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

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

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.*

June 2025

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.]

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

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

1 **Abstract**

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

10 **Keywords**

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

18 **Reports on Computer Systems Technology**

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

29

30 **Supplemental Content**

31 The following materials are available on the <u>publication details page</u> to supplement the
32 guidance provided in this publication:

33 • System Security Plan outline example

34 • System Privacy Plan outline example

35 • Cybersecurity Supply Chain Risk Management System Plan outline example

36 • System Plan Roles and Responsibilities

37 **Audience**

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

39 • Individuals with information security, privacy, and risk management program oversight
40   responsibilities (e.g., authorizing officials, senior agency information security officers,
41   senior agency officials for privacy)

42 • Individuals with system development responsibilities (e.g., mission or business owners,
43   program managers, systems engineers, systems security engineers, systems privacy
44   engineers, software developers, systems integrators, acquisition or procurement
45   officials)

46 • Individuals with system security and privacy implementation and operations
47   responsibilities (e.g., mission or business owners, system owners, information owners or
48   stewards, system administrators, system security officers, system privacy officers)

49 • Individuals with cybersecurity supply chain risk management-related responsibilities
50   (e.g., C-SCRM program managers)

51 • Individuals with acquisition and procurement-related responsibilities (e.g., acquisition
52   officials, contracting officers)

53 • Individuals with logistical or disposition-related responsibilities (e.g., program managers,
54   system integrators, property managers)

55 • Individuals with control assessment and monitoring responsibilities (e.g., auditors,
56   Inspectors General, system evaluators, control assessors, independent verifiers and
57   validators, analysts)

58 • Commercial entities and industry partners that produce component products and
59   systems, create security and privacy technologies, or provide services or capabilities that
60   support information security or privacy

61 The material presented in this publication assumes that the audience has a basic understanding
62 of the NIST Risk Management Framework (RMF).

63 **Note to Reviewers**

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

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

68 • The development and maintenance of system plans following the NIST RMF

69 • Privacy risk management as reflected in the NIST Privacy Framework, the inclusion of
70 privacy risk management in SP 800-37, and the updated controls in SP 800-53 to more
71 fully support privacy objectives

72 • The increased attention to cybersecurity-related supply chain risks reflected in SP 800-
73 161 and the supply chain risk management (SR) controls in SP 800-53

74 • The use of automation to capture, process, and report information in the system plans
75 to facilitate risk management activities and decisions

76 NIST is particularly interested in feedback on the following:

77 • How do these guidelines align with your existing organizational practices for
78 documenting or reporting security, privacy, and cybersecurity supply chain risk
79 management efforts at the system level?

80 • How do you expect the guidelines and supplemental materials to influence your future
81 practices and processes?

82 • What additional system plan elements would improve the usability of the information
83 captured for the system plans?

84 • What additional considerations are there for automating the capture of system
85 information using enterprise security tools that would improve organizational risk
86 management efforts and risk decision-making?

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

89

90   **Call for Patent Claims**

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

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

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

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

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

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

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

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

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

117   **Table of Contents**

155   **List of Tables**

157   **List of Figures**

160

161

162   **Acknowledgments**

171

172 **Executive Summary**

173 *System plans* collectively refer to the *system security plan*, *system privacy plan*, and
174 *cybersecurity supply chain risk management* (C-SCRM) *plan* that describe the design and
175 implementation of security, privacy, and cybersecurity supply chain protections throughout the
176 system life cycle. System plans include information about the data being created, collected,
177 disseminated, used, stored, and disposed; identify individuals who are responsible for system
178 risk management efforts; describe the environment of operation, system components, and data
179 flows within the environment; and account for system risks associated with information
180 exchanges involving systems outside the authorization boundary. The structure and format of
181 system plans are prepared according to organizational needs and the information described in
182 this publication.

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

186 • Provides content considerations for elements in system plans;

187 • Discusses the use of automation to develop and maintain system plans over the system
188 life cycle, including sharing and protecting system plan information; and

189 • Provides supplemental materials, including system plan outline examples and updated
190 roles and responsibilities associated with system plans that may factor into system plan
191 development.

192 Federal agencies are required to develop and maintain system plans for managing risks,
193 including implementation details for the controls allocated to address the requirements.
194 Nonfederal organizations may voluntarily apply these guidelines to develop and maintain
195 system plans consistent with their risk management strategies.

196 **1. Introduction**

197 All systems that process, store, and transmit information within an organization need
198 safeguards that adhere to an organization-wide risk management strategy to address security,
199 privacy, and cybersecurity supply chain risks. *System plans* collectively refer to the *system*
200 *security plan*, *system privacy plan*, and *cybersecurity supply chain risk management* (C-SCRM)
201 *plan*, which describe the assets and individuals being protected within an authorization
202 boundary and the system risks associated with information exchanges that involve systems
203 outside of the authorization boundary.

204 • The **system security plan** describes the system security requirements, including the
205 controls selected to protect the confidentiality, integrity, and availability of the system
206 and its information.

207 • The **system privacy plan** describes the system privacy risk management requirements,
208 including the controls selected to address predictability, manageability, and
209 disassociability.[1]

210 • The **C-SCRM plan** describes the system's C-SCRM requirements, including the controls to
211 manage, implement, and monitor the supply chain and develop and sustain the system
212 across mission and business functions.

213 The NIST Risk Management Framework (RMF) [SP800-37] provides a flexible methodology for
214 organizations and systems to manage security, privacy, and supply chain risks. The expected
215 outputs of RMF tasks (see Appendix A) inform the system plan elements that describe the
216 system's purpose; environment of operation; information that is stored, processed, and
217 transmitted; data flows within the environment and with interconnected systems; control
218 implementation details; and the roles and responsibilities of individuals associated with the
219 system. Automation and information management tools can facilitate the collection,
220 presentation, and update of system plan information.[2]

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

224 • Common control providers that provide implementation details for controls available to
225 be inherited by other systems;

226 • Requirements identified in [SP800-171] and [SP800-172] for the development of system
227 security plans for nonfederal organizations protecting Controlled Unclassified
228 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.

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

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

1.1. Relationship to Other NIST Guidelines

238   This publication is designed to support the NIST portfolio of risk management initiatives and
239   publications[4] that address security, privacy, and supply chain risk management concepts and
240   methodologies, including:

241   • SP 800-37, *Risk Management Framework for Information Systems and Organizations: A*
242   *System Life Cycle Approach for Security and Privacy* [SP800-37]

243   • SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*
244   [SP800-53]

245   • SP 800-53A, *Assessing Security and Privacy Controls in Information Systems and*
246   *Organizations* [SP800-53A]

247   • SP 800-53B, *Control Baselines for Information Systems and Organizations* [SP800-53B]

248   • SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and*
249   *Organizations* [SP800-161]

250   • SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and*
251   *Organizations* [SP800-171]

252   • SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified*
253   *Information* [SP800-172]

254   • *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk*
255   *Management* [NISTPF]

256   • *The NIST Cybersecurity Framework* (CSF) [NISTCSF]

1.2. Document Organization

258   The publication is organized into the following sections:

259   • 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].

