NIST Special Publication 800
NIST SP 800-18r2 ipd

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

Initial Public Draft

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.ipd

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

NIST Special Publication 800
NIST SP 800-18r2 ipd

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

Initial Public Draft

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

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

Julie Snyder, Jeremy Miller[2]
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.ipd

June 2025

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

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

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 YYYY-MM-DD [Will be added to final publication.]
Supersedes NIST Series XXX (Month Year) DOI [Will be added to final publication.]

How to Cite this NIST Technical Series Publication

Licata J, McWhite R, Calloway L, Gilbert D, Anderson M, Snyder J, Miller J (2025) Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-18r2 ipd. https://doi.org/10.6028/NIST.SP.800-18r2.ipd

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

Public Comment Period
June 4, 2025 – July 30, 2025

Submit Comments
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/ipd, 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; privacy plan; 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 guidance provided in this publication:

- System Security Plan outline example
- System Privacy Plan outline example
- Cybersecurity Supply Chain Risk Management System 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 NIST Risk Management Framework (RMF).

Note to Reviewers

NIST welcomes feedback on the quality of the draft revision of this publication, including the technical accuracy of the material presented, the ease of navigating and understanding the material, and the impacts of the added, modified, and removed content.

This updated guidance for the development of system plans is intended to support:

- The development and maintenance of system plans following the NIST RMF
- Privacy risk management as reflected in the NIST Privacy Framework, the inclusion of privacy risk management in SP 800-37, and the updated controls in SP 800-53 to more fully support privacy objectives
- The increased attention to cybersecurity-related supply chain risks reflected in SP 800-161 and the supply chain risk management (SR) controls in SP 800-53
- The use of automation to capture, process, and report information in the system plans to facilitate risk management activities and decisions

NIST is particularly interested in feedback on the following:

- How do these guidelines align with your existing organizational practices for documenting or reporting security, privacy, and cybersecurity supply chain risk management efforts at the system level?
- How do you expect the guidelines and supplemental materials to influence your future practices and processes?
- What additional system plan elements would improve the usability of the information captured for the system plans?
- What additional considerations are there for automating the capture of system information using enterprise security tools that would improve organizational risk management efforts and risk decision-making?

Comments can be submitted using the comment template posted on the publication details page and sent to sec-cert@nist.gov with the subject "SP 800-18r2 ipd comments."

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: sec-cert@nist.gov

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 draft of this publication, specifically Jon Boyens, Michaela Iorga, Victoria Yan Pillitteri, Eduardo Takamura, Jim Foti, Isabel Van Wyk, and the CSD web team of the National Institute of Standards and Technology (NIST); 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; 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 system risks associated with information exchanges involving systems outside the authorization boundary. The structure and format of system plans are prepared according to organizational needs and the information described in this publication.

NIST Special Publication (SP) 800-18r2 (Revision 2) addresses the development and maintenance 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 develop and 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.

Federal agencies are required 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 these guidelines 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. *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 an authorization boundary and the system risks associated with information exchanges that involve systems outside of the authorization boundary.

- 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 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 that describe the system's purpose; environment of operation; information that is stored, processed, and transmitted; data flows within the environment and with interconnected systems; control implementation details; and the roles and responsibilities of individuals associated with the system. Automation and information management tools can facilitate the collection, presentation, and update of system plan information.[2]

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. These guidelines can also 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

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

- Organizations developing system plans for service offerings from cloud service providers, including software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS).

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 also utilize these guidelines to support their risk management programs.

1.1. Relationship to Other NIST Guidelines

This publication is designed to support the NIST portfolio of risk management initiatives and publications[4] 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]

1.2. Document Organization

The publication is organized into the following sections:

- Section 2 describes system security, system privacy, and C-SCRM plans.

[3] [FISMA] includes privacy protections in the definition for confidentiality. as indicated in [44 USC3552].
[4] 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].

