6028/NIST.SP.800-18r1

How to Cite this NIST Technical Series Publication

Licata J, McWhite R, Calloway L, Gilbert D, Miller J (2026) Developing Security, Privacy, and Supply Chain Risk Management Plans for Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-18r2. https://doi.org/10.6028/NIST.SP.800-18r2

Author ORCID iDs
Meghan Anderson: 0009-0004-2875-5672
Laura Calloway: 0000-0003-4045-7307
Dylan Gilbert: 0009-0003-6061-3757
Jeremy Licata: 0000-0001-8793-5471
Rebecca McWhite: 0009-0000-9092-3500
Jeremy Miller: 0009-0004-3119-8803
Julie Snyder: 0009-0004-6352-2831

Contact Information
sec-cert@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/18/r2/final, including related content, potential updates, and document history.

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

Abstract

The system security plan, system privacy plan, and cybersecurity supply chain risk management plan are collectively referred to as system plans. They describe the purpose of the system, the operational status of the controls selected and allocated for meeting risk management requirements, and the responsibilities and expected behavior of all individuals who manage, support, and access the system. This publication identifies essential elements of system plans from security, privacy, and cybersecurity supply chain risk management perspectives to promote consistent information collection across the organization, regardless of the system's mission or business function.

Keywords

authorization boundary; authorizing official; common control authorization; control implementation details; cybersecurity supply chain risk management plan; privacy plan; privacy risk management; risk management framework; security plan; security risk management; authorization to operate; authorization to use; authorizing official designated representative; CASES Act; control implementation; controls; FASCSA; FISMA; ongoing authorization; Privacy Act; supply chain; supply chain risk management; system privacy plan; system security plan; system owner.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Supplemental Content

The following materials are available on the publication details page to supplement the guidelines provided in this publication:

- System Security Plan outline example
- System Privacy Plan outline example
- Cybersecurity Supply Chain Risk Management Plan outline example
- System Plan Roles and Responsibilities

Audience

This publication is intended to serve a diverse audience, including:

- Individuals with information security, privacy, and risk management program oversight responsibilities (e.g., authorizing officials, senior agency information security officers, senior agency officials for privacy)
- Individuals with system development responsibilities (e.g., mission or business owners, program managers, systems engineers, systems security engineers, systems privacy engineers, software developers, systems integrators, acquisition or procurement officials)
- Individuals with system security and privacy implementation and operations responsibilities (e.g., mission or business owners, system owners, information owners or stewards, system administrators, system security officers, system privacy officers)
- Individuals with cybersecurity supply chain risk management-related responsibilities (e.g., C-SCRM program managers)
- Individuals with acquisition and procurement-related responsibilities (e.g., acquisition officials, contracting officers)
- Individuals with logistical or disposition-related responsibilities (e.g., program managers, system integrators, property managers)
- Individuals with control assessment and monitoring responsibilities (e.g., auditors, Inspectors General, system evaluators, control assessors, independent verifiers and validators, analysts)
- Commercial entities and industry partners that produce component products and systems, create security and privacy technologies, or provide services or capabilities that support information security or privacy

The material presented in this publication assumes that the audience has a basic understanding of the concepts presented in NIST Special Publication (SP) 800-37, *NIST Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Tables

List of Figures

Acknowledgments

The authors would like to thank everyone who took the time to review and make comments on the revision of this publication, specifically Jon Boyens, Michaela Iorga, Victoria Yan Pillitteri, Eduardo Takamura, Daniel Eliott, Robert Staples, Claire Barrett, Jim Foti, Isabel Van Wyk, and the CSD web team of the National Institute of Standards and Technology (NIST); Ellen Nadeau of Fedwriters, Inc./Coralline; Michele Iversen of the Department of Defense; and Paul J. DeNaray of The Aerospace Corporation.

The authors would also like to acknowledge the original authors — Marianne Swanson, Joan Hash, and Pauline Bowen — as well as the individuals who contributed to the original version of this publication.

Executive Summary

System plans collectively refer to the *system security plan*, *system privacy plan*, and *cybersecurity supply chain risk management* (C-SCRM) *plan* that describe the design and implementation of security, privacy, and cybersecurity supply chain protections throughout the system life cycle. System plans:

- Include information about the data being created, collected, disseminated, used, stored, and disposed of;
- Identify individuals who are responsible for system risk management efforts;
- Describe the environment of operation, system components, and data flows within the environment; and
- Account for risks associated with the sharing of information outside the scope of the system.

The elements described in this publication provide building blocks for an organization to devise an effective method of collecting and consolidating information about a system so that it is readily available to organizational leadership, authorizing officials, system owners, and risk managers to support risk-based decisions. Organizations may also consider more responsive approaches to system plan structures (e.g., automated data collection methods, online reporting dashboards) in lieu of traditional document-focused system plans that may not support the rapid pace of modern system development.

NIST Special Publication (SP) 800-18r2 (Revision 2) addresses the development of system plans in support of risk management activities, such as tasks in the NIST Risk Management Framework (RMF) steps in [SP800-37]. This revision:

- Provides content considerations for elements in system plans;
- Discusses the use of automation to maintain system plans over the system life cycle, including sharing and protecting system plan information; and
- Provides supplemental materials, including system plan outline examples and updated roles and responsibilities associated with system plans, that may factor into system plan development.

Office of Management and Budget (OMB) Circular A-130 [OMBA-130] requires federal agencies to develop and maintain system plans for managing risks, including implementation details for the controls allocated to address the requirements. Nonfederal organizations may voluntarily apply the guidelines provided in this publication to develop and maintain system plans consistent with their risk management strategies.

1. Introduction

All systems that process, store, and transmit information within an organization need safeguards that adhere to an organization-wide risk management strategy to address security, privacy, and cybersecurity supply chain risks. A standardized method of presenting risk management information about a system can help organizational leadership, risk managers, and system personnel understand the safeguards that are designed to protect the organization and system assets.

System plans collectively refer to the *system security plan*, *system privacy plan*, and *cybersecurity supply chain risk management (C-SCRM) plan*, which describe the assets and individuals being protected within the scope of a system and the risks associated with information exchanges that involve systems outside the scope (e.g., database sharing, cloud- or web-based service, simple file exchange).

- The **system security plan** describes the system security requirements, including the controls selected to protect the confidentiality, integrity, and availability of the system and its information.
- The **system privacy plan** describes the system privacy risk management requirements, including the controls selected to address predictability, manageability, and disassociability.[1]
- The **C-SCRM plan** describes the system's C-SCRM requirements, including the controls to manage, implement, and monitor the supply chain and to develop and sustain the system across mission and business functions.

The NIST Risk Management Framework (RMF) [SP800-37] provides a flexible methodology for organizations and systems to manage security, privacy, and supply chain risks. The expected outputs of RMF tasks (see Appendix A) inform the system plan elements (see Sec. 3.1) that describe the purpose and scope of the system; the environment of operation; the information types created, collected, disseminated, used, stored, and disposed of; the data flows within the environment and with interconnected systems; the control implementation details; and the roles and responsibilities of individuals associated with the system. Organizations determine the level of detail and areas of focus that are appropriate for each system plan element based on the information needed to support:

- System assessment, ongoing assessment, and continuous monitoring activities by system personnel and assessment teams
- Risk-based decisions by senior leadership (i.e., authorizing official, senior agency official for privacy)

Organizations are encouraged to automate the collection of system information (see Sec. 3.3) using information management tools with a central data repository, including Governance, Risk, and Compliance (GRC); Security Orchestration, Automation, and Response (SOAR); and Security Information and Event Management (SIEM) tools. Automation can control the availability and

[1] The NIST Privacy Framework [NIST PF] explains the privacy engineering objectives of predictability, manageability, and disassociability.

shareability of collected system information, enabling personnel responsible for the system to access an appropriate level of detail based on their system risk management role.

While there is a shift toward automating information capture and managing system plans using standardized machine-readable formats,[2] organizations with limited resources to automate may rely on the manual preparation of traditional system plan artifacts.

1.1. Publication Scope

This publication focuses on the development of system plans that address system-level security, privacy, and C-SCRM requirements that are derived from enterprise, organization, and mission/business process requirements. The guidelines in this publication can be extended to:

- Common control providers that provide implementation details for controls available to be inherited by other systems;
- Requirements identified in [SP800-171] and [SP800-172] for the development of system security plans for nonfederal organizations protecting Controlled Unclassified Information (CUI); and
- Organizations developing system plans for service offerings from cloud service providers, including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

System plans are required for federal systems in accordance with Office of Management and Budget (OMB) Circular A-130 [OMBA-130] and the provisions of the Federal Information Security Modernization Act (FISMA) of 2014 [FISMA].[3] Nonfederal organizations — including private and small businesses, academic institutions, and state, local, and tribal governments — may utilize the guidelines provided in this publication to support their risk management programs.

The guidelines provided can support training for individuals in roles that are responsible for the development and maintenance of system plans. Organizations can leverage the example plans, provided as supplemental materials, to develop localized plan templates. Third-party templates are available[4] to address planning requirements for specific organizations or industry sectors.

[2] The NIST Open Security Controls Assessment Language [OSCAL] is designed to standardize the representation, implementation, and assessment of controls using machine-readable data formats (e.g., XML, JSON, YAML). These OSCAL representations can be used in conjunction with the other OSCAL schemas to represent structured and machine-readable system plan information, control assessment plans, and assessment results, which facilitate the continuous assessment and monitoring of system controls. Initially designed for security assessment, OSCAL has been proven suitable for the machine-readable representation of other control types (e.g., privacy, supply chain, accessibility, safety) and to support their continuous assessment and monitoring.

[3] [FISMA] includes privacy protections in the definition for confidentiality, as indicated in [44 USC3552].

[4] [SP1318] identifies https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/level-2/ca-l2-3-12-4/, https://www.fedramp.gov/rev5/documents-templates/ as potential sources for applicable system plan templates.

1.2. Relationship With Other NIST Publications

This publication is designed to support the NIST portfolio of risk management initiatives and publications[5] that address security, privacy, and supply chain risk management concepts and methodologies, including:

- SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy [SP800-37]
- SP 800-53, Security and Privacy Controls for Information Systems and Organizations [SP800-53]
- SP 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations [SP800-53A]
- SP 800-53B, Control Baselines for Information Systems and Organizations [SP800-53B]
- SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations [SP800-161]
- SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations [SP800-171]
- SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information [SP800-172]
- NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management [NISTPF]
- The NIST Cybersecurity Framework (CSF) [NISTCSF]

1.3. Document Organization

The publication is organized into the following sections:

- Section 2 describes system security, system privacy, and C-SCRM plans and discusses the development of consolidated plans.
- Section 3 identifies elements that may be included in system security, privacy, and C-SCRM plans and describes how automation can support the collection and reporting of system information.
- Section 4 provides a management-level overview of how system plans are developed and maintained in relation to the NIST RMF.
- The References section lists the source materials cited in this publication.

The following appendices provide additional information and resources that support the development of system plans:

[5] The full range of NIST cybersecurity-related publications can be found in the Information Technology Laboratory (ITL) Computer Security Resource Center [CSRC]. Additional resources are available through the NIST Cybersecurity and Privacy Reference Tool [CPRT].

- Appendix A summarizes the RMF task outputs included in system plans.
- Appendix B lists the abbreviations and acronyms used in this publication.
- Appendix C provides a glossary of the terms used in this publication.
- Appendix D provides a publication change log.

2. Overview

Based on the organization's risk management strategy and NIST guidelines (e.g., [SP800-37], [SP800-53], [SP800-161]), system plans:

- Identify the authorization boundary of the system;
- Identify individuals who are responsible for managing and supporting the system;
- Help organizational personnel understand how to manage risks to an acceptable level throughout the system life cycle and respond to changing risks in a timely manner;
- Demonstrate the application of security engineering approaches to building resilient and trustworthy systems following [SP800-160v1r1] and [SP800-160v2r1];
- Define capabilities to defend the organization against threats and threat actors;
- Consider requirements for information technology, operational technology, and emerging technologies that may be informed by system artifacts, such as risk assessments, business impact analyses (BIAs), and information exchange agreements;
- Address organizationally defined parameters, acceptable risk thresholds, and organizational policies that support the organization's security, privacy, and C-SCRM objectives;
- Provide sufficient evidence to support risk-based decisions regarding the ongoing operation or use of the system; and
- Require methodical reviews and periodic updates to maintain information about the system's mission, technologies, components, personnel, and the status of controls that are selected and allocated for system implementation.