260   • Section 3 identifies elements that may be included in system security, privacy, and
261   C-SCRM plans.

262   • Section 4 describes how system plans are developed and maintained in relation to the
263   RMF and with the support of automation.

264   • The References section lists the source materials cited in this publication.

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

267   • Appendix A summarizes the RMF task outputs included in system plans.

268   • Appendix B lists the abbreviations and acronyms used in this publication.

269   • Appendix C provides a glossary of the terms used in this publication.

270   • Appendix D provides a publication change log.

271 **2. Overview**

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

274 • Define the authorization boundary of the system;

275 • Support the organization's security, privacy, and C-SCRM objectives;

276 • Define capabilities to defend the organization against threats and threat actors;

277 • Identify individuals who are responsible for managing and supporting the system;

278 • Help organizational personnel understand how to manage risks to an acceptable level
279 throughout the system life cycle and respond to changing risks in a timely manner;

280 • Consider requirements for information technology, operational technology, and
281 emerging technologies that may be informed by system artifacts, such as risk
282 assessments, business impact analyses (BIAs), and information exchange agreements;

283 • Provide sufficient evidence to support risk-based decisions regarding the ongoing
284 operation or use of the system; and

285 • Require methodical reviews and periodic updates to maintain information about the
286 system's mission, technologies, components, personnel, and implemented controls.

287 The information contained in system plans can be captured as documents or using different
288 Governance, Risk and Compliance (GRC) tools. This section addresses the objectives and
289 purposes of the system security plan, system privacy plan, and C-SCRM plan.

290 **2.1. System Security Plan**

291 The system security plan identifies the system's security requirements and the protections that
292 are planned or in place to meet those requirements. The security plan:

293 • Enables organizational leadership and system management personnel to manage
294 security risks and make effective risk management decisions throughout the system life
295 cycle;

296 • Describes implemented or planned controls that address the system's security
297 requirements;

298 • Identifies the individuals responsible for maintaining the security protections for
299 information and information systems;

300 • Consolidates details about the system, including its purpose, authorization boundary,
301 [FIPS199] security categorization, operational status, and environment of operations;
302 and

303 • Demonstrates how security objectives (i.e., confidentiality, integrity, and availability) are
304 achieved by following security engineering approaches to building resilient and
305 trustworthy systems.

306 **2.2. System Privacy Plan**

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

- 309 • Aligns the system's privacy objectives with the organization's mission, risk tolerance,
  310 and privacy goals;

- 311 • Defines system requirements with respect to the privacy engineering objectives of
  312 predictability, manageability, and disassociability and the Fair Information Practice
  313 Principles (FIPPs)[5]; and

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

316 Privacy requirements may be informed by legal and regulatory obligations as well as privacy
317 activities and artifacts, such as Privacy Impact Assessments (PIAs), Privacy Risk Assessments
318 (PRAs),[7] System of Records Notices (SORNs), Memorandums of Understanding (MOUs), or
319 other types of contracts or agreements. This includes identifying and cataloging key inputs,
320 such as data actions, contextual factors that describe the circumstances surrounding data
321 processing, privacy capabilities, and privacy engineering and security objectives based on
322 organizational mission needs, risk tolerance, and privacy goals. The tasks in the RMF *Prepare*
323 step identify sources of system privacy requirements.

324 **2.2.1. Relationship Between the System Security Plan and System Privacy Plan**

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

327
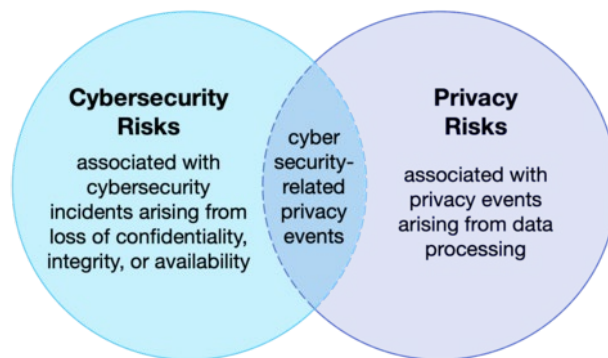
328 **Fig. 1. Relationship between security and privacy risks**

329 Both unauthorized data access and authorized disclosures that are made without sufficient
330 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.

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

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

340 **2.3. Cybersecurity Supply Chain Risk Management Plan**

341 A C-SCRM strategy[9] addresses cybersecurity risks at the organization level throughout the
342 supply chain, including commercial-of-the-shelf (COTS) products, turn-key solutions, and
343 support services. A C-SCRM plan then incorporates those organization-level priorities, policies,
344 and risk tolerances to address system-level risks and interdependencies with controls that
345 enhance trust and protection. The C-SCRM plan:

346   • Identifies policy implementations, requirements, constraints, and implications that are
347   specific to the cybersecurity supply chain at the system level;

348   • Describes the system's approach to managing supply chain risks that are associated with
349   the research, development, design, manufacturing, acquisition, delivery, integration,
350   operations, maintenance, and disposal of its components or services;

351   • Describes the system in the context of the organizational supply chain risk tolerance,
352   including acceptable supply chain risk response strategies or controls, a process for the
353   continuous evaluation and monitoring of supply chain risks, approaches for
354   implementing and communicating the plan, and a description of and justification for the
355   supply chain risk mitigation measures that are taken; and

356   • Includes supplier and/or component inventories that specify the associated criticality to
357   the system, key individuals who fill supply chain-relevant roles, security control
358   implementation information that is specific to supply chain considerations, system
359   diagrams, and interdependencies with other systems.

360 Different types of systems may have specific considerations that can be addressed in the
361 C-SCRM plan, such as the system architecture, security categorization [SP800-60v2], or type of
362 technology used within the system. All security controls from [SP800-53] with supply chain risk
363 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.

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

366 **2.4. Consolidated System Plans**

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

370 • Common elements in the security, privacy, and C-SCRM plans (e.g., System Name and
371   Identifier, System Operational Status, System Description, Authorization Boundary and
372   System Environment) provide consistent information about the system's mission,
373   purpose, and environment of operation.

374 • Roles and responsibilities are defined to support the ongoing collaboration between
375   individuals who are responsible for meeting system security, privacy, and C-SCRM
376   requirements.

377 • Each control that is allocated, tailored, and implemented or planned for implementation
378   has details that clearly address system requirements.