- Section 3 identifies elements that may be included in system security, privacy, and C-SCRM plans.
- Section 4 describes how system plans are developed and maintained in relation to the RMF and with the support of automation.
- 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:

- 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

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

- Define the authorization boundary of the system;
- Support the organization's security, privacy, and C-SCRM objectives;
- Define capabilities to defend the organization against threats and threat actors;
- 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;
- 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;
- 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 implemented controls.

The information contained in system plans can be captured as documents or using different Governance, Risk and Compliance (GRC) tools. 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 the protections that are planned or in place to meet those requirements. The security plan:

- Enables organizational leadership and system management personnel to manage security risks and make effective risk management decisions throughout the system life cycle;
- Describes implemented or planned controls that address the system's security requirements;
- Identifies the individuals responsible for maintaining the security protections for information and information systems;
- Consolidates details about the system, including its purpose, authorization boundary, [FIPS199] security categorization, operational status, and environment of operations; and
- Demonstrates how security objectives (i.e., confidentiality, integrity, and availability) are achieved by following security engineering approaches to building resilient and trustworthy systems.

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)[5]; and
- Describes planned and implemented controls to address privacy requirements and data processing activities that may compromise privacy (i.e., problematic data actions[6]).

Privacy requirements may be informed by legal and regulatory obligations as well as privacy activities and artifacts, such as Privacy Impact Assessments (PIAs), Privacy Risk Assessments (PRAs),[7] System of Records Notices (SORNs), Memorandums of Understanding (MOUs), or other types of contracts or agreements. 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. The tasks in the RMF *Prepare* step identify sources of system privacy requirements.

2.2.1. Relationship Between the System Security Plan and System Privacy Plan

Organizational security and privacy programs have complementary objectives and overlapping risks with regard to confidentiality, integrity, and availability, as shown in Fig. 1.

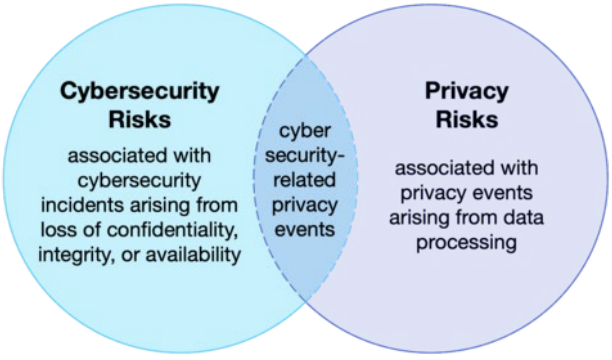

Fig. 1. Relationship between security and privacy risks

Both unauthorized data access and authorized disclosures that are made without sufficient disassociability can introduce privacy issues, physical harms, or economic losses. Systems must

[5] 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.
[6] Per the NIST Privacy Framework [NIST PF], a problematic data action (PDA) may cause an adverse effect for individuals.
[7] The NIST Privacy Risk Assessment Methodology [PRAM] helps organizations analyze, assess, and prioritize privacy risks to identify appropriate responses and solutions.

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.

Control implementation details differ between system privacy, security, and C-SCRM plans (see Sec. 3.8). While security-related controls can support system privacy outcomes, privacy risks require additional privacy-focused controls. Some controls may also introduce privacy risks that require additional management, such as controls related to monitoring for insider threats. Incorporating these privacy-focused controls into the system helps ensure that privacy is considered holistically alongside security concerns.

2.3. Cybersecurity Supply Chain Risk Management Plan

A C-SCRM strategy[9] addresses cybersecurity risks at the organization level throughout the supply chain, including commercial-of-the-shelf (COTS) products, turn-key solutions, and support services. A C-SCRM plan then incorporates those organization-level priorities, policies, and risk tolerances to address system-level risks and interdependencies with 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;
- 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; and
- Includes supplier and/or component inventories that specify the associated criticality to the system, key individuals who fill supply chain-relevant roles, security control implementation information that is specific to supply chain considerations, system diagrams, and interdependencies with other systems.