This section addresses the objectives and purposes of the system security plan, system privacy plan, and C-SCRM plan.

2.1. System Security Plan

The system security plan identifies the system's security requirements and describes the controls that are planned and implemented to meet those requirements. The system security plan:

- Supports situational awareness of the system security posture over the course of the system life cycle (i.e., "living document");
- Enables organizational leadership and system management personnel to manage security risks and make effective risk management decisions;
- Identifies the individuals responsible for maintaining the security protections and safeguards for information and systems;
- Consolidates details about the system, including its purpose, authorization boundary, [FIPS199] security categorization, operational status, and environment of operation; and

- Explains how controls are implemented to achieve security objectives (i.e., confidentiality, integrity, and availability).

2.2. System Privacy Plan

The system privacy plan identifies controls that are allocated and implemented to address privacy risks related to both cybersecurity events and data processing. The privacy plan:

- Aligns the system's privacy objectives with the organization's mission, risk tolerance, and privacy goals;
- Defines system requirements with respect to the privacy engineering objectives of predictability, manageability, and disassociability and the Fair Information Practice Principles (FIPPs)[6]; and
- Describes planned and implemented controls to address privacy requirements and data processing activities that may compromise privacy (i.e., problematic data actions[7]).

Systems must comply with laws governing data subject rights (i.e., the right to access, correct, or delete information[8]). The system privacy plan describes how the organization manages the risks of over-collection, unauthorized profiling, or the misuse of data about individuals.

Privacy requirements may be informed by the following:

- Legal and regulatory obligations
- Privacy activities and artifacts including the Privacy Impact Assessment (PIA) and Privacy Risk Assessment (PRA)[9]
- Information exchange agreements [SP800-47]
- Public notices for the collection and use of personal information, such as a System of Records Notice (SORN)[PRIVACT]

This includes identifying and cataloging key inputs, such as data actions, contextual factors that describe the circumstances surrounding data processing, privacy capabilities, and privacy engineering and security objectives based on organizational mission needs, risk tolerance, and privacy goals.

[6] The FIPPs have been adopted in various forms in law and policy within the U.S. Government and by international organizations, such as the Organization for Economic Cooperation and Development (OECD) and the European Union. [OMB A-130] identifies and explains the FIPPs for U.S. federal agencies.
[7] Per the NIST Privacy Framework [NIST PF], a problematic data action (PDA) may cause an adverse effect for individuals.
[8] Many laws, regulations, and guidance focus on a defined scope of information that is covered by privacy protections for PII, such as [OMB A-130] or the California Privacy Rights Act [CPRA]. However, data processing may still introduce privacy risks, even if data does not meet a narrow privacy definition (e.g., some data that is not PII can be combined with other information during processing to become PII).
[9] The NIST Privacy Risk Assessment Methodology [PRAM] helps organizations analyze, assess, and prioritize privacy risks to identify appropriate responses and solutions.

2.3. Cybersecurity Supply Chain Risk Management Plan

The system-level C-SCRM plan draws from the organization's overarching C-SCRM strategy[10] to address cybersecurity risks at the system level throughout the supply chain, including commercial-off-the-shelf (COTS) products, turn-key solutions, and support services. It incorporates organization-level priorities, policies, and risk tolerances to address system-level risks and interdependencies with inherited or system-specific controls that enhance trust and protection. The C-SCRM plan:

- Identifies policy implementations, requirements, constraints, and implications that are specific to the cybersecurity supply chain at the system level and that derive from the organization-level C-SCRM strategy and mission/business process risk priorities;
- Describes the system's approach to managing supply chain risks that are associated with the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of its components or services;
- Describes the system in the context of the organizational supply chain risk tolerance, including acceptable supply chain risk response strategies or controls, a process for the continuous evaluation and monitoring of supply chain risks, approaches for implementing and communicating the plan, and a description of and justification for the supply chain risk mitigation measures that are taken;
- Includes supplier and component inventories that specify the associated criticality to the system and identify key individuals who fill supply chain-relevant roles;
- Considers security control implementation information that is specific to supply chain considerations, system diagrams, and interdependencies with other systems; and
- Defines the relationships between key suppliers and the system owner by establishing roles and responsibilities, setting stakeholder expectations, managing supplier performance, and enumerating policies, processes, and procedures for supplier governance that can evolve as the system C-SCRM plan matures.

Different types of systems may have specific considerations that can be addressed in the C-SCRM plan, such as the system architecture, security category, or type of technology used within the system. [SP800-161] Appendix A, *C-SCRM Security Controls*, provides an enhanced overlay with selected [SP800-53] security and privacy controls along with implementation guidelines to support the effective implementation of the controls from a supply chain risk management perspective.

[10] The cybersecurity supply chain refers to the linked set of resources and processes between and among multiple levels of the organizational hierarchy. In general practice, C-SCRM is at the nexus of SCRM and information security, so C-SCRM and SCRM refer to the same concept for the purposes of this publication. Other organizations may use different definitions of C-SCRM and SCRM, which are outside of the scope of this publication. This publication does not address many of the non-cybersecurity aspects of SCRM.

2.4. Consolidated System Plan

Organizations determine whether to consolidate the system security, system privacy, or C-SCRM plans, as described in RMF [SP800-37] Task S-4, *Documentation of Planned Control Implementations*, and [SP800-161]. For a consolidated plan:

- Common elements in the security, privacy, and C-SCRM plans (e.g., System Name and Identifier, System Operational Status, System Overview, Authorization Boundary Description) provide consistent information about the system's mission, purpose, and environment of operation.
- Roles and responsibilities are defined to support the ongoing collaboration between individuals who are responsible for meeting system security, privacy, and C-SCRM requirements.
- Each control that is allocated, tailored, and implemented or planned for implementation has details that clearly address system requirements.

When choosing whether to consolidate plans, an organization may consider the interrelationship of controls that address the risks associated with overlapping cybersecurity, cybersecurity supply chain, and privacy incidents or events, as shown in Fig. 1.

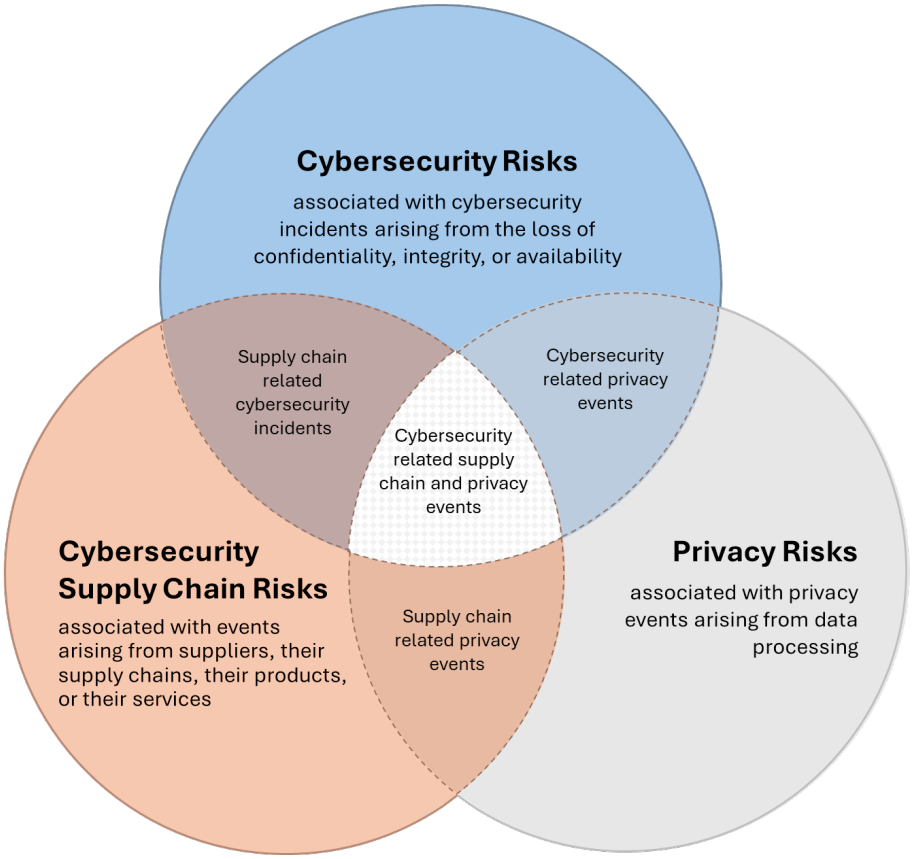

Fig. 1. Cybersecurity, privacy, and cybersecurity supply chain risk relationships

While security-related controls can support system privacy outcomes, privacy risks may require additional privacy-focused controls that go beyond protecting confidentiality, integrity, and availability. Some may also introduce privacy risks that require additional management, such as monitoring for insider threats. For example, an implemented software component may have vulnerabilities that allow organization users to gain unauthorized access to datasets with employees' personal information.

Cybersecurity and cybersecurity supply chain controls may not address certain aspects of data handling and governance that can arise from the authorized processing of personal information. For example, an attacker may exfiltrate an organization's customer data files through the exploitation of a third-party service provider entrusted with the data.

Unauthorized data access and authorized disclosures that are made without sufficient disassociability can introduce privacy problems for individuals that may have an impact on the organization and result in noncompliance costs, direct business costs, or other impacts [PDAP]. Incorporating the security, privacy, and C-SCRM controls into a unified system plan provides a holistic view of the risk management requirements and activities throughout the system life cycle.

3. System Plan Elements

This section describes the types of system information to include in the system plan. Information management tools (e.g., GRC, SOAR, SIEM) can be used to capture, report, and update system information details following consistent and logical structures that address security, privacy, and C-SCRM risk management objectives. Organizations define the methods, structures, and formats used to develop system plans that include the described elements and additional organization- or system-specific elements as needed to achieve security, privacy, and cybersecurity supply chain risk management program objectives.

3.1. System Plan Elements Summary

The system plan elements summary in Table 1 is organized based on the RMF tasks in [SP800-37], where the system and privacy plan are identified as either potential inputs or expected outputs for tasks. Inputs and outputs from multiple RMF tasks may be combined to fully address some system plan element.

This structure provides a basis for the logical development and maintenance of a "living" system plan. The system plan elements enable an organization to determine a method for collecting and presenting information about the system, whether it is being developed or is authorized to operate. The information collected and reported for each element accurately communicates the efforts to safeguard the system information and components to organizational leadership, authorizing officials, system owners, and risk managers throughout the system life cycle.

Each system plan element in Table 1 is cross-referenced with the corresponding RMF task outputs in Appendix A, Table 2. Section 3.2 discusses the objectives and content considerations for each system plan element. Section 4 describes additional considerations for the RMF steps to support those responsible for managing the development of system plans.

System plan outline examples are provided as supplemental materials to this publication and show potential ways to combine these elements into an automated system plan report or system plan artifact.

Table 1. System Plan Elements Summary

RMF Step	Source RMF Task(s)	System Plan Element	System Plan Element Overview
Prepare	P-18, System Registration	System Name and Identifier	Identify the system name and unique system identifier.
Prepare	P-8, Mission or Business Focus C-1, System Description	System Type	Identify the type of system.
Prepare	P-8, Mission or Business Focus C-1, System Description M-1, System and Environment Changes	System Overview	Identify the mission processes and business functions that the system is intended to support.
Prepare	P-9, System Stakeholders	Role Identification and Responsible Personnel	Identify the individuals who serve as authorizing officials and system owners as well as other key roles with system responsibilities.
Prepare	P-12, Information Types P-13, Information Life Cycle	System Information Types	Identify the information types that are processed, stored, or transmitted by the system.
Prepare	P-15, Requirements Definition P-17, Requirements Allocation	Laws, Regulations, and Policies Affecting the System Requirements	Identify current laws, regulations, and policies that influence organizational policies and system requirements.
Prepare	P-10, Asset Identification P-11, Authorization Boundary P-13, Information Life Cycle P-16, Enterprise Architecture M-1, System and Environment Changes	Authorization Boundary Description	Define the scope of the system protections that encompass the authorization boundary, including all components and subsystems of the system to be authorized for operation.
Prepare	P-10, Asset Identification M-7, System Disposal	System Component Inventory	Identify the inventory of components being used within the authorization boundary.