379 Automation using information management tools (see Sec. 4.8) can support the collection and
380 compilation of distinct security, privacy, and C-SCRM control implementation details; common
381 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

416 Updates to the system plan are approved and applied as part of organizational or system-
417 specific change management processes. The records help management understand the content
418 updates that have been implemented and verify that the authorization package contains the
419 most current revision of the system plans. While document management processes may
420 require manual change record updates, information management tools can automatically track
421 the changes made to specific system plan elements and generate reports that identify those
422 changes and the users who approved and implemented them.

423 **3.3. Role Identification and Responsible Personnel**

424 Identify the individuals who serve as authorizing officials and system owners as
425 well as other key roles with system responsibilities.

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

431 Organizations include the following contact information for each individual:

432 • Name

433 • Role (e.g., system-specific role, organizational role)

434 • Organizational unit, department, or division

435 • Primary business phone number

436 • Alternate business phone number

437 • Business email address

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

441 **3.4. System Operational Status**

442 Indicate the operational status of the system.

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

445 • **Under development** — The system is being designed or developed and is not fully
446 functioning in an operational environment.

447 • **Operational** — The authorized system is operating in the operational environment.

448 • **Undergoing a major modification** —The authorized operational system is undergoing a
449 major change to the operational environment.

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

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

System Plan Approval

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

459   • The system security plan requires concurrence from the senior accountable official for
460   risk management or risk executive (function), chief information officer (CIO), or senior
461   agency information security officer.

462   • The system privacy plan requires concurrence from the senior agency official for privacy
463   to demonstrate alignment between the organization's privacy and security programs.

464   • The C-SCRM plan requires coordination with the C-SCRM PMO.

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

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

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

System Authorization Decision

476 Prior to a system being put into the operational environment, or to maintain its operational
477 status, an authorization decision is made by the authorizing official. The system plan may
478 include references to authorization decision artifacts, such as an authorization to operate (ATO)
479 letter or memorandum issued by the authorizing official that explains the terms and conditions
480 of the authorization decision. If the organization implements a program for ongoing system
481 authorization, the ongoing authorization decision information may be referenced in the system
482 plan. The organization determines how to identify the authorization status of the system as a
483 part of an information security continuous monitoring (ISCM) strategy that includes ongoing
484 authorization.

485 **3.5. System Description**

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

488 Identify technologies or factors that present additional security- or privacy-specific risks, such
489 as cloud-based products and services, "bring your own device" (BYOD) policies, or the
490 processing of data about individuals. Summarize the system user base and identify user roles
491 that require privileged access and access to data about individuals to ensure accountability and
492 transparency.

493 While the system security plan may focus on broad cybersecurity risks, the system privacy plan
494 highlights the role of the system in handling personal data and the controls implemented in
495 response to associated privacy risks. For example, the system privacy plan addresses how risks
496 related to the collection, use, and sharing of data are managed and how those practices align
497 with the organization's privacy policies. The system description in the privacy plan aligns with
498 the information provided in the PIA, PRA, and other applicable privacy documentation (e.g.,
499 SORN, MOU, other types of contracts or agreements).

500 **3.6. System Information Types and System Categorization**

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

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

511 **3.7. Authorization Boundary and System Environment**

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

515 The system plan can summarize key aspects of the system architecture, including the use of
516 subsystems and external service providers; physical or logical separations; local and remote
517 management functionalities; customized or specialized components, functions, or data flows;
518 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

553   • The flow of information that results from information exchanges with external
554   organization systems

3.7.2. System Component Inventory

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

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

562   • Hardware component description, function, role, and deployment date

563   o Unique component identifier (e.g., serial number, asset tracking identifier, other
564   service codes that identify supply chain information)

565   o Manufacturer and model, including sub-model identifiers or distinctions (e.g.,
566   subcomponent country of origin)

567   o Warranty duration, expiration date, and/or maintenance support contract status

568   o Specific physical locations (e.g., a rack in a server room)

569   • Software product version, revision number, or build information

570   o Software developer, manufacturer, and vendor, including for subcomponents

571   o Secure software development attestation[11]

572   o Product license type (e.g., single user, volume license, public license, freeware)

573   o Software warranty and maintenance support contract status

574   o Product license expiration date

575   System personnel maintain the system component inventory that is included or referenced in
576   the system plan. The physical inventory is often distinct from the system component inventory
577   and is handled through procurement and property management procedures. For instance, the
578   system component inventory accounts for hardware as well as instances of virtualized
579   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.

580   **3.8. Control Implementation Details**

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

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

596   Additional information supporting control implementation includes:

597   •   Control implementation status (e.g., planning, planned/implementation incomplete,
598   implemented as planned, implemented/tailored)

599   •   Planned inputs, related data sources, and expected system outputs for controls that are
600   implemented in the hardware, software, or firmware components of the system

601   •   Special considerations for data processing and distribution

602   •   Summary of tailoring activities and resulting tailoring decisions

603   •   Location of related policy and procedure artifacts

604   •   Components, products, or services associated with the control

605   •   Roles or specific entities that are responsible for control implementation, including
606   information about shared responsibilities for hybrid controls

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

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

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

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

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

622   • **Scope and focus:** While the system security plan primarily addresses safeguarding the
623   system against unauthorized access and ensuring data confidentiality, integrity, and
624   availability, the system privacy plan focuses on the broader implications of data
625   processing. This includes considerations such as the context of data use, the potential
626   impact on individuals, and adherence to privacy principles like transparency, data
627   minimization, and purpose specification.

628   • **Privacy-specific risks:** The system privacy plan addresses privacy-specific risks that might
629   arise, even from authorized data processing activities. For example, privacy controls
630   might include measures to minimize data collection to only what is necessary, restrict
631   data sharing with third parties, or implement mechanisms that allow individuals to
632   exercise their rights over their personal data.

633   • **Individual autonomy and transparency:** Privacy controls often emphasize giving
634   individuals control over their data (i.e., autonomy) and ensuring that individuals are
635   informed about how their data is processed (i.e., transparency). These aspects require
636   different control implementations compared to security controls, which are primarily
637   concerned with protecting systems and information rather than individuals.

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

645   **3.9. Information Exchanges**

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

648   Information exchanges are defined between systems that exchange data across authorization
649   boundaries, whether inside or outside the organization [SP800-47]. Such agreements may vary
650   based on the impact level of the information being exchanged, the relationship between the
651   organizations exchanging information, or the level of access granted to personnel from the
652   interconnected system.