Different types of systems may have specific considerations that can be addressed in the C-SCRM plan, such as the system architecture, security categorization [SP800-60v2], or type of technology used within the system. All security controls from [SP800-53] with supply chain risk management applicability are listed in [SP800-161], Appendix A, which also features an

[8] Many laws, regulations, and guidance focus on a defined scope of information that is covered by privacy protections, such as [OMB A-130] and PII. However, data processing may potentially introduce privacy risks 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 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 the scope of this publication. This publication does not address many of the non-cybersecurity aspects of SCRM.

enhanced overlay of control enhancements that are specific to supply chains as well as implementation guidance.

2.4. Consolidated System Plans

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 Description, Authorization Boundary and System Environment) 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.

Automation using information management tools (see Sec. 4.8) can support the collection and compilation of distinct security, privacy, and C-SCRM control implementation details; common system plan elements; and roles and responsibilities.

3. Elements of System Plans

This section recommends informational elements to include in system plans. Information management tools (e.g., GRC) can be used to capture and report system information and control implementation details following consistent and logical structures that address security, privacy, and C-SCRM risk management objectives.

3.1. System Name and Identifier

Designate a unique system name and identifier to distinguish one system from another in organizational records.

The assigned system identifier is applied to the system plans and artifacts that are associated with the system and remains the same throughout the system life cycle. It facilitates the traceability of, identification of, and responses to privacy and security events (e.g., access to data, data transfers). Where possible, the system identifier is referenced in PIAs and PRAs to link privacy risks to specific systems and their associated controls.

For a complex system (e.g., [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.

3.2. System Plan Reviews and Change Records

Provide a method for recording system plan reviews and changes over the course of the system life cycle.

System plan reviews ensure accountability for periodic (e.g., life cycle milestones, gate reviews, and significant contracting activities) and ad hoc changes. Organization-designated individuals can verify the accuracy and completeness of the information included 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. A system plan change record focuses on specific updates that are made to the system plan rather than changes that are addressed by system change control processes (e.g., CM-03, *Configuration Change Control*). The change record may include additional information, such as:

- Date of review and revision
- Plan revision or version identifier
- Description of change or revision
- The section affected
- Changes made by name, title, and/or organization

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. While document management processes may require manual change record updates, information management tools can automatically track the changes made to specific system plan elements and generate reports that identify those changes and the users who approved and implemented them.

3.3. 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.

Depending on the system plan type, individuals with roles and responsibilities for coordinating system-specific risk management activities may be identified, including the system security officer, system privacy officer, and personnel who support the C-SCRM Program Management Office (PMO). An organization may identify other individuals who support system plan development, as needed.

Organizations include the following contact information for each individual:

- Name
- Role (e.g., system-specific role, organizational role)
- 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 individuals.

3.4. System Operational Status

Indicate the operational status of the system.

The system operational status identifies the readiness of system functionality in an operational environment with the following indicators:

- **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 major modification** —The authorized operational system is undergoing a major change to the operational environment.

- **Disposal** — The system is no longer authorized, operational, or under development.

For complex systems, include the operational status of the subsystems within the authorization boundary.

System Plan Approval

System plan approval is critical prior to control implementation for systems under development. By approving the system plans, the authorizing official or designated representative accepts and agrees to the set of controls and their proposed allocation and implementation. Input from other organizational officials provides information to support approval of the system plans, such as:

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

The 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.

Subsequent reauthorizations or ongoing authorizations ensure that updates to the system plan based on the actual implementation of the controls are reviewed and approved [SP800-37]. System management may update the system plan approval each time the system plan is reviewed to maintain accountability for the content.

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

System Authorization Decision

Prior to a system being put into the operational environment, or to maintain its operational status, an authorization decision is made by the authorizing official. The system plan may include references to authorization decision artifacts, such as an authorization to operate (ATO) letter or memorandum issued by the authorizing official that explains the terms and conditions of the authorization decision. If the organization implements a 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 information security continuous monitoring (ISCM) strategy that includes ongoing authorization.