RMF Step	Source RMF Task(s)	System Plan Element	System Plan Element Overview
Prepare	P-10, Asset Identification P-11, Authorization Boundary P-13, Information Life Cycle P-16, Enterprise Architecture M-1, System and Environment Changes	Environment of Operation Diagrams	Include system diagrams that clearly depict the components of the system architecture within the authorization boundary.
Categorize	C-2, Security Categorization C-3, Security Categorization Review and Approval	System Categorization	Categorize information types by their impact level for each security objective (i.e., confidentiality, integrity, availability). The system security category reflects the high-water mark of the security category of all designated subsystems.
Select	P-4, Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles (Optional) P-5, Common Control Identification S-1, Control Selection S-2, Control Tailoring S-3, Control Allocation S-4, Documentation of Planned Control Implementations S-5, Continuous Monitoring Strategy - System I-1, Control Implementation I-2, Update Control Implementation Information A-5, Remediation Actions R-3, Risk Response M-1, System and Environment Changes M-3, Ongoing Response	Control Implementation Details	Provide implementation details for all controls that are allocated to the system. Identify the location of artifacts that are referenced in the control implementation details.
Select	S-6, Plan Review and Approval	System Plan Approval	Indicate whether the plan has been approved by the authorizing official.

RMF Step	Source RMF Task(s)	System Plan Element	System Plan Element Overview
Implement	S-4, Documentation of Planned Control Implementations I-2, Update Control Implementation Information	Control Implementation Status	Indicate the implementation status of the control.
Implement	P-13, Information Life Cycle I-1, Control Implementation I-2, Update Control Implementation Information R-3, Risk Response M-1, System and Environment Changes M-3, Ongoing Response	Information Exchanges Summary	Summarize the flow of information exchanged with other systems outside the authorization boundary.
Assess	A-5, Remediation Actions A-6, Plan of Actions and Milestones M-2, Ongoing Assessments	Control Assessment Status	Indicate the assessment status of each allocated control resulting from the assessment process.
Assess	I-2, Update Control Implementation Information A-5, Remediation Actions A-6, Plan of Action and Milestones R-1, Authorization Package R-3, Risk Response M-3, Ongoing Risk Response M-4, Authorization Package Updates	Remediation Actions	Identify controls that require remediation action resulting from assessment results and the associated plan of action and milestones.
Authorize	R-1, Authorization Package M-4, Authorization Package Updates	Digital Identity Acceptance Statement (optional)	Provide a Digital Identity Acceptance Statement (DIAS), as described in [SP800-63-4].
Authorize	A-5, Remediation Actions R-2, Risk Analysis and Determination R-4, Authorization Decision M-4, Authorization Package Updates M-6, Ongoing Authorization	System Authorization Decision	Identify the authorization decision and the effective date and duration of the authorization provided by the authorizing official.

RMF Step	Source RMF Task(s)	System Plan Element	System Plan Element Overview
Monitor	C-1, System Description M-1, System and Environment Changes M-7, System Disposal	System Operational Status	Indicate the operational status of the system and subsystems.
Monitor	M-4, Authorization Package Updates	System Plan Review Records	Provide a method for recording system plan reviews over the course of the system life cycle.
Monitor	I-2, Update Control Implementation Information A-5, Remediation Actions A-6, Plan of Action and Milestones R-3, Risk Response M-1, System and Environment Changes M-3, Ongoing Risk Response M-4, Authorization Package Updates M-7, System Disposal	System Plan Change Records	Provide a method for recording system plan changes over the course of the system life cycle.

3.2. System Plan Element Details

This section provides a discussion of each of the system plan elements identified in Table 1.

System Name and Identifier

Discussion: Designate a unique system name and identifier to distinguish one system from another in organizational records. Organizations determine the method for assigning the system name, an associated acronym, and a unique system identifier for all systems in the organization's inventory based on the implementation of [SP800-53] PM-05, *System Inventory*. The system identifier may be automatically generated or manually assigned using organization-defined conventions.

The system name and identifier remain the same throughout the system life cycle to facilitate the management and tracking of system components, artifacts, assessment and monitoring reports, and risk-based decisions, as well as the traceability of responses to privacy and security events (e.g., access to data, data transfers). Where possible, the system name and identifier are referenced in PIAs and PRAs to link privacy risks to specific systems and their associated controls.

For a complex system (see [SP800-37] Appendix G, *Authorization Boundary Considerations*), additional subsystem or system element identifiers may be assigned to reflect the relationship between the authorization boundary and the individual subsystems within the environment of operation.

Related plan elements: System Type, System Overview

System Type

Discussion: Identify key characteristics that define the type of system, such as:

- Common control provider (e.g., data center facility, enterprise architecture services)
- Implemented or supported technology (e.g., operational technology, cloud-based system, cloud-supported application, artificial intelligence system, high-performance computing)
- Environment Type (e.g., development, testing, training, production)
- System exposure (e.g., restricted access, public-facing system, physically or logically isolated)
- System criticality[11] (e.g., organization-critical, mission-critical, high-availability, low-priority)
- Ownership of the system (e.g., federal information system; government-owned, contractor-supported system; contractor-owned and operated system)

[11] [IR8179] Discusses the system/subsystem- and component/subcomponent-level criticality analysis based on their importance to the goals of an organization and the impact that their loss may present to those goals.

- Function of the system (e.g., transaction processing, operational management, decision support, customer relationship management, science data processing, machine learning)

The terms “general support system,” “major application,” and “minor application” for system types have been deprecated for federal information systems following [OMBA-130] requirements. This change reflects shifts in technology away from perimeter-based security and toward risk-based requirements for holistically protecting systems and system data, including the system infrastructure and applications within the infrastructure.

The system type is distinct from the system information types used to assign the security categorization of the system.

Related plan elements: System Overview, Authorization Boundary Description

System Overview

Discussion: Provide a brief overview of the mission/business functions of the system and the purpose of the system (e.g., economic indicator, network support for an agency, business census data analysis, crop reporting support).The overview may highlight risk management strategies for high-risk aspects of the environment of operation, such as high-availability components or public-facing services.

Summarize the data and information types handled by the system (e.g., CUI, privacy). Highlight the relationship between the system owner and data owner responsibilities for data collection, processing, and disposal as provided from the organization or system data governance strategy. In the privacy plan, the overview aligns with the information provided in the PIA, PRA, and other applicable privacy documentation (e.g., notices to the public, information exchange agreements).

Compile a list of the technologies being used to support the mission/business functions and factors that present additional security- or privacy-specific risks, such as cloud-based products and services, “bring your own device” (BYOD) policies, or the processing of data about individuals. Reference key design considerations (e.g., centralization methods, continuous integration and continuous delivery, zero trust architecture, emerging technologies) in the approach for identifying and managing system risks.

Identify the system user base and user roles that require privileged access to specific components, enclaves, or data flows that contain data about individuals to ensure accountability and transparency.

Summarize the system’s supply chain profile and highlight C-SCRM-relevant technologies (e.g., foreign-sourced components, vendor-managed services, TAA/Common Criteria/NIAP compliance or open-source dependencies) to support a holistic understanding of system risks and to ensure alignment of security, privacy, and C-SCRM risk management.

Related plan elements: System Type, System Information Types, Authorization Boundary Description

Role Identification and Responsible Personnel

Discussion: Identify the role of each individual that has responsibilities for coordinating system-specific risk management activities. An individual's organizational job title may not clearly demonstrate or align with the risk management role and responsibilities. Identified individuals are generally held accountable for the ongoing operation of the system, the continuous monitoring of the implemented controls, and additional risk mitigation efforts that are required throughout the system life cycle. Based on the plan type, key roles include the system security officer, system privacy officer, and personnel who support the C-SCRM Program Management Office (PMO).

Common roles and responsibilities of key participants involved in risk management activities are provided in [SP800-37] Appendix D, *Roles and Responsibilities*. Additional responsibilities for roles related to the development and management of system plans are provided as a supplement to this publication. An organization may identify other individuals in roles that directly support system plan development, as needed.

If an individual has multiple roles related to system security, privacy, or cybersecurity supply chain risk management, the system plan may provide additional information for managing the separation of duties and define the risk mitigations for any conflicts of interest.

When applicable, identify the roles and responsibilities of personnel responsible for external services supporting the system (i.e., account manager, service coordinator). These individuals may be different from those identified in information exchange artifacts that support [SP800-53] CA-03, *Information Exchange*.

Organizations include the following contact information for each identified individual:

- Name
- Risk-management-related role (e.g., system-specific role, organizational role)[12]
- Organizational unit, department, or division
- Primary business phone number
- Alternate business phone number
- Business email address

Restrict contact information to business information to avoid exposing personal information. Using personal information (e.g., a home phone or personal cell phone number as the "alternate business phone number") may create unnecessary privacy risks for the individuals identified as having a role protecting the system.

[12] Identifying the risk-management related role of an individual can be more indicative of system responsibility than a position or title.

Related plan elements: System Overview, Authorization Boundary Description

System Information Types

Discussion: Identify the [SP800-60v2] information types processed, stored, and transmitted by the system. Understanding the information types handled by the system and the information life cycle for each information type across all stages of the system life cycle can assist the system owner in recognizing where security and privacy risks could arise, identifying considerations for protecting the information, and applying controls where they can be most effective.

The types of information handled by the system in support of organizational mission/business functions and processes are key to determining the system security category and the initial selection of controls.

Related plan elements: System Categorization

Laws, Regulations, and Policies Affecting the System Requirements

Discussion: Identify the sources of specific requirements for the:

- Confidentiality, integrity, or availability of the system components and information
- Predictability, manageability, and disassociability of information processed, stored, or transmitted by the system
- Acquisition of trustworthy system components through the supply chain

Organizational policies may identify the laws, regulations, and policies that are applicable to all systems within the organization or include a standardized list of requirement sources in an organizational template for system plans. As the legal and regulatory landscape evolves, the system plans are updated to adapt to new security, privacy, and cybersecurity supply chain risk management requirements, such as those that arise from the use of emerging technologies, automated decision-making, and data analytics. For example, privacy laws that govern data subject rights directly influence the development of the system privacy plan, including how data is handled and how the system protects individual rights, frames broader privacy risks, and addresses organizational privacy goals. The C-SCRM plan identifies suppliers or products that are prohibited by law, subject to regulatory exclusions, and constrained by organization- or system-specific policies.

Related plan elements: System Overview, Control Implementation Details

Authorization Boundary Description

Discussion: Identify the subsystems and system elements that comprise the system to be authorized for operation or use by an authorizing official (i.e., the scope of the authorization). Summarize key aspects of the system architecture, including the use of subsystems and external service providers; physical or logical separations; local and

remote management functionalities; customized or specialized components, functions, or data flows; and the use of private, public, or hybrid cloud service provider services.

The description can also identify the following:

- Enabling systems that may provide services or functionalities used or inherited by the system or other systems that interact with the operational environment outside of the authorization boundary and may exist outside the environment of operation, as explained in [SP800-37]
- System elements that are critical to both the mission and organization
- System functions that are subject to additional requirements, such as the protection of CUI
- Any third-party authorization services and API implementations as part of the identification of external system services that support the system
- The set of common controls to be authorized for inheritance purposes

While the system security plan may focus on broad cybersecurity risks, the system privacy plan highlights the role of the system in handling personal data and the controls implemented in response to associated privacy risks. For example, the system privacy plan may address how risks related to the collection, use, and sharing of data across multiple authorization boundaries are managed and how those practices align with the organization's privacy policies

Related plan elements: System Type, Environment of Operation Diagrams, System Component Inventory

System Component Inventory

Discussion: Summarize the component inventory provided in the [SP800-53] CM-08, *System Component Inventory*, control implementation. System components are discrete, identifiable information technology assets that represent the building blocks of a system, including hardware, software, and firmware. Organizations can associate distinct hardware and software components with specific system elements defined in the authorization boundary. Identify the criticality of individual system components, particularly those that support mission-critical functions or multiple system elements.

The component inventory presented in the privacy plan can support an understanding of the components that participate in the business process flows and the data transactions that involve individual PII data elements. While specific technical details about the components are generally included as part of the security plan, the privacy plan can associate specific privacy-related data flows with individual components or groups of components (e.g., databases, applications, file storage arrays) which are subject to privacy management requirements.