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

- 655 • Type of agreement used for the information exchange (e.g., information exchange
  656 agreement, interconnection security agreement, memorandum of agreement,
  657 memorandum of understanding)

- 658 • Effective start and end dates of the agreement

- 659 • Systems participating in the agreement, including:

  - 660 o Name, role, title, and organization of the system owner and authorizing official

  - 661 o System name and unique system identifier assigned by the system owner's
    662 organization

  - 663 o FIPS 199 categorization of the system and the information being exchanged

  - 664 o System authorization decisions status

- 665 • Brief description of the exchange, including the purpose, type of data, and expected
  666 outputs

- 667 • Method of information exchange (e.g., virtual private network, extranet, dedicated data
  668 transfer application)

- 669 • Interface characteristics that explain how the information is being exchanged between
  670 the systems

- 671 • Diagrams that show the data flows, system components, and technologies involved

- 672 • Findings and mitigation strategies that are relevant to the components involved in the
  673 information exchange and may be identified in:

  - 674 o Security, privacy, or cybersecurity supply chain risk assessment reports;

  - 675 o Security and privacy control assessments; or

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

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

683 **3.10. Laws, Regulations, and Policies Affecting the System**

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

686 The system plan can identify the sources of specific requirements for the confidentiality,
687 integrity, or availability of the system; the predictability, manageability, and disassociability of
688 information processed, stored, or transmitted by the system; and the protection of the supply
689 chain. Organizational policies may identify the laws, regulations, and policies that are applicable
690 to all systems within the organization or include a standardized list of requirement sources in
691 an organizational template for system plans. As the legal and regulatory landscape evolves, the
692 system plans are updated to adapt to new security, privacy, and cybersecurity supply chain risk
693 management requirements, such as those that arise from the use of emerging technologies,
694 automated decision-making, and data analytics.

695 For example, privacy laws that govern data subject rights directly influence the development of
696 the system privacy plan, including how data is handled and how the system protects individual
697 rights, frames broader privacy risks, and addresses organizational privacy goals. The C-SCRM
698 plan identifies suppliers or products that are prohibited by law, organizational policy, or other
699 regulatory exclusions that define system-specific constraints.

700 **3.11. Digital Identity Acceptance Statement**

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

702 Organizational and system-level risk assessments determine the extent to which risk is
703 managed by various processes,[12] which in turn drive decisions regarding applicable
704 technologies and mitigation strategies. During the risk management process, the organization
705 determines the assurance levels for identity proofing, authentication, and federation, if
706 applicable; selects appropriate processes and technologies to meet each assurance level; and
707 identifies compensating controls when necessary.

708 **3.12. Referenced Artifacts**

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

711 Verify that the system artifacts referenced in control implementation details or other system
712 plan elements are available to authorized reviewers, such as organizational leadership, system
713 management, and control assessors. Example artifacts may include the authorization decision
714 artifact, contingency plan, configuration management plan, ISCM plan, incident response plan,
715 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.

716　**3.13. Acronym List and Glossary**

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

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

723 **4. System Plan Development and Maintenance**

724 The RMF provides a methodology for managing system risks using organizational policies and
725 system-level procedures to support system plan development, including responsibilities,
726 ongoing reviews and updates, the approval of system plans, and assessments of control
727 implementations. Fig. 2 shows the seven steps of the RMF. The following section identifies how
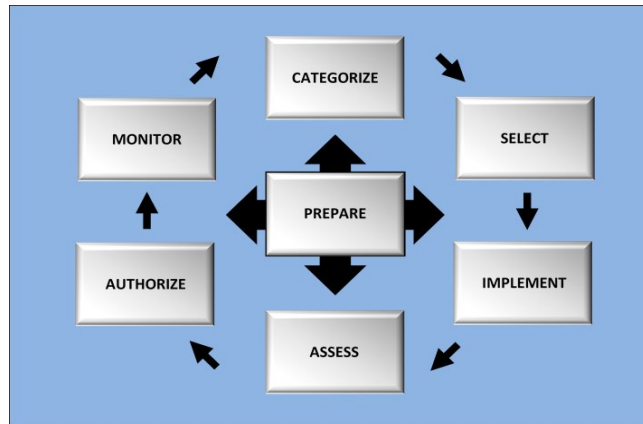728 systems plans are related to each step of the RMF.

729

730 **Fig. 2. NIST Risk Management Framework Steps**

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

733 **4.1. Prepare**

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

741 *Common control providers* develop system plan artifacts that identify and provide
742 implementation details for inheritable common controls. A common control plan describes
743 privacy protections, such as data minimization, transparency, and consent management. It may
744 also identify systems outside of the authorization boundary as a common control provider from
745 which implemented controls are inherited. Inherent relationships with common control
746 providers may be based on specific operational relationships with service providers in the
747 supply chain.

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

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

753 • Additional controls, control enhancements, and compensating controls to address
754 organization-specific risks

755 • Supplemental scoping guidance to explain the applicability of the tailored controls to
756 specialized system, system element, or component operations based on security and
757 privacy assumptions

Prepare — System Level

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

761 • The mission or business focus supported by the system

762 • System stakeholders

763 • The information types handled by system

764 • Unique security and privacy risks in the information life cycle that are managed across
765 the entire data ecosystem

766 • How the authorization boundary is defined within the organizational infrastructure or
767 enterprise architecture

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

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

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

Defining the Authorization Boundary

781 The system plans identify how data flows through various subsystems, third-party services, and
782 external networks to ensure that privacy risks are managed comprehensively. The authorization
783 boundary establishes the scope of protection for the system based on mission, management, or
784 budgetary responsibilities. Privacy risks can arise at any stage of data processing because of the

785 interconnected nature of modern systems, and identifying and responding to them may require
786 looking beyond the authorization boundary.

787 System-specific C-SCRM concerns may include risks derived from suppliers that are several
788 layers removed from the end user or supply chain risks associated with specific organization-
789 defined technologies. For example, C-SCRM considers the complexities of new technologies and
790 dynamic system interdependencies that can result in suppliers gaining incidental access[13] to
791 data. C-SCRM plan considerations include vendor-controlled SaaS offerings, hybrid or cloud
792 environments, open-source software, information and communications technology and
793 operational technology from suppliers outside of Trade Agreements Act nations, and general
794 procurement from unauthorized resellers.

4.2. Categorize

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

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

807 The C-SCRM plan is generally developed for high- and moderate-impact systems, as indicated in
808 [SP800-161]. However, there is value in developing the C-SCRM plan to protect low-impact
809 systems as well, particularly if the low-impact system uses the same components found in high-
810 and moderate-impact systems. In the absence of a C-SCRM plan for a low-impact system, the
811 system security plan can identify the inheritance of C-SCRM controls from organization-level
812 common control providers, enumerate organizational and system risk tolerances, and
813 demonstrate the acceptance versus the transfer or mitigation of cybersecurity supply chain
814 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.

815   **4.3. Select**

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

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

823   • **Baseline control selection:** Controls in the organizationally tailored control baselines
824   that were determined during the RMF *Prepare* step are factored into the control
825   selection process.

826   o The initial security baselines in [SP800-53B] group controls that are designed to
827   support the [FIPS200] minimum security requirements for systems based on the
828   [FIPS199] security impact level.