3.5. System Description

> Provide a high-level overview of the system's characteristics, its purpose, and how it supports the organization's mission.

Identify technologies or 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. Summarize the system user base and identify user roles that require privileged access and access to data about individuals to ensure accountability and transparency.

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 addresses how risks related to the collection, use, and sharing of data are managed and how those practices align with the organization's privacy policies. The system description in the privacy plan aligns with the information provided in the PIA, PRA, and other applicable privacy documentation (e.g., SORN, MOU, other types of contracts or agreements).

3.6. System Information Types and System Categorization

> Identify the information types that are processed, stored, or transmitted by the system, and categorize them by their impact level for each security objective (i.e., confidentiality, integrity, availability).

Organizations identify the [SP800-60v2] information types that are processed, stored, or transmitted by the system; their impact levels (i.e., low, moderate, and high) based on risk management activities, system artifacts (e.g., Risk Assessment Report, PIA, SORN), and guidance on the categorization of federal information and systems [FIPS199]; and justifications for adjusting the provisional impact levels following the guidelines in [SP800-60v1]. Special conditions may be applied to the information type provisional impact levels, and the high-water mark for each of the security impacts determine the final system categorization.

3.7. Authorization Boundary and System Environment

> Define the scope of the system protections that encompass the authorization boundary, including all components of the system to be authorized for operation.

The system plan can 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 providers or offerings.

3.7.1. Authorization Boundary Description

Include system diagrams that clearly depict the components of the system architecture within the authorization boundary. Supporting topology narratives may also be provided.

Graphic representations of the key internal boundaries, critical components, subsystems, primary and secondary data stores, virtual components, information exchanges, and services from third-party providers demonstrate how resilience and redundancy are addressed in the system architecture. 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.

System Diagrams

Identify the physical and logical locations of the system components in the authorization boundary. 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.

Physical and environmental protections are identified, including physical entry points and the locations of environmental control systems (e.g., climate control systems, fire control systems).

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 physical and logical protections 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:

- Where data is created
- Where data enters and exits key internal boundaries

- The flow of information that results from information exchanges with external organization systems

3.7.2. System Component Inventory

Identify the inventory of components being used within the authorization boundary.

System components are discrete, identifiable information technology assets that represent the building blocks of a system. The system plan may summarize the component inventory and provide instructions for acquiring information about their provenance[10] and the following component details from an authoritative source (e.g., an endpoint management application):

- Hardware component description, function, role, and deployment date
    - Unique component identifier (e.g., serial number, asset tracking identifier, other service codes that identify supply chain information)
    - Manufacturer and model, including sub-model identifiers or distinctions (e.g., subcomponent country of origin)
    - Warranty duration, expiration date, and/or maintenance support contract status
    - Specific physical locations (e.g., a rack in a server room)
- Software product version, revision number, or build information
    - Software developer, manufacturer, and vendor, including for subcomponents
    - Secure software development attestation[11]
    - Product license type (e.g., single user, volume license, public license, freeware)
    - Software warranty and maintenance support contract status
    - Product license expiration date

System personnel maintain the system component inventory that is included or referenced in the system plan. The physical inventory is often distinct from the system component inventory and is handled through procurement and property management procedures. 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.

[10] 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."

[11] [SP 800-218] discusses the Secure Software Development Framework (SSDF), which supports the provisions of [EO 14028] for ensuring the secure functionality of software. [OMB M-22-18] and [OMB M-23-16] require an attestation form in which software producers confirm the implementation of specific security practices in the development of software products.

3.8. Control Implementation Details

Identify the selected controls — starting with the control selection approach used — and provide implementation details for all of the controls that are allocated to the system.