- Hardware component description

- Component function and role
- Unique component identifier (e.g., serial number, asset tracking identifier, other service codes that identify supply chain information, designation for physical or virtual implementation)
- Manufacturer and model, including sub-model identifiers or distinctions (e.g., subcomponent country of origin)
- Deployment date, warranty duration, expiration date, and maintenance support contract status
- Specific physical locations (e.g., room number, rack and slot number) or logical locations for virtualized components either hosted on-premises or using external third-party services
- Differentiate between physical and virtual "hardware" components that host the software products that support organizational missions, business functions, and mission/business processes

- Software product description
  - Purpose
  - Product type (e.g., COTS, GOTS)
  - Software developer, manufacturer, vendor, and version or build information, as indicated in the Software Bill of Materials (SBOM)
  - Secure software development attestation[13]
  - Product license
    - Type (e.g., single user, volume license, public license, freeware)
    - Expiration date/renewal date
    - Component installation location
  - Software warranty and maintenance support contract status

The validation of the SBOM can be addressed as part of the control implementation for the retention and management of the software inventory. Reviews of other supplier-provided component inventory lists can provide a way to also check for manifestless components, which may contain additional vulnerabilities. [SP800-53] SR-04, *Provenance*, provides guidelines for acquiring information about the provenance/pedigree[14] of the software and firmware included in the inventory.

[13] [SP800-218] discusses the Secure Software Development Framework (SSDF), which supports the provisions of [EO14028] for ensuring the secure functionality of software. [OMBM-26-05] provides flexibility for how an agency can confirm the implementation of specific security practices in the development of software products accounting for associated hardware risks.

[14] Per [SP 800-53], provenance is "the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data." Pedigree refers to "the validation of the internal composition and provenance of technologies, products, and services."

The capture date of the inventory summary can convey the timeliness of the summary related to continuous monitoring activities, system plan approval, and system authorization. Automation may be used to generate a summary from the authoritative inventory data repository.

Provide a reference to the authoritative system component inventory data repository. The system component inventory is often distinct from the organization's physical inventory, which may be handled through a distinct procurement and property management repository. For instance, the system component inventory accounts for hardware as well as instances of virtualized components on host devices that may not be included in the physical inventory repository.

Related plan elements: Authorization Boundary Description, Environment of Operation Diagrams

Environment of Operation Diagrams

Discussion: Provide visual representations of key internal boundaries, critical components, subsystems, primary and secondary data stores, virtual components, information exchanges, and services from third-party providers to demonstrate how resilience and redundancy are addressed in the system architecture. Supporting topology narratives may be included.

Diagrams may identify the usage of API implementations as part of the identification of external system services as well as connection points and data flow for information exchanges.

When developing or generating diagrams, certain system architecture information (e.g., IP addresses, network routing and access rules) may be redacted commensurate with organizational system data protection requirements. Additional artifacts associated with the diagram may detail information about the architecture, such as IP subnets, MAC addresses, and relevant ports that support communication for key services.

- System/Subsystem Diagrams

  Identify the physical and logical locations of active system components in the authorization boundary inventory. Components are identified based on their roles in the system, such as application interfaces, information data stores, or development, test, and production environments. Diagrams account for all system components, whether they are located on premises, hosted by an external system, virtualized on system host devices, physically or logically isolated within the authorization boundary, or physically or virtually hosted by third-party service providers. Automation may be used to link the components represented in the diagram to the inventory source data.

  Physical and environmental protections are identified, including physical entry points and the locations of key environmental control systems (e.g., climate control, fire control, water control and detection) components, such as sensors and shut-off valves.

- System/Network Architecture Diagrams

  Illustrate the physical and logical boundaries for communication between system components, including:

  - Technologies used to define the authorization boundary and to enable communication between components and services within the boundary or from third-party providers
  - Data routing and traffic controls, including monitoring for suspicious network activity
  - Communication routes for specialized components (e.g., operational technology, Internet of Things)
  - Components involved in the physical and logical protection of other components
  - Components that are physically or logically isolated (e.g., air-gapped)

- Data Flow Diagrams

  Identify the direction of data exchanges and the components that receive and transmit data, including:

  - Data types (e.g., privacy, CUI) and associated security impact levels
  - Where data is created, processed, and delivered (e.g., database servers, application servers, storage networks, replication services)
  - Where data enters and exits key internal boundaries, including any data loss protection mechanisms and flow control mechanisms based on data labels or data classification
  - The flow of information that results from information exchanges with external organization systems, including any data movement constraints due to laws, regulations, policies, or agreement limitations

Related plan elements: System Type, System Information Types, Authorization Boundary Description, System Component Inventory

System Categorization

Discussion: Assign the security category according to the security impact levels (i.e., low, moderate, and high) associated with the information types processed, stored, and transmitted by the system following the guidelines in [SP800-60v1]. The security category is a key factor when selecting a [SP800-53B] security baseline as the starting point for the selection of controls.

Impact levels are based on risk management activities, system artifacts (e.g., Risk Assessment Report, PIA, SORN), guidelines on the categorization of federal information and systems [FIPS199], and justifications for adjusting the [SP800-60v2] provisional impact levels. Special conditions may be applied to the provisional impact levels for

each information type. The high-water mark for each of the security impacts determines the final system category.

Related plan elements: System Information Types

Control Implementation Details

Discussion: Provide implementation details for each control that is selected and allocated to the system. Maintaining accurate control implementation details throughout the system life cycle supports ongoing assessment and continuous monitoring activities that evaluate the effectiveness of the control implementation.

As explained in [SP800-53], controls are *outcome-based* and "are selected and implemented by the organization in order to satisfy the system requirements." The implementation details reflect how requirement outcomes are achieved, rather than restating the control statement as a requirement. System-specific implementation details or common control implementation details for a common control plan indicate how to address risk management requirements based on the "as-implemented" state of the control, including:

- Information that addresses basic questions (i.e., who, what, where, when, why, and how) about security, privacy, and supply chain risk management requirements
    - Roles or specific entities that are responsible for control implementation, including information about shared responsibilities for hybrid controls
    - Components, products, or services associated with the control
    - Results of tailoring activities and tailoring decisions
    - Planned inputs, related data sources, and expected system outputs for controls that are implemented in the hardware, software, or firmware components of the system
    - Considerations for additional technical objectives (i.e., continuous integration/continuous delivery, zero trust architecture, artificial intelligence and machine learning) addressed by the control implementation
    - Reliance on automation for control monitoring, including performance thresholds defined for the implementation that can be evaluated using automation, or a combination of manual and automated methods
- Rationale and approval for tailoring associated with the control (see Sec. 4.3.1)
- Location of policy and procedure artifacts associated with the implementation
    - Reference sections of operational procedures rather than including the procedures in the system plan.
    - Identify sources of information relevant to the control, such as network monitoring tools, vulnerability scanning tools, endpoint management tools, and GRC, SOAR, and SIEM tools.

- Description of metrics that are collected and analyzed to monitor the control implementation, including the baseline and threshold definitions used to evaluate control conformance to implementation procedures and parameters
- Inherited risks from the common control implementations
- Control assessment status (i.e., satisfied, other than satisfied)
    - Automation can provide the ability to include the assessment history, including the results of control monitoring activities.
    - Reference plans of action and milestones (POA&Ms), remediation, and retest artifacts for controls that are identified as "other than satisfied."

To address the inheritance of controls from common control providers, the control implementation details in the system plan may:

- Include a reference to common controls inherited by the system
    - Implementation details for common controls are provided in the artifacts developed by common control providers that are made available to system owners.
    - Controls that are inherited from cloud service providers may require additional documentation, such as the Control Implementation Summary/Customer Responsibility Matrix (CIS/CRM), which conveys the control implementation responsibilities between the cloud service provider and their customer.
- Provide system-specific implementation details for hybrid controls with considerations for:
    - Which parts of the control are provided by the common control provider or are implemented at the system level
    - How the associated security, privacy, and cybersecurity supply chain risks are shared between the system and the common control provider

Control implementation details in the C-SCRM plan reflect the mitigation of cybersecurity risks throughout the supply chain. [SP800-161] Appendix A, *C-SCRM Security Controls*, discusses the application of C-SCRM controls, requiring controls to flow down through key suppliers, and controls for monitoring adherence with organizational supply chain requirements. Implementation details for C-SCRM controls reference applicable organizational and mission/business process policies that provide inherited controls or are issued by the chief information officer (CIO), senior accountable official for risk management, C-SCRM PMO, or senior procurement executive.

Control implementation details in a system privacy plan differ from those in system security and C-SCRM plans in several ways, including:

- **Scope and focus:** While the system security plan primarily addresses safeguarding the system against unauthorized access and ensuring data confidentiality, integrity,

and availability, the system privacy plan focuses on the broader implications of data processing. This includes considerations such as the context of data use, the potential impact on individuals, and adherence to privacy principles (e.g., transparency, data minimization, purpose specification). In this way, privacy controls may address more foundational data handling and data governance in pursuit of privacy objectives.

- **Privacy-specific risks:** The system privacy plan addresses privacy-specific risks that might arise, even from authorized data processing activities. For example, privacy controls might include measures to minimize data collection to only what is necessary, restrict data sharing with third parties, or implement mechanisms that allow individuals to exercise their rights over their personal data. The system privacy plan may address privacy-specific risks that may arise from cybersecurity or C-SCRM controls, such as monitoring for insider threats.
- **Individual autonomy and transparency:** Privacy controls often emphasize giving individuals control over their data (i.e., autonomy) and ensuring that individuals are informed about how their data is processed (i.e., transparency). These aspects may require different implementations compared to security controls, which are primarily concerned with protecting systems and information rather than individuals.

Related plan elements: Control Implementation Status, Control Assessment Status

System Plan Approval

Discussion: System plan approval is critical prior to control implementation for systems under development. By approving the system plans before the system is in operation, the authorizing official or designated representative accepts and agrees to the allocated set of controls, the proposed implementation of the allocated controls, and the inheritance of controls from common control provider plans. Input from other organizational officials provides information to support the approval of system plans. For example:

- System security plan approval includes concurrence between the system owner and the senior accountable official for risk management or risk executive (function), CIO, or senior agency information security officer.
- System privacy plan approval includes concurrence between the system owner and the senior agency official for privacy to demonstrate alignment between the organization's privacy and security programs.
- C-SCRM plan approval includes coordination with the C-SCRM PMO.

System plan approval includes the full names, system roles, organizational titles, signatures, and signature dates of the individuals who approved the plan. Information management tools and document management systems can electronically capture the required signatures from the appropriate approvers.

The system owner or common control provider is responsible for updates to the system plan. System plan reviews and change records, along with the subsequent reauthorization or ongoing authorization of the system, ensure that updates to the system plan based on the "as-implemented" state of the controls are reviewed and approved [SP800-37] by the authorizing official.

Approval of the system plans does not authorize the operation of the system or the offering of common controls for inheritance.

Related plan elements: System Plan Review Records, System Plan Change Records

Control Implementation Status

Discussion: Identify the implementation status of the control following the system plan approval. The control implementation status indicator may be included in the control implementation details.

Typical control implementation status indicators include:

- **Planned:** Control is selected but implementation has not started.
- **Partially Implemented:** Planned control implementation has started but has not been completed. This may indicate that an implemented control is in the process of being changed based on items in POA&Ms.
- **Fully Implemented:** The "as-implemented" state of the control has been fully realized in the operational system.

Details related to the timeline for full implementation may be provided. For complex systems, the control implementation status may differentiate the control implementation status for individual subsystems that may be at different stages of planning and development.

Related plan elements: Control Implementation Details

Information Exchanges Summary

Discussion: Summarize the information exchanges that are defined between the system and systems outside of the authorization boundary [SP800-47], whether inside or outside the organization. Agreements can vary based on the impact level of the information being exchanged, the relationship between the organizations exchanging information, or the level of access granted to personnel from the interconnected system.

The summary of information exchanges may include information about outstanding risks from the interconnected systems to support the implementation of secure system interconnections. Information collected about each valid information exchange in which the system participates may include the following, as determined by the organization implementation of the [SP800-53] CA-03, *Information Exchange*, control:

- Type of agreement used for the information exchange (e.g., information exchange agreement, interconnection security agreement, memorandum of agreement, memorandum of understanding)
- Effective start and end dates of the agreement based on the acceptance signatures provided in the agreement artifact
- Systems participating in the agreement, including:
  - Name, role, title, and organization of the system owner and authorizing official
  - System name and unique system identifier assigned by the system owner's organization
  - FIPS 199 categorization of the system and the information being exchanged
  - System authorization decisions status
- Brief description of the exchange, including purpose, type of data, and expected outputs
- Method of information exchange (e.g., virtual private network, extranet, dedicated data transfer application)
- Interface characteristics that explain how the information is being exchanged between the systems
- Diagrams that show the data flows, system components, and technologies involved
- Findings and mitigation strategies that are relevant to the components involved in the information exchange and may be identified in:
  - Security, privacy, or cybersecurity supply chain risk assessment reports;
  - Security and privacy control assessments; or
  - Information security continuous monitoring (ISCM) processes that identify security and privacy risks and mitigation strategies.