829   o The initial privacy baseline in [SP800-53B] identifies controls for federal agencies
830   to address privacy requirements and manage privacy risks that arise from
831   processing data about individuals based on privacy program responsibilities
832   under [OMBA-130].[14] These controls are rooted in privacy engineering objectives
833   and are designed to respond to privacy risks with effective data protection
834   strategies. System privacy and security officials collaborate on the selection of
835   privacy controls to ensure that both privacy and security risks are managed,
836   particularly in areas where the risks overlap.

837   o Organizations can use a control overlay (e.g., C-SCRM extended overlay[15]) as a
838   starting point for selecting controls with broad-based support across
839   communities of interest for specific circumstances, situations, and/or conditions.

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

843   **4.3.1. Control Tailoring**

844   The control tailoring activities in [SP800-53B] provide flexibility for aligning the allocated
845   controls with system-specific needs, such as addressing organizational policies or specific use
846   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.

847 with poor quality or counterfeit products, supplier misuse of intellectual property, supplier
848 tampering with or compromise of mission-critical information, and exposure to cyber attacks
849 through vulnerable supplier systems.

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

851 • Common controls that are inherited by the system from common control providers;

852 • Scoping considerations for selected controls;

853 • Compensating controls that are selected and allocated;

854 • ODP values for control assignment and selection operations;

855 • Additional controls that supplement the baseline, such as controls based on
856 Cybersecurity and Privacy Framework Profiles;[16]

857 • Additional specification information for control implementation; and

858 • Controls that are tailored out of the selected control baseline.

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

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

870 **4.3.2. Identification of Planned Control Implementations**

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

877 For fully inherited or hybrid controls, system plans reference the source of the common control
878 to avoid duplicating the common control implementation details.[17] Notes may be added to the
879 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.

880 Control implementation details in the system privacy plan describe how the controls meet
881 privacy-specific requirements, such as those that address risks related to the processing of
882 personal information, the context of data use, and potential consequences for individuals.

883 ### 4.3.3. Plan Review and Approval

884 The senior agency official for privacy is responsible for reviewing and approving the system
885 privacy plan or consolidated plan before it is submitted to the authorizing official or designated
886 representative (see Sec. 3.4). This review ensures that privacy risks have been thoroughly
887 identified and that privacy controls and risk management strategies are aligned with
888 organizational policies, legal requirements, and privacy objectives. When reviewing the system-
889 specific C-SCRM plan in the authorization package, authorizing officials consult with the C-SCRM
890 PMO as well as acquisitions personnel in cases of technology procurements. The C-SCRM
891 review ensures that the C-SCRM controls and risk management strategies align with the overall
892 organizational risk tolerances.

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

896 • If the system plans are acceptable, the authorizing official or designated representative
897   approves the system plans, enabling the system owner to begin execution of the RMF
898   *Implement* step.

899 • If the system plans are unacceptable, the authorizing official or designated
900   representative may recommend changes for the system owner or common control
901   provider to implement.

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

905 ## 4.4. Implement

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

910 ## 4.5. Assess

911 Control assessments are based on the information in system plans to prepare for, create, and
912 execute the assessment plan [SP800-53A]. The subsequent report identifies whether the
913 controls in the assessment scope are implemented correctly, operating as intended, and
914 producing the desired outcome with respect to meeting the system's security, privacy, and
915 supply chain risk management requirements. Personnel update the system plans based on

916 remediation actions that are taken to resolve control deficiencies reported during the
917 assessment. At the conclusion of the control assessment, system plans provide a "point-in-
918 time" understanding of the system's operation and the implemented controls that support the
919 RMF *Authorize* step.[18]

4.6. Authorize

921 The system owner or common control provider assembles and submits an authorization
922 package to the authorizing official for an authorization decision. The authorization package
923 includes the system security and system privacy plans and any referenced artifacts. The C-SCRM
924 plan is not required but may be included.

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

929 • Authorize a system to operate or be used within the organization,

930 • Issue a *common control authorization*, or

931 • Deny authorization to the system or common control provider to protect the
932 organization from risks that are outside of established organizational risk tolerances.

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

4.7. Monitor

937 System plans are reviewed and revised on an organization-defined schedule[19] to ensure their
938 continued accuracy and relevancy after authorization. Reviews may also occur in response to
939 events that affect security, privacy, or C-SCRM risks, such as:

940 • Revisions to the [SP800-53] security and privacy control catalog, [SP800-53B] control
941 baselines, or [SP800-53A] assessment procedures

942 • New or revised laws, regulations, and organizational policies that affect security,
943 privacy, or SCRM requirements

944 • Updates to the system risk assessment report that identify new risks that render existing
945 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.

946   • Weaknesses identified during control assessments and monitoring or after a security,
947   privacy, or supply chain cybersecurity incident or compromise (e.g., system data breach)

948   • Changes that significantly alter the risk posture of the system and justify control
949   reassessment and system reauthorization (e.g., revisions to the information types or
950   special factors that affect system categorization, the selection and implementation of
951   additional controls, additional tailoring activities that align control implementations with
952   identified risks)

953   • Changes to key system personnel (e.g., if the authorizing official changes, the incoming
954   authorizing official reviews the system plans and artifacts to confirm the existing
955   authorization or issue a new authorization decision)

956   • Changes to the operational status of the system (e.g., promoting the system from
957   "in development" to "operational," system disposal)

958   • Renewal of or modifications to existing agreements for information exchanges, the
959   creation of new information exchanges, or the termination of information exchanges
960   [SP800-47]

961   • Changes to the organizational baseline supply chain risk strategy or inherited C-SCRM
962   controls due to:

963   o Changes in critical suppliers that potentially affect supply chain risks, including
964   ownership changes, mergers and acquisitions activity, and geopolitical or
965   environmental activity

966   o Reviews of suppliers' foreign ownership, control, or influence (FOCI)

967   o Cybersecurity attacks or data breaches that affect a supplier's ability to support
968   confidentiality, integrity, or availability objectives

969 Change management processes ensure that updates to system plans are tracked and noted,
970 including revision or version identifiers to maintain a record of changes as well as specific
971 procedures for tracking and managing modifications in the system configuration management
972 plan. Automating information collection methods (see Sec. 4.8) can result in more efficient and
973 effective system plan maintenance.

Reauthorization or Ongoing Authorization

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

980 For example, the system privacy plan can define privacy metrics (e.g., access requests from
981 individuals, data sharing frequency, incidents) that are regularly analyzed during monitoring
982 activities to track trends and risks. The system privacy officer is responsible for identifying
983 assessment methodologies and metrics to determine whether privacy controls are

984 implemented correctly, operating as intended, and complying with applicable privacy
985 requirements. Appropriate updates to privacy controls and the system privacy plan can
986 strengthen protections.