The organization determines their approach for selecting, tailoring, and allocating controls for systems. [SP800-37] describes two approaches for selecting controls: an organization-generated control selection approach and a baseline control selection approach. The organization-generated control selection approach allows organizations to apply their own methodology to select controls to manage risk. Organizations consider applicable Cybersecurity and Privacy Framework Profiles to identify controls that support the achievement of security and privacy risk management outcomes. When using the baselines in [SP800-53B], identify baseline controls that have been removed, supplemental controls that were added as a result of tailoring activities, and the rationale and approval for all changes. The planned and actual control implementation details for each allocated control provide sufficient information to implement and assess the effectiveness of the control in addressing security, privacy, and C-SCRM requirements throughout the authorization boundary.

Additional information supporting control implementation includes:

- Control implementation status (e.g., planning, planned/implementation incomplete, implemented as planned, implemented/tailored)
- Planned inputs, related data sources, and expected system outputs for controls that are implemented in the hardware, software, or firmware components of the system
- Special considerations for data processing and distribution
- Summary of tailoring activities and resulting tailoring decisions
- Location of related policy and procedure artifacts
- Components, products, or services associated with the control
- Roles or specific entities that are responsible for control implementation, including information about shared responsibilities for hybrid controls

Other system artifacts may be referenced, including risk assessment results, plans of action and milestones (POA&Ms), authorization decision information, and other plans (e.g., contingency plan, configuration management plan, incident response plan) that provide more details about the control implementation. Additional information can be obtained from a variety of sources, such as network monitoring tools, security orchestration services, vulnerability scanning tools, endpoint management tools, and GRC tools.

Common controls inherited by the system are identified in the system plan by reference. The implementation details for common controls are provided in the artifacts developed by common control providers that are made available to system owners.

For hybrid controls, the system plan identifies who is responsible for the control implementation; how the associated security, privacy, and cybersecurity supply chain risks are

shared; and which parts of the control are provided by the common control provider or are implemented at the system level.

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 like transparency, data minimization, and purpose specification.
- **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.
- **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 require different control implementations compared to security controls, which are primarily concerned with protecting systems and information rather than individuals.

Control implementation details in the C-SCRM plan reflect the mitigation of cybersecurity risks throughout the supply chain. [SP800-161], Appendix A, 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 CIO, senior accountable official for risk management, C-SCRM PMO, or senior procurement executive.

3.9. Information Exchanges

Provide an overview of the information exchanges in which the system participates.

Information exchanges are defined between systems that exchange data across authorization boundaries, whether inside or outside the organization [SP800-47]. Such agreements may 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.

In the system plan, identify the following for each information exchange in which the system participates:

- 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
- 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 the 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
    - ISCM processes that identify security and privacy risks and mitigation strategies.

Exchanges involving data about individuals have the potential to introduce additional privacy risks. The system privacy plan describes the 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.

3.10. Laws, Regulations, and Policies Affecting the System

Identify current laws, regulations, and policies that influence organizational policies and system requirements.

The system plan can identify the sources of specific requirements for the confidentiality, integrity, or availability of the system; the predictability, manageability, and disassociability of information processed, stored, or transmitted by the system; and the protection of 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, organizational policy, or other regulatory exclusions that define system-specific constraints.

3.11. Digital Identity Acceptance Statement

Provide a Digital Identity Acceptance Statement, as described in [SP800-63-3].

Organizational and system-level risk assessments determine the extent to which risk is managed by various processes,[12] 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.

3.12. Referenced Artifacts

Provide or identify the location of artifacts that are referenced in the system plan.

Verify that the system artifacts referenced in control implementation details or other system plan elements are available to authorized reviewers, such as organizational leadership, system management, and control assessors. Example artifacts may include the authorization decision artifact, contingency plan, configuration management plan, ISCM plan, incident response plan, information exchange and data sharing agreements, and risk assessment reports.

[12] [SP 800-63-3] 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.

3.13. Acronym List and Glossary

Define acronyms or terms that are used in the system plan and have organization- or system-specific meanings.

An information management tool may provide organization-specific terms and acronyms defined to standardize references to system objectives, objects, requirements, and technologies. If necessary, system-specific terms and acronyms may be explained in the system plan to provide additional context.

4. System Plan Development and Maintenance

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. The following section identifies how systems plans are related to each step of the RMF.