Exchanges that involve data about individuals have the potential to introduce additional privacy risks. The system privacy plan describes protections for ensuring the confidentiality and integrity of data about individuals during transmission and storage, including details about the information being exchanged, the organizations and systems involved, and data sharing and service agreements between the system and entities that are outside of the authorization boundary.

Related plan elements: System Overview, Authorization Boundary Description, Environment of Operation Diagrams, Control Implementation Details

Control Assessment Status

Discussion: Identify the assessment status of the control. The plan can specify whether the control was "satisfied" or "other than satisfied" based on the requirements provided in the assessment plan. The assessment status may specify when the control was last

assessed and provide a reference to the assessment report and the assessment plan that explains the scope, breadth, and depth of the assessment performed.

The control assessment status indicator may be included in the control implementation details. Automation can provide the ability to include the assessment history, including the results of control monitoring activities. References to POA&Ms and retest artifacts may be included for controls identified as "other than satisfied."

Related plan elements: Control Implementation Details, Control Implementation Status

Remediation Actions

Discussion: Identify the status of control remediation actions that result from assessment activities. A list of outstanding risk remediation activities, including POA&M items and system changes that result from control monitoring, can provide information about the risk posture of the system to organizational leadership, risk managers, and the managers of systems with which information exchange agreements are in place.

The control assessment status indicator may be included in the control implementation details. Automating the generation of this information based on assessment reports and monitoring results provides transparency about existing threats and vulnerabilities that have not been fully remediated.

Related plan elements: Control Implementation Details, Control Implementation Status, Control Assessment Status

Digital Identity Acceptance Statement (DIAS) (optional)

Discussion: Organization- and system-level risk assessments determine the extent to which risk is managed by various processes,[15] which in turn drive decisions regarding applicable technologies and mitigation strategies. During the risk management process, the organization determines the assurance levels for identity proofing, authentication, and federation, if applicable; selects appropriate processes and technologies to meet each assurance level; and identifies compensating controls when necessary.

The DIAS is not required to be included in the system plan but is required to be included in the system authorization package for federal systems.

Related plan elements: System Authorization Decision

System Authorization Decision

Discussion: The authorization decision is made by the authorizing official before the system is put into the operational environment and to maintain its operational status. The system plan may refer to authorization decision artifacts, such as an authorization to operate (ATO) letter or memorandum issued by the authorizing official, to explain the terms and conditions of the authorization decision. If the organization implements a

[15] [SP 800-63-4] guidelines refer to the Identity Assurance Level (IAL), Authenticator AL (AAL), and Federation AL (FAL) as ***xAL***, where "***x***" refers to either I, A, or F for the individual assurance levels.

program for ongoing system authorization, the ongoing authorization decision information may be referenced in the system plan. The organization determines how to identify the authorization status of the system as a part of an ISCM strategy that includes ongoing authorization.

Related plan elements: Remediation Actions

System Operational Status

Discussion: Identify the readiness of the system and related subsystems within the environment of operation. Common status indicators include:

- **Under development:** The system is being designed or developed and is not fully functioning in an operational environment.
- **Operational:** The authorized system is operating in the operational environment.
- **Undergoing a significant modification:** The authorized operational system is undergoing a significant change to the operational environment that is likely to substantively affect the security, privacy, or supply chain posture of a system. [SP800-37]
- **Disposal:** The system is no longer authorized or operational.

Organizations may use other operational status indicators as needed based on the components and services within the environment of operation.

For complex systems, include the operational status of the subsystems within the authorization boundary. Using automation, the operational status of key components within the system or subsystems can be identified to provide organizational management with a full accounting of the status of the mission or business process supported by the system.

Related plan elements: System Overview, System Authorization Decision

System Plan Review Records

Discussion: System plan reviews ensure accountability for periodic (e.g., life cycle milestones, gate reviews, significant contracting activities) and ad hoc changes. Organization-designated individuals can verify the accuracy and completeness of the information in the system plans and alignment between system plans.

A system plan review log records the name and role of the individual performing the review, the review date, the feedback generated during the review process, and associated notes. The review record may include additional information, such as:

- Dates of review
- Review Participants
- Notable outcomes (i.e., recommended revisions, concerns, other action items)

Updates to the system plan are approved and applied as part of organizational or system-specific change management processes. The records help management understand the content updates that have been implemented and verify that the authorization package contains the most current revision of the system plans.

Related plan elements: System Plan Approval, Control Implementation Status, Control Assessment Status

System Plan Change Records

Discussion: A system plan change record focuses on specific updates that are made to the system plan. Updates to the system plan are often the result of changes to the system that are approved and applied as part of organization- or system-specific change management processes implemented as part of [SP800-53] CM-03, *Configuration Change Control*. A system plan change record can include the following information:

- Date of revision
- Plan revision identifier
- Identity of individual making the system plan change
- The system plan elements affected (e.g., control implementation details, authorization boundary description, information exchange summary)
- Details of the plan changes (e.g., controls affected, role assignment changes, updated links to referenced artifacts)

The records help management understand the content updates that have been implemented and verify that the authorization package contains the most current revision of the system plans. While document management processes may require manual change record updates, information management tools (e.g., IT service desk solutions, ticketing systems) can automatically track changes made to specific system plan elements. Organizational and system managers can generate reports that identify the users who approved and implemented individual changes to the system plans.

Related plan elements: System Plan Approval, Control Implementation Details, Remediation Actions

3.3. Automation Support for System Plan Information

Automating the collection of system plan element information can increase the effectiveness and efficiency of maintaining system plans. Organizations have the flexibility to decide when, where, and how to use automation tools (e.g., GRC, SOAR, SIEM) to manage information for the system plan elements associated with each system. For instance, automation tools can:

- Capture control implementation status information to demonstrate ongoing risk management activities,[16]
- Support the tracking of POA&M activities to ensure that remediation actions are completed,
- Facilitate the management of system plan reviews, and
- Control access to system plan information.

While some organizations have the resources to implement dedicated, organization-wide information management tools to manage many system plans, organizations with limited resources may be able to leverage commercially available services (e.g., office productivity applications, open-source solutions, cloud-based services) to manage information for the limited number of system plans within the organization.

NIST does not recommend, endorse, or certify specific products, vendors, or technologies for the automation of system plan development and maintenance.

3.3.1. System Plan Information Collection

The information contained in the system elements may be collected from both organization-wide and system-specific data sources, including:

- System component inventory information (e.g., technology, function, role, and configuration of components used within the operational environment[17])
- Personnel contact information from an organizational directory
- Information types that are detected within the system but excluded from system categorization determination
- Changes to common controls and the inherited portion of hybrid controls
- Changes to system plan information to enforce separation of duties
- New, in-process, and resolved POA&Ms

The collected information informs various management activities, such as prioritizing security, privacy, or C-SCRM initiatives and allocating resources based on impact priorities. Automating the collection of system-level risk information in a centralized repository following organization-defined data standards can reduce inconsistencies that may lead to erroneous risk-based decisions.

[16] The [OSCAL] implementation layer includes a system security plan model that allows for the granular implementation and documentation of various controls (e.g., security, privacy, safety, accessibility) that require automated governance, risk management, and compliance processes. The OSCAL resources provide additional information and examples at https://nist.gov/OSCAL (documentation), https://github.com/usnistgov/OSCAL (OSCAL models), and https://github.com/usnistgov/oscal-content (OSCAL SP 800-53 catalog, SP 800-53B baselines, and SP 800-53A included in the OSCAL catalog).

[17] [OSCAL] provides a "Component Definition" model that can be used by vendors to convey how controls are implemented by their products or by organizations to create playbooks that describe the implementation of specific controls that support secure configurations for system components.

3.3.2. System Plan Information Sharing and Usability

Maintaining system plan element information in a central repository using well-designed user interfaces (e.g., dashboards, search functions, reporting methods) in place of potentially lengthy traditional security plan artifacts may improve the responsiveness of risk-based decision-making. Increased information usability supports various stakeholders, including:

- Senior leadership and risk managers to evaluate the organizational risk profile across all systems in the organization's inventory
- Authorizing officials, senior agency officials for privacy, and system owners to quickly locate, review, and update specific system plan elements in support of continuous monitoring activities and ongoing authorization processes
- System management personnel to track approval processes for change management functions and review control implementation metrics

The dashboard interfaces and reporting functions of organization-wide information management tools can ensure that authorized personnel receive updates on system component inventory information and the status of risk management efforts, including the system's operational status, assessment and reauthorization schedules, POA&M statuses (e.g., late POA&Ms, expiring POA&Ms), and accepted risk information.

Information management tools may share control implementation statuses, control assessment statuses, and implementation details with system owners and other authorized individuals from:

- Interconnected systems within the organization,
- Systems inheriting common controls, and
- External organizations participating in approved information exchanges.

Relevant control assessment status information may also be shared in support of information exchanges with external organizations.

Information that is relevant to the preparation, planning, and execution of control assessments can be restricted to prevent the inadvertent release of system information by third-party assessors. Assessors may be given limited access to input assessment results and artifacts directly into the information management tool to generate assessment reports.

3.3.3. System Plan Information Management

Automation facilitates system plan information management throughout the system life cycle, including:

- Tracking changes to system plan elements, including control implementations, agreements for information exchanges, POA&Ms, and supporting roles
- Managing specific configuration settings on defined components within a system or across all systems within the organization to facilitate continuous monitoring reporting

- Alerting organizational leaders and system management of changes or inconsistencies in the collected system plan information
- Generating system plans using organization-approved templates to minimize the duplication of element-specific content (e.g., system description, system environment, identification of roles related to risk management or system operations)

Automation can be particularly useful in assessing and continuously monitoring controls throughout the system life cycle. Storing system plan data in machine-readable formats can facilitate updates to control implementation details due to assessment results, control catalog or baseline updates, and other system changes. For example, POA&Ms for "other than satisfied" findings in a machine-readable assessment report can trigger updates to system plans and other system artifacts that are stored within a central repository.

3.3.4. System Plan Information Protection

Organizations determine the level of protection required for system plan element information based on the system's information types [SP800-60v2] and organizational requirements. Centralized access control policies in an organization-wide information management tool can manage logical access to information about the system to:

- Limit the visibility of information about the system to specific access holders based on their management role
- Ensure that only authorized users can update system information, review change records, and approve changes that have been made

Additional access controls can be applied to prevent unauthorized access to the system's weakness and vulnerability information. Organization- and system-specific policies may further control access to technical details about the system, such as IP addresses, vulnerability information, and architectural designs.

4. System Plan Development Through the Risk Management Framework Steps

The following subsections provide organizational leadership and risk managers with a broader understanding of each RMF step in relation to the development and maintenance of system plans. The RMF provides a methodology for managing system risks using organizational policies and system-level procedures to support system plan development, including responsibilities, ongoing reviews and updates, the approval of system plans, and assessments of control implementations. Fig. 2 shows the seven steps of the RMF.

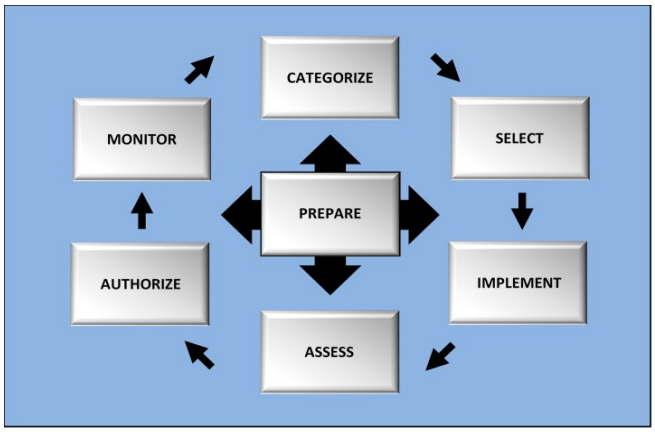

Fig. 2. NIST Risk Management Framework Steps

4.1. Prepare

System plans support organization- and system-level risk management strategies, including regulatory and compliance obligations that define system-level requirements. To enable oversight and promote accountability, the plans designate individuals with roles and responsibilities for security, privacy, and supply chain risk management, such as those identified in [SP800-37] Appendix D, *Roles and Responsibilities*. These roles align with broader organizational information security and privacy program plans [SP800-37] and the C-SCRM strategy and implementation plan [SP800-161] for consistency across all systems within the organization.