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

991 **Disposal of System Components**

992 System components and information assets may be disposed of at any time during the system
993 life cycle, which may introduce opportunities to compromise both physical and logical data.
994 System plans include instructions for properly disposing of systems or components (e.g.,
995 sanitization of storage media), the date of system disposal, and records of information assets
996 that are transferred to other systems. The disposal strategy may also be integrated into the
997 control implementation details. Updates to the system component inventory may trigger
998 additional updates to the system plans to reflect changes in the environment of operations.

999 Additionally, the roles and responsibilities of all parties are clearly defined and communicated,
1000 including policies and procedures for responding to data exposure incidents that may occur
1001 during or after the disposal process. Decisions regarding the retention, transfer, or deletion of
1002 data are made by the system owner, information owner, authorizing official, and/or senior
1003 organization official for privacy in compliance with applicable data and records retention
1004 requirements, such as those provided by the National Archives and Records Administration
1005 [NARARECM].

1006 Key considerations for the removal of a system or system elements from operation include the
1007 responsibilities of the system owner for protecting system data, the responsibility of the
1008 authorizing official for risks associated with data remanence,[20] and the organizational liability
1009 for inadequate data sanitization. Demonstrating due diligence can address the legal and
1010 financial liabilities of data breaches caused by inadequate sanitization, unauthorized access to
1011 residual data, or the improper transfer of data to another system.

1012 **4.8. Automation Support**

1013 Maximizing the use of automation, wherever possible, can increase the effectiveness and
1014 efficiency of maintaining system plans throughout the system life cycle. Organizations have the
1015 flexibility to decide when, where, and how to use automation or automated support tools for
1016 plan development and monitoring.[21] Smaller organizations (e.g., micro government agencies,
1017 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).

1018 individual system plans that can be stored in an organization-wide repository. Larger
1019 organizations that operate more systems may benefit from an organization-wide information
1020 management tool (e.g., GRC tool) with a centralized data repository to consolidate and
1021 correlate system plan information across the organization.

1022 **NIST does not recommend, endorse, or certify specific products, vendors, or technologies for**
1023 **the automation of system plan development and maintenance.**

4.8.1. Collection

1025 Information is collected from both organization-wide and system-specific data sources,
1026 including:

1027 • System component inventory information (e.g., technology, function, role, and
1028 configuration of components used within the operational environment[22])

1029 • Personnel contact information from an organizational directory

1030 • Information types that are detected within the system but are excluded from system
1031 categorization determination

1032 • Changes to common controls and the inherited portion of hybrid controls

1033 • Changes to system plan information to enforce separation of duties

1034 • New, in-process, and resolved POA&Ms

1035 This data informs various management activities, such as prioritizing security, privacy, or SCRM
1036 initiatives and allocating resource based on impact priorities. Automating the collection of
1037 system-level risk information in a centralized repository following organization-defined data
1038 standards can reduce inconsistencies.

4.8.2. Protection

1040 Organizations determine the level of protection required for system plan information based on
1041 the system's information types [SP800-60v2] and organizational requirements. Access control
1042 policies in an organization-wide information management tool can:

1043 • Control the visibility of system plan data to specific access holders based on their roles

1044 • Ensure that only authorized users can update system information, review change
1045 records, and approve changes that have been made

1046 Additional access controls can be applied to prevent unauthorized access to the system's
1047 weakness and vulnerability information. Organization- and system-specific policies may further
1048 control access to technical details about the system, such as IP addresses, vulnerability
1049 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.

1050 **4.8.3. Sharing and Usability**

1051 Maintaining system plan information in a central repository can improve the responsiveness of
1052 risk-based decision-making by senior officials and system risk managers. Authorizing officials
1053 and system owners review and update system information as needed (e.g., using automated
1054 information collection) to support continuous monitoring activities, ongoing assessments, and
1055 authorization processes. System management personnel track approval processes for change
1056 management functions and review control implementation metrics.

1057 The dashboard interfaces and reporting functions of organization-wide information
1058 management tools can ensure that authorized personnel receive updates on system
1059 component inventory information and the status of risk management efforts, including the
1060 system's operational status, assessment and authorization schedules, POA&M status (e.g., late
1061 POA&Ms, expiring POA&Ms), and accepted risk information.

1062 The information management tool can also share control status and implementation
1063 information with internal and external interconnected systems, systems that inherit common
1064 and hybrid controls, external organizations, and system owners with authorized visibility.
1065 Compensating controls can be applied at the system level and included in the system plans to
1066 account for unresolved POA&Ms and inherited risks in the common control implementations
1067 and to maintain the necessary levels of protection to safeguard system assets and information.

1068 Information that is relevant to the preparation, planning, and execution of control assessments
1069 can be restricted to prevent the inadvertent release of system information by third-party
1070 assessors. Assessors may be given limited access to input assessment results and artifacts
1071 directly into the information management tool to generate assessment reports.

1072 **4.8.4. Management**

1073 Automation also facilitates system plan management, including:

1074 • Tracking changes to system plan elements, including the control implementations,
1075   agreements for information exchanges, POA&Ms, and supporting roles

1076 • Alerting organizational leaders and system management of changes or inconsistencies in
1077   the collected system plan information

1078 • Generating system plans using organization-approved templates to minimize the
1079   duplication of element-specific content (e.g., system description, system environment,
1080   identification of roles related to risk management or system operations)

1081 Automation can be particularly useful in assessing and continuously monitoring controls
1082 throughout the system life cycle. Storing system plan data in machine-readable formats can
1083 facilitate updates to control implementation details due to assessment results, control catalog
1084 or baseline updates, and other system changes. For example, POA&Ms for *other than satisfied*
1085 findings in a machine-readable assessment report can trigger updates to system plans and
1086 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