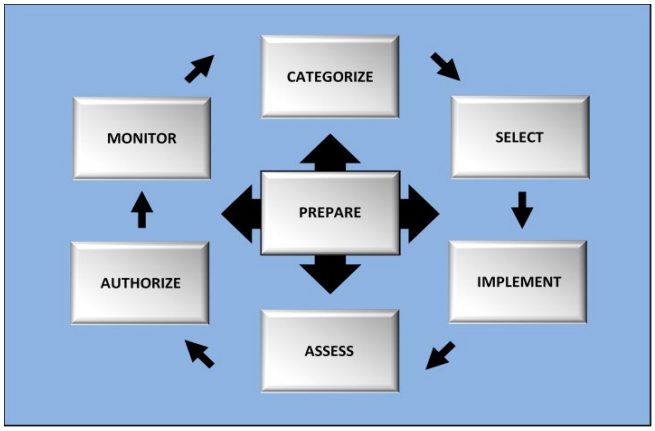

Fig. 2. NIST Risk Management Framework Steps

Appendix A summarizes the outputs associated with specific RMF tasks that are included in the system plans.

4.1. Prepare

System plans support organizational 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. 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, such as data minimization, transparency, and consent management. It may also identify 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 guidance 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 and 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 updated to revise existing or 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[13] 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, and general procurement from unauthorized resellers.

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 also 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.

[13] 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.

4.3. Select

System plans identify the controls that are selected and allocated to the system for implementation. More than one approach for selecting controls may be used as circumstances dictate, such as:

- **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.
- **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].[14] 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[15]) as a starting point for selecting controls with broad-based support across communities of interest for specific circumstances, situations, and/or conditions.

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 environment of operations. Tailoring can address the impacts associated

[14] 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.

[15] [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.

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;
- ODP values for control assignment and selection operations;
- Additional controls that supplement the baseline, such as controls based on Cybersecurity and Privacy Framework Profiles;[16]
- 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 guidance 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.[17] Notes may be added to the implementation details to describe how fully inherited controls address system requirements.

[16] 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.

[17] 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.

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 (see Sec. 3.4). This review ensures that privacy risks have been thoroughly identified and that 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 the assessment plan [SP800-53A]. The subsequent report identifies whether the controls in the assessment scope are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system’s security, privacy, and supply chain risk management requirements. 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.[18]

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 includes the system security and system privacy plans and any referenced artifacts. The C-SCRM plan is not required but may be included.

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[19] to ensure their continued accuracy and relevancy after authorization. Reviews may also 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 SCRM requirements
- Updates to the system risk assessment report that identify new risks that render existing controls less effective

[18] A system may go through multiple assessments and system plan updates during the system development life cycle in preparation for the RMF *Authorize* step.
[19] [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.

- 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)
- 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, including revision or version identifiers to maintain a record of changes as well as specific procedures for tracking and managing modifications in the system configuration management plan. Automating information collection methods (see Sec. 4.8) can result in more efficient and effective system plan maintenance.

Reauthorization or Ongoing Authorization

The continued operation of an authorized system requires periodic or ongoing assessments to verify that the implemented controls still 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 to compromise both physical and logical data. System plans include instructions for properly disposing of systems or components (e.g., sanitization of storage media), the date of system disposal, and records of information assets that are transferred to other systems. The disposal strategy may also be integrated into the control implementation details. Updates to the system component inventory may trigger additional updates to the system plans to reflect changes in the environment of operations.

Additionally, the roles and responsibilities of all parties are clearly defined and communicated, including policies and procedures for responding to data exposure incidents that may occur during or after the disposal process. Decisions regarding the retention, transfer, or deletion of data are made by the system owner, information owner, authorizing official, and/or senior organization official for privacy in compliance with applicable data and records retention requirements, such as those provided by the National Archives and Records Administration [NARARECM].

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,[20] 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.