Common control providers develop system plan artifacts that identify and provide implementation details for inheritable common controls. A common control plan describes privacy protections (e.g., data minimization, transparency, consent management) and identifies systems outside of the authorization boundary as a common control provider from which implemented controls are inherited. Inherent relationships with common control providers may be based on specific operational relationships with service providers in the supply chain.

Organizations may develop tailored control baselines for systems with specialized or unconventional mission, business, or operational requirements to provide details that are incorporated into system plans, including:

- Predetermined organization-defined parameter (ODP) values for control assignment and selection operations

- Additional controls, control enhancements, and compensating controls to address organization-specific risks
- Supplemental scoping information to explain the applicability of the tailored controls to specialized system, system element, or component operations based on security and privacy assumptions

Prepare — System Level

When the system life cycle is initiated, key information is collected to inform initial drafts of system plans, including:

- The mission or business focus supported by the system
- System stakeholders
- The information types handled by system
- Unique security and privacy risks in the information life cycle that are managed across the entire data ecosystem
- How the authorization boundary is defined within the organizational infrastructure or enterprise architecture

The organization assigns a system identifier to associate component inventory records, device event audit records, and system-related artifacts.

The system-level C-SCRM plan provides a context for how organizational C-SCRM policies are applied at the system level by enumerating requirements, describing constraints, and addressing other supply chain risk implications. C-SCRM plans for systems align with the established organization-wide risk tolerances and C-SCRM strategy. Many organizations choose to enable systems to inherit common controls that support the organization or enterprise C-SCRM requirements. In cases where multiple components within an organization are responsible for different subsets of the same system, the organization decides the scope of the C-SCRM plan.

During each of the subsequent RMF steps, the system plans are revised or updated to add additional information as the system is developed.

Defining the Authorization Boundary

The system plans identify how data flows through various subsystems, third-party services, and external networks to ensure that privacy risks are managed comprehensively. The authorization boundary establishes the scope of protection for the system based on mission, management, or budgetary responsibilities. Privacy risks can arise at any stage of data processing because of the interconnected nature of modern systems, and identifying and responding to them may require looking beyond the authorization boundary.

System-specific C-SCRM concerns may include risks derived from suppliers that are several layers removed from the end user or supply chain risks associated with specific organization-defined technologies. For example, C-SCRM considers the complexities of new technologies and

dynamic system interdependencies that can result in suppliers gaining incidental access[18] to data. C-SCRM plan considerations include vendor-controlled SaaS offerings, hybrid or cloud environments, open-source software, information and communications technology and operational technology from suppliers outside of Trade Agreements Act nations, general procurement from unauthorized resellers, and supply chains of emerging technologies, such as artificial intelligence capabilities.

4.2. Categorize

The system's [FIPS199] security categorization reflects potential adverse impacts of the loss of confidentiality, integrity, or availability; determines the [FIPS200] minimum security requirements; and supports the RMF *Select* step. Security categorization information in the system plan provides the rationale for categorization decisions, including privacy and C-SCRM impacts [SP800-60v2]. Approving the security categorization may require additional input from the senior agency official for privacy and the senior procurement official.

To account for both privacy and security risks in system plans, impact levels for each information type reflect potential adverse impacts on organizational operations and assets and the privacy of individuals whose data is processed by the system. Privacy impacts are informed by other risk management activities and documentation, such as PIAs, SORNs, MOUs, and the NIST PRAM.

The C-SCRM plan is generally developed for high- and moderate-impact systems, as indicated in [SP800-161]. However, there is value in developing the C-SCRM plan to protect low-impact systems as well, particularly if the low-impact system uses the same components found in high- and moderate-impact systems. In the absence of a C-SCRM plan for a low-impact system, the system security plan can identify the inheritance of C-SCRM controls from organization-level common control providers, enumerate organizational and system risk tolerances, and demonstrate the acceptance versus the transfer or mitigation of cybersecurity supply chain risks via system-specific controls.

4.3. Select

The organization determines the approach for selecting, tailoring, and allocating controls for systems based on system requirements. System plans identify the controls that are selected and allocated to the system for implementation. [SP800-37] describes two approaches for selecting controls:

- **Organization-generated control selection:** The organization uses its own process to select and tailor the controls in the system plan based on a variety of factors, including organizational mission or business priorities, system capabilities, the context in which the system operates, and threats. Organizations may consider applicable Cybersecurity

[18] This derives from the work done regarding third-party risks in the Zero Trust Data Security Guide [ZTDATASEC], which discusses third parties and suppliers with incidental access to data. [SP 800-88] provides minimum sanitization requirements for use in determining recommended sanitization methods for specific media to minimize data remanence and the availability of residual data.

and Privacy Framework Profiles to identify controls that support the achievement of security and privacy risk management outcomes.

- **Baseline control selection:** Controls in the organizationally tailored control baselines that were determined during the RMF *Prepare* step are factored into the control selection process. The initial security baselines in [SP800-53B] group controls that are designed to support the [FIPS200] minimum security requirements for systems based on the [FIPS199] security impact level.

The initial privacy baseline in [SP800-53B] identifies controls for federal agencies to address privacy requirements and manage privacy risks that arise from processing data about individuals based on privacy program responsibilities under [OMBA-130].[19] These controls are rooted in privacy engineering objectives and are designed to respond to privacy risks with effective data protection strategies. System privacy and security officials collaborate on the selection of privacy controls to ensure that both privacy and security risks are managed, particularly in areas where the risks overlap.

Organizations can use a control overlay (e.g., C-SCRM extended overlay[20]) as a starting point for selecting controls with broad-based support across communities of interest for specific circumstances, situations, and conditions [SCOR].

Completing the tasks in the RMF *Select* step results in system plans that explain how the security, privacy, and C-SCRM risk management controls are being met for information that is transmitted, processed, and stored by the system.

4.3.1. Control Tailoring

The control tailoring activities in [SP800-53B] provide flexibility for aligning the allocated controls with system-specific needs, such as addressing organizational policies or specific use cases in the system's environment of operation. Tailoring can address the impacts associated with poor quality or counterfeit products, supplier misuse of intellectual property, supplier tampering with or compromise of mission-critical information, and exposure to cyber attacks through vulnerable supplier systems.

The system plans record the justification and decision for control tailoring activities, including:

- Common controls that are inherited by the system from common control providers;
- Scoping considerations for selected controls;
- Compensating controls that are selected and allocated;

[19] Implementing the privacy control baseline does not necessarily mean that a federal agency has met all of its obligations under [OMB A-130]. Agencies may be required to take additional, separate actions to fully comply with OMB privacy requirements. Documenting all actions to address privacy risk management and compliance efforts in the system privacy plan can provide essential information to support control assessments, authorization decisions, and control monitoring processes.

[20] [SP 800-161] includes specific C-SCRM instructions for selecting, tailoring, and implementing controls based on (i) the environments in which enterprise information systems are acquired and operate; (ii) the nature of operations conducted by enterprises; (iii) the types of threats facing enterprises, mission and business processes, supply chains, and information systems; and (iv) the type of information processed, stored, or transmitted by information systems and the supply chain infrastructure.

- ODP values for control assignment and selection operations;
- Additional controls that supplement the baseline, such as controls based on Cybersecurity and Privacy Framework Profiles;[21]
- Additional specification information for control implementation; and
- Controls that are tailored out of the selected control baseline.

Security, privacy, and supply chain risk management officials coordinate to adequately address overlapping requirements and potential conflicts related to tailoring activities, and all decisions are approved through the system plan approval process. However, only the authorizing official can accept the risks associated with removing controls from the selected baseline.

Tailoring can involve enhancing existing controls to meet system-specific operational needs, such as strengthening consent mechanisms or implementing stricter access controls for high-risk data processing activities. Privacy officials tailor controls to address system-specific privacy requirements (e.g., additional safeguards for health or financial data) and confirm that tailoring decisions do not result in compliance gaps or additional privacy risks. The C-SCRM PMO can provide input for C-SCRM plan development through tailored common controls that may apply across the organization or mission, such as supplier risk assessments.

4.3.2. Identification of Planned Control Implementations

System plans identify the intended system-specific application of each allocated control along with an adequate level of implementation detail to support the assessment and monitoring of the control and associated control enhancements. Controls that are partially implemented by a common control provider are identified in the system plan as hybrid controls. Implementation details for the system-specific part of hybrid controls describe the risk management responsibilities that are shared between the system and the common control provider.

For fully inherited or hybrid controls, system plans reference the source of the common control to avoid duplicating the common control implementation details.[22] Notes may be added to the implementation details to describe how fully inherited controls address system requirements. Control implementation details in the system privacy plan describe how the controls meet privacy-specific requirements, such as those that address risks related to the processing of personal information, the context of data use, and potential consequences for individuals.

4.3.3. Plan Review and Approval

The senior agency official for privacy is responsible for reviewing and approving the system privacy plan or consolidated plan before it is submitted to the authorizing official or designated representative. This review ensures that privacy risks have been thoroughly identified and that

[21] The National Online Informative References Program maps CSF Subcategories to [SP 800-53] controls, and the NIST Privacy Engineering Program maps the Privacy Framework to [SP 800-53] controls.

[22] If the common control provider implementation details are considered controlled information (e.g., those associated with a cloud service provider or cloud service offering), restrictions in applicable service agreements related to the distribution of organizational and system information are followed.

privacy controls and risk management strategies are aligned with organizational policies, legal requirements, and privacy objectives. When reviewing the system-specific C-SCRM plan in the authorization package, authorizing officials consult with the C-SCRM PMO as well as acquisitions personnel in cases of technology procurements. The C-SCRM review ensures that the C-SCRM controls and risk management strategies align with the overall organizational risk tolerances.

The authorizing official may request additional input from the senior accountable official for risk management, CIO, senior agency information security officer, senior agency official for privacy, or senior procurement executive to support the system plan approval decision.

- If the system plans are acceptable, the authorizing official or designated representative approves the system plans, enabling the system owner to begin execution of the RMF *Implement* step.
- If the system plans are unacceptable, the authorizing official or designated representative may recommend changes for the system owner or common control provider to implement.

Approving system plans at this step does not authorize system operation or the offering of common controls for inheritance. System authorization to operate, authorization to use, or common control authorization are tasks in the RMF *Authorize* step.

4.4. Implement

Allocated controls are designed, built, tested, and deployed following the details in the system plans. If a control is not implemented as planned or requires additional compensating controls, the system plans are updated to reflect the details of the actual "as-implemented" controls and the selected compensating controls.

4.5. Assess

Control assessments are based on the information in system plans to prepare for, create, and execute an assessment plan [SP800-53A]. Personnel update the system plans based on remediation actions that are taken to resolve control deficiencies reported during the assessment. At the conclusion of the control assessment, system plans provide a "point-in-time" understanding of the system's operation and the implemented controls that support the RMF *Authorize* step.[23]

4.6. Authorize

The system owner or common control provider assembles and submits an authorization package to the authorizing official for an authorization decision. The authorization package

[23] A system may go through multiple assessments and system plan updates during the system development life cycle in preparation for the RMF *Authorize* step.

includes the system security and system privacy plans as well as any additional artifacts that demonstrate risk management activities (e.g., signed interconnection agreements, signed SBOM artifacts, signed POA&M completion artifacts) to enable an informed authorization decision. The C-SCRM plan is not required but is recommended if supply chain risk management is a key organizational concern.

The senior agency official for privacy reviews the authorization package to verify that the system aligns with organizational privacy objectives and legal obligations. The authorizing official relies on information in the system plan and feedback from the system owner and senior agency officials to:

- Authorize a system to operate or be used within the organization,
- Issue a common control authorization, or
- Deny authorization to the system or common control provider to protect the organization from risks that are outside of established organizational risk tolerances.

The authorization decision is included in the authorization package, identified in the system plans, and relayed to the system owner, common control provider, and other organization officials as appropriate.