1128		STANDARDS, GUIDELINES, AND REPORTS
1129	[FIPS199]	National Institute of Standards and Technology (2004) Standards for Security
1130		Categorization of Federal Information and Information Systems. (U.S.
1131		Department of Commerce, Washington, DC), Federal Information Processing
1132		Standards Publication (FIPS) NIST FIPS 199.
1133		https://doi.org/10.6028/NIST.FIPS.199
1134	[FIPS200]	National Institute of Standards and Technology (2006) Minimum Security
1135		Requirements for Federal Information and Information Systems. (U.S.
1136		Department of Commerce, Washington, DC), Federal Information Processing
1137		Standards Publication (FIPS) NIST FIPS 200.
1138		https://doi.org/10.6028/NIST.FIPS.200
1139	[IR8062]	An Introduction to Privacy Engineering and Risk Management in Federal
1140		Systems (2017) (National Institute of Standards and Technology,
1141		Gaithersburg, MD), NIST Interagency/Internal reports (IR) NIST IR 8062.
1142		https://doi.org/10.6028/NIST.IR.8062
1143	[NISTCSF]	National Institute of Standards and Technology Framework for Improving
1144		Critical Infrastructure Cybersecurity (Cybersecurity Framework), Version 2.0.
1145		(February 2024) (National Institute of Standards and Technology,
1146		Gaithersburg, MD), NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29
1147	[NISTPF]	NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise
1148		Risk Management (2020) (National Institute of Standards and Technology,
1149		Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020
1150	[NTIASBOM]	The Minimum Elements For a Software Bill of Materials (SBOM) (2021) NTIA
1151		and Department of Commerce. Available at
1152		https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements
1153		_report.pdf
1154	[SP800-30]	Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk
1155		Assessments. (National Institute of Standards and Technology, Gaithersburg,
1156		MD), NIST Special Publication (SP) NIST SP 800-30r1.
1157		https://doi.org/10.6028/NIST.SP.800-30r1
1158	[SP800-37]	Joint Task Force (2018) Risk Management Framework for Information
1159		Systems and Organizations: A System Life Cycle Approach for Security and
1160		Privacy. (National Institute of Standards and Technology, Gaithersburg, MD),
1161		NIST Special Publication (SP) NIST SP 800-37r2.
1162		https://doi.org/10.6028/NIST.SP.800-37r2
1163	[SP800-39]	Joint Task Force Transformation Initiative (2011) Managing Information
1164		Security Risk: Organization, Mission, and Information System View. (National
1165		Institute of Standards and Technology, Gaithersburg, MD), NIST Special
1166		Publication (SP) NIST SP 800-39. https://doi.org/10.6028/NIST.SP.800-39
1167	[SP800-47]	Dempsey KL, Pillitteri VY, Regenscheid A (2021) Managing the Security of
1168		Information Exchanges. (National Institute of Standards and Technology,
1169		Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-47r1.
1170		https://doi.org/10.6028/NIST.SP.800-47r1

1171	[SP800-53]	Joint Task Force (2020) Security and Privacy Controls for Information Systems
1172		and Organizations. (National Institute of Standards and Technology,
1173		Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53r5. Includes
1174		updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5
1175	[SP800-53A]	Joint Task Force Transformation Initiative (2022) Assessing Security and
1176		Privacy Controls in Information Systems and Organizations. (National
1177		Institute of Standards and Technology, Gaithersburg, MD), NIST Special
1178		Publication (SP) NIST SP 800-53Ar5.
1179		https://doi.org/10.6028/NIST.SP.800-53Ar5
1180	[SP800-53B]	Joint Task Force (2020) Control Baselines for Systems and Organizations.
1181		(National Institute of Standards and Technology, Gaithersburg, MD), NIST
1182		Special Publication (SP) NIST SP 800-53B. Includes updates as of December
1183		10, 2020. https://doi.org/10.6028/NIST.SP.800-53B
1184	[SP800-60v1]	Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping
1185		Types of Information and Information Systems to Security Categories.
1186		(National Institute of Standards and Technology, Gaithersburg, MD), NIST
1187		Special Publication (SP) NIST SP 800-60v1r1.
1188		https://doi.org/10.6028/NIST.SP.800-60v1r1
1189	[SP800-60v2]	Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping
1190		Types of Information and Information Systems to Security Categories:
1191		Appendices. (National Institute of Standards and Technology, Gaithersburg,
1192		MD), NIST Special Publication (SP) NIST SP 800-60v2r1.
1193		https://doi.org/10.6028/NIST.SP.800-60v2r1
1194	[SP800-63-3]	Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National
1195		Institute of Standards and Technology, Gaithersburg, MD), NIST Special
1196		Publication (SP) NIST SP 800-63-3. Includes updates as of March 2, 2020.
1197		https://doi.org/10.6028/NIST.SP.800-63-3
1198	[SP800-88]	Kissel R, Regenscheid A, Scholl M (2014) Guidelines for Media Sanitization
1199		(National Institute of Standards and Technology, Gaithersburg, MD), NIST
1200		Special Publication (SP) NIST SP 800-88r1.
1201		https://doi.org/10.6028/NIST.SP.800-88r1
1202	[SP800-137]	Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD,
1203		Scholl MA, Stine KM (2011) Information Security Continuous Monitoring
1204		(ISCM) for Federal Information Systems and Organizations. (National Institute
1205		of Standards and Technology, Gaithersburg, MD), NIST Special Publication
1206		(SP) NIST SP 800-137. https://doi.org/10.6028/NIST.SP.800-137
1207	[SP800-161]	Boyens JM, Smith A, Bartol N (2022) Cybersecurity Supply Chain Risk
1208		Management Practices for Systems and Organizations. (National Institute of
1209		Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
1210		NIST SP 800-161r1. Includes updates as of November 1, 2024.
1211		https://doi.org/10.6028/NIST.SP.800-161r1-upd1

1212	[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
1216	[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
1220	[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
1225	[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
1229	[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
1233	[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
1238		MISCELLANEOUS PUBLICATIONS AND RESOURCES
1239	[CPRT]	National Institute of Standards and Technology (2025), *NIST Cybersecurity and Privacy Reference Tool* (CPRT). Available at https://csrc.nist.gov/projects/cprt
1242	[CSRC]	National Institute of Standards and Technology (2025), *NIST Computer Security Resource Center* (CSRC). Available at https://csrc.nist.gov
1244	[NARACUI]	National Archives and Records Administration, Controlled Unclassified Information (CUI) Registry. Available at https://www.archives.gov/cui
1246	[NARARECM]	National Archives and Records Administration, NARA Records Management Guidance and Regulations. Available at https://www.archives.gov/records-mgmt/policy
1249	[OSCAL]	National Institute of Standards and Technology (2025), *Open Security Controls Assessment Language* (OSCAL). Available at https://nist.gov/oscal
1251	[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

1255	[SCOR]	National Institute of Standards and Technology (2025), *NIST Security and*
1256		*Privacy Control Overlay Repository* (SCOR). Available at
1257		https://csrc.nist.gov/projects/risk-management/sp800-53-controls/overlay-
1258		repository
1259	[ZTDATASEC]	Zero Trust Data Security Guide, October 2024. Available at
1260		https://www.cio.gov/zero-trust-data-security-guide-oct2024
1261		

1262 Appendix A. RMF Task Outputs Related to System Plan Elements

1263 The tasks indicated in Table 1 either explicitly identify the system and privacy plan as expected outputs or identify expected outputs
1264 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
1265 the [CPRT] reference dataset for SP 800-37.