4.8. Automation Support

Maximizing the use of automation, wherever possible, can increase the effectiveness and efficiency of maintaining system plans throughout the system life cycle. Organizations have the flexibility to decide when, where, and how to use automation or automated support tools for plan development and monitoring.[21] Smaller organizations (e.g., micro government agencies, small businesses with fewer systems) may benefit from collecting system information in

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

[21] 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).

individual system plans that can be stored in an organization-wide repository. Larger organizations that operate more systems may benefit from an organization-wide information management tool (e.g., GRC tool) with a centralized data repository to consolidate and correlate system plan information across the organization.

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

4.8.1. Collection

Information is 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[22])
- Personnel contact information from an organizational directory
- Information types that are detected within the system but are 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

This data informs various management activities, such as prioritizing security, privacy, or SCRM initiatives and allocating resource based on impact priorities. Automating the collection of system-level risk information in a centralized repository following organization-defined data standards can reduce inconsistencies.

4.8.2. Protection

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

- Control the visibility of system plan data to specific access holders based on their roles
- 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.

[22] [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 configuration for particular system components.

4.8.3. Sharing and Usability

Maintaining system plan information in a central repository can improve the responsiveness of risk-based decision-making by senior officials and system risk managers. Authorizing officials and system owners review and update system information as needed (e.g., using automated information collection) to support continuous monitoring activities, ongoing assessments, and authorization processes. System management personnel 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 authorization schedules, POA&M status (e.g., late POA&Ms, expiring POA&Ms), and accepted risk information.

The information management tool can also share control status and implementation information with internal and external interconnected systems, systems that inherit common and hybrid controls, external organizations, and system owners with authorized visibility. Compensating controls can be applied at the system level and included in the system plans to account for unresolved POA&Ms and inherited risks in the common control implementations and to maintain the necessary levels of protection to safeguard system assets and information.

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.

4.8.4. Management

Automation also facilitates system plan management, including:

- Tracking changes to system plan elements, including the control implementations, agreements for information exchanges, POA&Ms, and supporting roles
- 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.

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
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-22-18]	Office of Management and Budget Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, September 2022. Available at https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf
[OMBM-23-16]	Office of Management and Budget Memorandum M-23-16, Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, June 2023. Available at https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security-1.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

[NISTCSF] National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), Version 2.0. (February 2024) (National Institute of Standards and Technology, Gaithersburg, MD), 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

[SP800-63-3] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63-3. Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[SP800-88] Kissel R, Regenscheid A, Scholl M (2014) Guidelines for Media Sanitization (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-88r1. https://doi.org/10.6028/NIST.SP.800-88r1

[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

[SP800-161] 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 RS, Pillitteri VY (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 RS, Pillitteri VY (2024) Assessing Security Requirements for Controlled Unclassified Information. (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] Ross RS, Pillitteri VY (2021) Enhanced Security Requirements for Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.: A Supplement to NIST Special Publication 800-171. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-172. https://doi.org/10.6028/NIST.SP.800-172

[SP800-172A] Ross RRS, Pillitteri VY (2022) Assessing Enhanced Security Requirements for Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-172A. https://doi.org/10.6028/NIST.SP.800-172A

[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

MISCELLANEOUS PUBLICATIONS AND RESOURCES

[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

[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

[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 1 can be found in the [CPRT] reference dataset for SP 800-37.

Table 1. RMF task outputs related to system plan elements

RMF Step	RMF Task	RMF Task Outputs	Related System Plan Element
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 controls and providers that are available for inheritance; security and privacy plans (or equivalent documents) that describe 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 or business processes that the system will support	• System Description
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 Narrative and Diagrams • System Component Inventory
Prepare — System Level	TASK P-11 Authorization Boundary	Documented authorization boundary	• Authorization Boundary and System Environment
Prepare — System Level	TASK P-12 Information Types	A list of information types for the system	• System Information Types and System Categorization
Prepare — System Level	TASK P-13 Information Life Cycle	Documentation of the stages through which information passes in the system throughout its life cycle, including data maps, data flow diagrams, entity relationship diagrams, database schemas, and data dictionaries	• Authorization Boundary and System Environment