4.7. Monitor

System plans are reviewed and revised on an organization-defined schedule[24] to ensure their continued accuracy and relevancy after authorization. Reviews may occur in response to events that affect security, privacy, or C-SCRM risks, such as:

- Revisions to the [SP800-53] security and privacy control catalog, [SP800-53B] control baselines, or [SP800-53A] assessment procedures
- New or revised laws, regulations, and organizational policies that affect security, privacy, or C-SCRM requirements
- Updates to the system risk assessment report, often resulting from threat intelligence, that identify new risks that render existing controls less effective
- Weaknesses identified during control assessments and monitoring or after a security, privacy, or supply chain cybersecurity incident or compromise (e.g., system data breach)
- Changes that significantly alter the risk posture of the system and justify control reassessment and system reauthorization (e.g., revisions to the information types or special factors that affect system categorization, the selection and implementation of additional controls, additional tailoring activities that align control implementations with identified risks)

[24] [SP 800-53] controls PL-02, *System Security and Privacy Plans*, and SR-02, *Supply Chain Risk Management Plan* discuss requirements for the frequency of system plan reviews.

- Changes to key system personnel (e.g., if the authorizing official changes, the incoming authorizing official reviews the system plans and artifacts to confirm the existing authorization or issue a new authorization decision)
- Changes to the operational status of the system (e.g., promoting the system from "in development" to "operational," system disposal)
- Renewal of or modifications to existing agreements for information exchanges, the creation of new information exchanges, or the termination of information exchanges [SP800-47]
- Changes to the organizational baseline supply chain risk strategy or inherited C-SCRM controls due to:
    - Changes in critical suppliers that potentially affect supply chain risks, including ownership changes, mergers and acquisitions activity, and geopolitical or environmental activity
    - Reviews of suppliers' foreign ownership, control, or influence (FOCI)
    - Cybersecurity attacks or data breaches that affect a supplier's ability to support confidentiality, integrity, or availability objectives

Change management processes ensure that updates to system plans are tracked and noted. Specific procedures for tracking and managing modifications, including the use of revision or version identifiers to maintain a record of changes, can be included in the system configuration management plan. Automating information collection methods (see Sec. 3.3) can result in more efficient and effective system plan maintenance.

Reauthorization or Ongoing Authorization

The operation of an authorized system requires periodic or ongoing assessments to verify that the implemented controls continue to effectively satisfy security, privacy, and C-SCRM requirements [SP800-53A]. Authorizing officials can reauthorize the system based on these assessment results or update system plans to reflect changes to the control implementation details and environment of operation after ISCM activities [SP800-137].

For example, the system privacy plan can define privacy metrics (e.g., access requests from individuals, data sharing frequency, incidents) that are regularly analyzed during monitoring activities to track trends and risks. The system privacy officer is responsible for identifying assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and complying with applicable privacy requirements. Appropriate updates to privacy controls and the system privacy plan can strengthen protections.

Additionally, the system C-SCRM plan can identify a continuous monitoring capability for critical suppliers to alert system owners to changes that might affect the system's risk posture. New critical components or technology refresh activities can trigger reviews of and updates to the C-SCRM plan, which may require system reauthorization.

Disposal of System Components

System components and information assets may be disposed of at any time during the system life cycle, which may introduce opportunities for the compromise of stored data. System plans can include or reference the instructions for properly disposing of systems or components (e.g., sanitization of storage media) in accordance with applicable data and records retention requirements, such as those provided by the National Archives and Records Administration [NARARECM]. Component disposal records may be referenced in the system plan to indicate the date of component disposal and details about the information assets that are transferred to other systems. Updates to the system component inventory may trigger additional updates to the system plans to reflect changes in the environment of operation.

Key considerations for the removal of a system or system elements from operation include the responsibilities of the system owner for protecting system data, the responsibility of the authorizing official for risks associated with data remanence,[25] and the organizational liability for inadequate data sanitization. Demonstrating due diligence can address the legal and financial liabilities of data breaches caused by inadequate sanitization, unauthorized access to residual data, or the improper transfer of data to another system.

[25] [SP 800-88] defines remanence as "residual information remaining on storage media."

References

	LAWS AND EXECUTIVE ORDERS
[EO14028]	Executive Order 14028 (2021) Improving the Nation's Cybersecurity. (The White House, Washington, DC), DCPD-202100401, May 12, 2021. Available at https://www.govinfo.gov/app/details/DCPD-202100401
[44USC3502]	Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed. Available at https://www.govinfo.gov/app/details/USCODE-2023-title44/USCODE-2023-title44-chap35-subchapI-sec3502
[44USC3552]	Title 44 U.S. Code, Sec. 3552, Definitions, 2023 ed. Available at https://www.govinfo.gov/app/details/USCODE-2023-title44/USCODE-2023-title44-chap35-subchapII-sec3552
[FASCSA]	Federal Acquisition Supply Chain Security Act of 2018 (FASCSA), Title II of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology Act of 2018, Pub. L. 115-390, 132 Stat. 5173. Available at https://www.congress.gov/115/plaws/publ390/PLAW-115publ390.pdf
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available at https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[FOIA]	Freedom of Information Act (FOIA), 5 USC § 552, as amended by Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. Available at https://www.govinfo.gov/app/details/PLAW-104publ231
[PRIVACT]	Privacy Act (P.L. 93-579), December 1974. Available at https://www.govinfo.gov/app/details/STATUTE-88/STATUTE-88-Pg1896
	REGULATIONS, DIRECTIVES, PLANS, AND POLICIES
[OMBA-130]	Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016. Available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
[OMBM-17-12]	Office of Management and Budget Memorandum M-17-12, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017. Available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf
[OMBM-26-05]	Office of Management and Budget Memorandum M-26-05, *Adopting a Risk-based Approach to Software and Hardware Security*, January 2026. Available at https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf
	STANDARDS, GUIDELINES, AND REPORTS
[FIPS199]	National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing

Standards Publication (FIPS) NIST FIPS 199. https://doi.org/10.6028/NIST.FIPS.199

[FIPS200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) NIST FIPS 200. https://doi.org/10.6028/NIST.FIPS.200

[IR8062] An Introduction to Privacy Engineering and Risk Management in Federal Systems (2017) (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/Internal reports (IR) NIST IR 8062. https://doi.org/10.6028/NIST.IR.8062

[IR8179] Paulsen C, Boyens J, Bartol N, Winkler K (2018) Criticality Analysis Process: Model Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8179. https://doi.org/10.6028/NIST.IR.8179

[IR8286] Quinn SD, Chua J, Ivy N, Gardner RK, Kent K, Smith MC, Witte GA (2025) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286r1. https://doi.org/10.6028/NIST.IR.8286r1

[ISO73] International Organization for Standardization/Technical Management Board (2009) ISO/TMBG 73:2009 – Risk Management – Vocabulary (ISO, Geneva, Switzerland) [withdrawn]. Available at https://www.iso.org/standard/44651

[NISTCSF] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[NISTPF] NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (2020) (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020

[NTIASBOM] The Minimum Elements For a Software Bill of Materials (SBOM) (2021) NTIA and Department of Commerce. Available at https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

[SP800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-30r1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-37r2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National

Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP800-47] Dempsey KL, Pillitteri VY, Regenscheid A (2021) Managing the Security of Information Exchanges. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-47r1. https://doi.org/10.6028/NIST.SP.800-47r1

[SP800-53] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53r5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[SP800-53A] Joint Task Force Transformation Initiative (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53Ar5. https://doi.org/10.6028/NIST.SP.800-53Ar5

[SP800-53B] Joint Task Force (2020) Control Baselines for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53B. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53B

[SP800-60v1] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-60v1r1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[SP800-60v2] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-60v2r1. https://doi.org/10.6028/NIST.SP.800-60v2r1

[SP800-63-4] Temoshok D, Galluzzo R, LaSalle C, Lefkovitz N, Regenscheid A, Choong YY, Proud-Madruga D, Gupta S (2025) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63-4. https://doi.org/10.6028/NIST.SP.800-63-4

[SP800-88] Chandramouli R, Hibbard EA (2025) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-88r2. https://doi.org/10.6028/NIST.SP.800-88r2

[SP800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-137. https://doi.org/10.6028/NIST.SP.800-137

[SP800-160v1r1] Ross R, McEvilley M, Winstead M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD),

NIST Special Publication (SP) NIST SP 800-160v1r1. https://doi.org/10.6028/NIST.SP.800-160v1r1

[SP800-160v2r1] Ross R, Pillitteri VY, Graubert R, Bodeau D, McQuaid R (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v2r1. https://doi.org/10.6028/NIST.SP.800-160v2r1

[SP800-161] Boyens JM, Smith A, Bartol N (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-161r1. Includes updates as of November 1, 2024. https://doi.org/10.6028/NIST.SP.800-161r1-upd1

[SP800-171] Ross R, Pillitteri V (2024) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171r3. https://doi.org/10.6028/NIST.SP.800-171r3

[SP800-171A] Ross R, Pillitteri V (2024) Assessing Security Requirements for Controlled Unclassified Information and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171Ar3. https://doi.org/10.6028/NIST.SP.800-171Ar3

[SP800-172] Pillitteri V, Ross R (2026) Enhanced Security Requirements for Protecting Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-172r3. https://doi.org/10.6028/NIST.SP.800-172r3

[SP800-172A] Pillitteri V, Ross R (2026) Assessing Enhanced Security Requirements for Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-172Ar3. https://doi.org/10.6028/NIST.SP.800-172Ar3

[SP800-188] Garfinkel S, Guttman B, Near J (2023) De-Identifying Government Datasets: Techniques and Governance. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-188. https://doi.org/10.6028/NIST.SP.800-188

[SP800-218] Souppaya MP, Scarfone KA, Dodson D (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-218. https://doi.org/10.6028/NIST.SP.800-218

[SP1318] NIST JTC (2025) Protecting Controlled Unclassified Information (CUI): NIST Special Publication 800-171, Revision 3 Small Business Primer. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-1318. https://doi.org/10.6028/NIST.SP.1318

MISCELLANEOUS PUBLICATIONS AND RESOURCES

[CPRA] California Privacy Rights Act of 2020 (2025). Available at https://thecpra.org/

[CPRT] National Institute of Standards and Technology (2025), *NIST Cybersecurity and Privacy Reference Tool* (CPRT). Available at https://csrc.nist.gov/projects/cprt

[CSRC] National Institute of Standards and Technology (2025), *NIST Computer Security Resource Center* (CSRC). Available at https://csrc.nist.gov

[NARACUI] National Archives and Records Administration, Controlled Unclassified Information (CUI) Registry. Available at https://www.archives.gov/cui

[NARARECM] National Archives and Records Administration, NARA Records Management Guidance and Regulations. Available at https://www.archives.gov/records-mgmt/policy

[OSCAL] National Institute of Standards and Technology (2025), *Open Security Controls Assessment Language* (OSCAL). Available at https://nist.gov/oscal

[PDAP] National Institute of Standards and Technology (2025), *Catalog of Problems and Problematic Data Actions* (PDAP). Available at https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md

[PRAM] National Institute of Standards and Technology (2025), *NIST Privacy Risk Assessment Methodology* (PRAM). Available at https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

[RMF] National Institute of Standards and Technology (2025), *NIST Risk Management Framework*. Available at https://nist.gov/rmf

[SCOR] National Institute of Standards and Technology (2025), *NIST Security and Privacy Control Overlay Repository* (SCOR). Available at https://csrc.nist.gov/projects/risk-management/sp800-53-controls/overlay-repository

[ZTDATASEC] Zero Trust Data Security Guide, October 2024. Available at https://www.cio.gov/zero-trust-data-security-guide-oct2024

Appendix A. RMF Task Outputs Related to System Plan Elements

The tasks indicated in Table 1 either explicitly identify the system and privacy plan as expected outputs or identify expected outputs that are directly related to the system plan elements identified in Sec. 3. Details about the individual tasks in Table 2 can be found in the CPRT reference dataset for SP 800-37r2.