RMF Step	RMF Task	RMF Task Outputs	Related System Plan Element
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 and System Environment
Prepare — System Level	TASK P-17 Requirements Allocation	List of security and privacy requirements for the system, system elements, and environment of operation	• Control Implementation Details
Prepare — System Level	TASK P-18 System Registration	A system identifier that is added to the organization-wide system inventory as part of the system registration process	• System Name and Identifier
Categorize	TASK C-1 System Description	Documented system description	• System Description
Categorize	TASK C-2 Security Categorization	Impact levels that are determined for each information type and security objective (i.e., confidentiality, integrity, availability); security categorization based on a high-water mark of information type impact levels	• System Information Types and System Categorization
Categorize	TASK C-3 Security Categorization Review and Approval	Approval of security categorization for the system	• System Information Types and System Categorization
Select	TASK S-1 Control Selection	Controls that are selected for the system and 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
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	Documentation of the controls for the system and environment of operation in security and privacy plans	• Control Implementation Details
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

RMF Step	RMF Task	RMF Task Outputs	Related System Plan Element
Select	TASK S-6 Plan Review and Approval	Privacy plan reviewed by the senior agency official for privacy; C-SCRM plan reviewed by the senior procurement executive and/or C-SCRM Program Management Office (PMO); security, privacy, and C-SCRM plans approved by the authorizing official	• System Operational Status
Implement	TASK I-1 Control Implementation	Implemented controls	• Control Implementation Details
Implement	TASK I-2 Update Control Implementation Information	System plans updated with implementation details that are sufficient for use by assessors	• Control Implementation Details
Assess	TASK A-5 Remediation Actions	Initial remediation actions completed based on security and privacy assessment reports; changes to implementations reassessed by the assessment team; updated security and privacy assessment reports; updated security and privacy plans, including changes to control implementations	• Control Implementation Details
Authorize	TASK R-2 Risk Analysis and Determination	Authorizing official analyzes the relevant security and privacy risk information provided by the automated security/privacy management and reporting tool to determine the current security and privacy posture of the system	• Control Implementation Details
Authorize	TASK R-3 Risk Response	Security and privacy plans include an accurate description of implemented controls, including compensating controls after control reassessments are completed	• Control Implementation Details
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 Operational Status
Authorize	TASK R-5 Authorization Reporting	Authorization decision	• System Operational Status
Monitor	TASK M-1 System and Environment Changes	Updated security, privacy, and C-SCRM plans	• System Description • Authorization Boundary and System Environment • Control Implementation Details • Information Exchanges

RMF Step	RMF Task	RMF Task Outputs	Related System Plan Element
Monitor	TASK M-2 Ongoing Assessments	Updated security and privacy assessment reports; updated supplier assessments required for C-SCRM plan	• Authorization Boundary and System Environment • Control Implementation Details • Information Exchanges
Monitor	TASK M-3 Ongoing Risk Response	Modified, enhanced, or added controls are reassessed by assessors to ensure that they have been implemented correctly, are operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements of the system	• Authorization Boundary and System Environment • Control Implementation Details • Information Exchanges
Monitor	TASK M-4 Authorization Package Updates	Organization updates security and privacy plans, security and privacy assessment reports, and POA&Ms on an ongoing basis to reflect modifications to controls based on risk mitigation activities	• System Operational Status
Monitor	TASK M-7 System Disposal	Disposal strategy; up-to-date system component inventory; up-to-date security and privacy plans	• System Plan Reviews and Change Records • System Operational Status

1267

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

SCRM
Supply Chain Risk Management

SecCM
Security-focused Configuration Management

SORN
System of Records Notice

Appendix C. Glossary

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 also *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.

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 also *privacy program plan*.

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]

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 also *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.

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 also *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

Draft 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.
- Section 4 relates the development and maintenance of system security, privacy, and C-SCRM plans to the implementation of the RMF. 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.

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].