Table 2. RMF task outputs related to the system plan elements summary in Table 1

RMF Step	RMF Task	RMF Task Expected Outputs [SP 800-37r2]	System Plan Elements
Prepare — Organization Level	TASK P-4 Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles (Optional)	List of approved or directed organizationally tailored control baselines.	• Control Implementation Details
Prepare — Organization Level	TASK P-5 Common Control Identification	List of common control providers and common controls available for inheritance; security and privacy plans (or equivalent documents) that provide a description of the common control implementation (including inputs, expected behavior, and expected outputs).	• Control Implementation Details
Prepare — System Level	TASK P-8 Mission or Business Focus	Missions, business functions, and mission/business processes that the system will support.	• System Overview • System Type
Prepare — System Level	TASK P-9 System Stakeholders	List of system stakeholders.	• Role Identification and Responsible Personnel
Prepare — System Level	TASK P-10 Asset Identification	Set of assets to be protected.	• Authorization Boundary Description • System Component Inventory • Environment of Operation Diagrams
Prepare — System Level	TASK P-11 Authorization Boundary	Documented authorization boundary.	• Authorization Boundary Description • Environment of Operation Diagrams
Prepare — System Level	TASK P-12 Information Types	A list of information types for the system.	• System Information Types

RMF Step	RMF Task	RMF Task Expected Outputs [SP 800-37r2]	System Plan Elements
Prepare — System Level	TASK P-13 Information Life Cycle	Documentation of the stages through which information passes in the system, such as a data map or model illustrating how information is structured or processed by the system throughout its life cycle. Such documentation may include data flow diagrams, entity relationship diagrams, database schemas, and data dictionaries.	• System Information Types • Authorization Boundary Description • Environment of Operation Diagrams • Information Exchanges Summary
Prepare — System Level	TASK P-15 Requirements Definition	Documented security, privacy, and C-SCRM requirements.	• Laws, Regulations, and Policies Affecting the System
Prepare — System Level	TASK P-16 Enterprise Architecture	Updated enterprise architecture; updated security architecture; updated privacy architecture; plans to use cloud-based systems and shared systems, services, or applications.	• Authorization Boundary Description • Environment of Operation Diagrams
Prepare — System Level	TASK P-17 Requirements Allocation	List of security, privacy, and C-SCRM requirements for the system, system elements, and environment of operation.	• Laws, Regulations, and Policies Affecting the System
Prepare — System Level	TASK P-18 System Registration	Registered system in accordance with organizational policy.	• System Name and Identifier
Categorize	TASK C-1 System Description	Documented system description.	• System Overview • System Information Types • System Operational Status
Categorize	TASK C-2 Security Categorization	Impact levels determined for each information type and for each security objective (confidentiality, integrity, availability); security categorization based on high-water mark of information type impact levels.	• System Categorization
Categorize	TASK C-3 Security Categorization Review and Approval	Approval of security categorization for the system.	• System Categorization
Select	TASK S-1 Control Selection	Controls selected for the system and the environment of operation.	• Control Implementation Details
Select	TASK S-2 Control Tailoring	List of tailored controls for the system and environment of operation (i.e., tailored control baselines).	• Control Implementation Details

RMF Step	RMF Task	RMF Task Expected Outputs [SP 800-37r2]	System Plan Elements
Select	TASK S-3 Control Allocation	List of security and privacy controls that are allocated to the system, system elements, and environment of operation.	• Control Implementation Details
Select	TASK S-4 Documentation of Planned Control Implementations	Security, privacy, and C-SCRM plans for the system.	• Control Implementation Details • Control Implementation Status
Select	TASK S-5 Continuous Monitoring Strategy — System	Continuous monitoring strategy for the system, including a time-based trigger for ongoing authorization.	• Control Implementation Details
Select	TASK S-6 Plan Review and Approval	System plans approved by the authorizing official.	• System Plan Approval
Implement	TASK I-1 Control Implementation	Implemented controls.	• Control Implementation Details • Information Exchanges Summary
Implement	TASK I-2 Update Control Implementation Information	System plans updated with implementation detail sufficient for use by assessors; system configuration baseline.	• Control Implementation Details • Control Implementation Status • Information Exchanges Summary • Remediation Actions • System Plan Change Records
Assess	TASK A-5 Remediation Actions	Initial remediation actions completed based on assessment reports; changes to implementations reassessed by the assessment team; updated assessment reports; updated system plans, including changes to control implementations.	• Control Implementation Details • Control Assessment Status • Remediation Actions • System Authorization Decision • System Plan Change Records
Assess	TASK A-6 Plan of Action and Milestones	A plan of action and milestones detailing the findings from the security and privacy assessment reports that are to be remediated.	• Control Assessment Status • Remediation Actions • System Plan Change Records
Authorize	TASK R-1 Authorization Package	Authorization package (with an executive summary), which may be generated from a security or privacy management tool for submission to the authorizing official.	• Remediation Actions • Digital Identity Acceptance Statement (DIAS) (optional)

RMF Step	RMF Task	RMF Task Expected Outputs [SP 800-37r2]	System Plan Elements
Authorize	TASK R-2 Risk Analysis and Determination	Risk determination.	• System Authorization Decision
Authorize	TASK R-3 Risk Response	Risk responses for determined risks.	• Control Implementation Details • Information Exchanges Summary • Remediation Actions • System Plan Change Records
Authorize	TASK R-4 Authorization Decision	Authorization to operate, authorization to use, common control authorization; denial of authorization to operate, denial of authorization to use, denial of common control authorization.	• System Authorization Decision
Monitor	TASK M-1 System and Environment Changes	Updated system plans; updated plans of action and milestones; updated assessment reports.	• System Overview • Authorization Boundary Description • Environment of Operation Diagrams • Control Implementation Details • Information Exchanges Summary • System Operational Status • System Plan Change Records
Monitor	TASK M-2 Ongoing Assessments	Updated assessment reports; updated supplier assessments.	• Control Assessment Status
Monitor	TASK M-3 Ongoing Risk Response	Mitigation actions or risk acceptance decisions; updated assessment reports.	• Control Implementation Details • Information Exchanges Summary • Remediation Actions • System Plan Change Records

RMF Step	RMF Task	RMF Task Expected Outputs [SP 800-37r2]	System Plan Elements
Monitor	TASK M-4 Authorization Package Updates	Updated assessment reports; updated plans of action and milestones; updated risk assessment results; updated system plans.	• Remediation Actions • System Authorization Decision • System Plan Review Records • System Plan Change Records • Digital Identity Acceptance Statement (DIAS) (optional)
Monitor	TASK M-6 Ongoing Authorization	A determination of risk; ongoing authorization to operate, ongoing authorization to use, ongoing common control authorization; denial of ongoing authorization to operate, denial of ongoing authorization to use, denial of ongoing common control authorization.	• System Authorization Decision
Monitor	TASK M-7 System Disposal	Disposal strategy; up-to-date system component inventory; up-to-date system plans.	• System Component Inventory • System Operational Status • System Plan Change Records

Appendix B. List of Abbreviations and Acronyms

C-SCRM
Cybersecurity Supply Chain Risk Management

CIO
Chief Information Officer

CPRT
Cybersecurity and Privacy Reference Tool

CUI
Controlled Unclassified Information

DevSecOps
Development, Security, and Operations

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Modernization Act

FOCI
Foreign Ownership, Control, or Influence

GRC
Governance, Risk, and Compliance

IR
Internal Report or Interagency Report

ISCM
Information Security Continuous Monitoring

MOU
Memorandum of Understanding

NARA
National Archives and Records Administration

OMB
Office of Management and Budget

OSCAL
Open Security Controls Assessment Language

PIA
Privacy Impact Assessment

PMO
Program Management Office

PRA
Privacy Risk Assessment

PRAM
Privacy Risk Assessment Methodology

RMF
Risk Management Framework

SBOM
Software Bill of Materials

SCRM
Supply Chain Risk Management

SIEM
Security Information and Event Management

SOAR
Security Orchestration, Automation, and Response

SecCM
Security-focused Configuration Management

SORN
System of Records Notice

Appendix C. Glossary

availability
Ensuring timely and reliable access to and use of information. [44 U.S.C., Sec. 3542]

confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]

cybersecurity supply chain risk management
A systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. [SP800-161]

See *supply chain risk management*.

cybersecurity supply chain risk management plan
A formal document that describes the implementations, requirements, constraints, and implications of cybersecurity supply chain risk management (C-SCRM) controls selected for an information system or environment of operation that work in collaboration with the C-SCRM strategy, policies, and implementation plan to provide a systematic and holistic approach to cybersecurity supply chain risk management across an enterprise. The C-SCRM plan may be integrated with the system privacy and security plans into one consolidated document.

disassociability
Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system. [NIST PF]

information security program plan
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. [SP800-37] from [OMBA-130]

See *privacy program plan*.

integrity
Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]

machine-readable
When used with respect to data, means data in a format that can be easily processed by a computer without human intervention while ensuring no semantic meaning is lost. [44USC3502]

manageability
Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure. [NIST PF]

predictability
Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service. [NIST PF]

privacy
Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. [SP800-188]

privacy continuous monitoring program
An agency-wide program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or

dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at an agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. [OMBA-130]

privacy control
The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. [OMBA-130]

privacy control assessment
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. [OMBA-130]

privacy plan
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. [OMBA-130]

> *Note*: The security plan and the privacy plan may be integrated into one consolidated system artifact.

privacy program plan
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. [SP800-37] from [OMBA-130]

See *information security program plan*.

privacy requirements
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. [SP800-37]

> *Note*: The term "privacy requirement" can be used in a variety of contexts, from high-level policy activities to low-level implementation activities in system development and engineering disciplines.

privacy risk
The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur. [NISTPF]

privacy risk management
A cross-organizational set of processes for identifying, assessing, and responding to privacy risks. [NISTPF]

risk management
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. [OMBA-130]

security
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. [SP800-37]

security plan
A 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 system security plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems. [SP800-53]

Note: The security plan and the privacy plan may be integrated into one consolidated system artifact.

software bill of materials
A formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open-source and commercial software components. The SBOM enumerates these components in a product. [EO14028]

supply chain
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. [OMBA-130]

supply chain risk
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. [OMBA-130]

supply chain risk information
Includes, but is not limited to, information that describes or identifies: (1) Functionality of covered articles, including access to data and information system privileges; (2) Information on the user environment where a covered article is used or installed; (3) The ability of the source to produce and deliver covered articles as expected (i.e., supply chain assurance); (4) Foreign control of, or influence over, the source (e.g., foreign ownership, personal and professional ties between the source and any foreign entity, legal regime of any foreign country in which the source is headquartered or conducts operations); (5) Implications to national security, homeland security, and/or national critical functions associated with use of the covered source; (6) Vulnerability of federal systems, programs, or facilities; (7) Market alternatives to the covered source; (8) Potential impact or harm caused by the possible loss, damage, or compromise of a product, material, or service to an organization's operations or mission; (9) Likelihood of a potential impact or harm, or the exploitability of a system; (10) Security, authenticity, and integrity of covered articles and their supply and compilation chain; (11) Capacity to mitigate risks identified; (12) Credibility of and confidence in other supply chain risk information; (13) Any other information that would factor into an analysis of the security, integrity, resilience, quality, trustworthiness, or authenticity of covered articles or sources; (14) A summary of the above information and, any other information determined to be relevant to the determination of supply chain risk. [FASCSA]

supply chain risk management
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. [OMBA-130]

See *cybersecurity supply chain risk management*.

system-related privacy risk
Risk to an individual or individuals associated with the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their PII. [OMBA-130]

system-related security risk
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. [SP800-30]

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. [SP800-37]

A specialty engineering discipline of systems engineering. It applies scientific, mathematical, engineering, and measurement concepts, principles, and methods to deliver, consistent with defined constraints and necessary trade-offs, a trustworthy asset protection capability that satisfies stakeholder requirements; is seamlessly integrated into the delivered system; and presents residual risk that is deemed acceptable and manageable to stakeholders. [OMBA-130]

Appendix D. Change Log

NIST Special Publication (SP) 800-18r2 (Revision 2), *Developing Security, Privacy, and Supply Chain Risk Management Plans for Systems*, provides guidelines for developing and maintaining system security plans, system privacy plans, and C-SCRM plans.

- Section 2 defines and explains the system plan types based on the RMF [SP800-37], [SP800-161], and the NIST Privacy Framework.
- Section 3 updates the suggested elements for system security, privacy, C-SCRM plans and addresses the relationship between security risk management and privacy risk management. Material has been added to address the use of information management tools and automation to support the development, management, maintenance, and protection of system plan information.
- Section 4 relates the development and maintenance of system security, privacy, and C-SCRM plans to the implementation of the RMF.

In addition, the publication has been restructured and the following content changes have been applied:

- Technical content from other NIST publications is now included by reference rather than repeated.
- The terms *general support system*, *major application*, and *minor application* have been deprecated to be consistent with OMB Circular A-130 (July 2016) [OMBA-130].
- The term *system boundary* has been updated to *authorization boundary* for consistency with the terminology in [SP800-37].