1266 **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

1268 **Appendix B. List of Abbreviations and Acronyms**

1269 **C-SCRM**
1270 Cybersecurity Supply Chain Risk Management

1271 **CIO**
1272 Chief Information Officer

1273 **CPRT**
1274 Cybersecurity and Privacy Reference Tool

1275 **CUI**
1276 Controlled Unclassified Information

1277 **DevSecOps**
1278 Development, Security, and Operations

1279 **FIPS**
1280 Federal Information Processing Standards

1281 **FISMA**
1282 Federal Information Security Modernization Act

1283 **FOCI**
1284 Foreign Ownership, Control, or Influence

1285 **GRC**
1286 Governance, Risk, and Compliance

1287 **IR**
1288 Internal Report or Interagency Report

1289 **ISCM**
1290 Information Security Continuous Monitoring

1291 **MOU**
1292 Memorandum of Understanding

1293 **NARA**
1294 National Archives and Records Administration

1295 **OMB**
1296 Office of Management and Budget

1297 **OSCAL**
1298 Open Security Controls Assessment Language

1299 **PIA**
1300 Privacy Impact Assessment

1301 **PMO**
1302 Program Management Office

1303 **PRA**
1304 Privacy Risk Assessment

1305 **PRAM**
1306 Privacy Risk Assessment Methodology

1307 **RMF**
1308 Risk Management Framework

1309 **SCRM**
1310 Supply Chain Risk Management

1311 **SecCM**
1312 Security-focused Configuration Management

1313 **SORN**
1314 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.

1358 **privacy program plan**
1359 A formal document that provides an overview of an agency's privacy program, including a description of the
1360 structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency
1361 Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program,
1362 and the program management controls and common controls in place or planned for meeting applicable privacy
1363 requirements and managing privacy risks. [SP800-37] from [OMBA-130]

1364   See also *information security program plan*.

1365 **privacy requirements**
1366 A requirement that applies to an information system or an organization that is derived from applicable laws,
1367 executive orders, directives, policies, standards, regulations, procedures, and/or mission/business needs with
1368 respect to privacy. [SP800-37]

1369   *Note*: The term "privacy requirement" can be used in a variety of contexts, from high-level policy activities
1370   to low-level implementation activities in system development and engineering disciplines.

1371 **privacy risk**
1372 The likelihood that individuals will experience problems resulting from data processing, and the impact should they
1373 occur. [NISTPF]

1374 **privacy risk management**
1375 A cross-organizational set of processes for identifying, assessing, and responding to privacy risks. [NISTPF]

1376 **risk management**
1377 The program and supporting processes to manage risk to agency operations (including mission, functions, image,
1378 reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context
1379 for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.
1380 [OMBA-130]

1381 **security**
1382 A condition that results from the establishment and maintenance of protective measures that enable an
1383 organization to perform its mission or critical functions despite risks posed by threats to its use of systems.
1384 Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and
1385 correction that should form part of the organization's risk management approach. [SP800-37]

1386 **security plan**
1387 A formal document that provides an overview of the security requirements for an information system or an
1388 information security program and describes the security controls in place or planned for meeting those
1389 requirements. The system security plan describes the system components that are included within the system, the
1390 environment in which the system operates, how the security requirements are implemented, and the relationships
1391 with or connections to other systems. [SP800-53]

1392   *Note*: The security plan and the privacy plan may be integrated into one consolidated system artifact.

1393 **supply chain**
1394 Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of
1395 products and services and extends through the design, development, manufacturing, processing, handling, and
1396 delivery of products and services to the acquirer. [OMBA-130]

1397 **supply chain risk**
1398 Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and
1399 reflect the potential adverse impacts to organizational operations (including mission, functions, image, or
1400 reputation), organizational assets, individuals, other organizations, and the Nation. [OMBA-130]

1401 **supply chain risk information**
1402 Includes, but is not limited to, information that describes or identifies: (1) Functionality of covered articles,
1403 including access to data and information system privileges; (2) Information on the user environment where a
1404 covered article is used or installed; (3) The ability of the source to produce and deliver covered articles as expected
1405 (i.e., supply chain assurance); (4) Foreign control of, or influence over, the source (e.g., foreign ownership,
1406 personal and professional ties between the source and any foreign entity, legal regime of any foreign country in
1407 which the source is headquartered or conducts operations); (5) Implications to national security, homeland
1408 security, and/or national critical functions associated with use of the covered source; (6) Vulnerability of federal
1409 systems, programs, or facilities; (7) Market alternatives to the covered source; (8) Potential impact or harm caused
1410 by the possible loss, damage, or compromise of a product, material, or service to an organization's operations or
1411 mission; (9) Likelihood of a potential impact or harm, or the exploitability of a system; (10) Security, authenticity,
1412 and integrity of covered articles and their supply and compilation chain; (11) Capacity to mitigate risks identified;
1413 (12) Credibility of and confidence in other supply chain risk information; (13) Any other information that would
1414 factor into an analysis of the security, integrity, resilience, quality, trustworthiness, or authenticity of covered
1415 articles or sources; (14) A summary of the above information and, any other information determined to be
1416 relevant to the determination of supply chain risk. [FASCSA]

1417 **supply chain risk management**
1418 The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of
1419 information and communications technology product and service supply chains. [OMBA-130]

1420   See also *cybersecurity supply chain risk management*.

1421 **system-related privacy risk**
1422 Risk to an individual or individuals associated with the agency's creation, collection, use, processing, storage,
1423 maintenance, dissemination, disclosure, and disposal of their PII. [OMBA-130]

1424 **system-related security risk**
1425 Risk that arises through the loss of confidentiality, integrity, or availability of information or systems and that
1426 considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other
1427 organizations, and the Nation. [SP800-30]

1428 **systems privacy engineering**
1429 Process that captures and refines privacy requirements and ensures their integration into information technology
1430 component products and information systems through purposeful privacy design or configuration. [SP800-37]

1431 A specialty engineering discipline of systems engineering. It applies scientific, mathematical, engineering, and
1432 measurement concepts, principles, and methods to deliver, consistent with defined constraints and necessary
1433 trade-offs, a trustworthy asset protection capability that satisfies stakeholder requirements; is seamlessly
1434 integrated into the delivered system; and presents residual risk that is deemed acceptable and manageable to
1435 stakeholders. [OMBA-130]

1436 **Appendix D. Change Log**

1437 Draft NIST Special Publication (SP) 800-18r2 (Revision 2), *Developing Security, Privacy, and*
1438 *Supply Chain Risk Management Plans for Systems*, provides guidelines for developing and
1439 maintaining system security plans, system privacy plans, and C-SCRM plans.

1440 • Section 2 defines and explains the system plan types based on the RMF [SP800-37],
1441 [SP800-161], and the NIST Privacy Framework.

1442 • Section 3 updates the suggested elements for system security, privacy, C-SCRM plans
1443 and addresses the relationship between security risk management and privacy risk
1444 management.

1445 • Section 4 relates the development and maintenance of system security, privacy, and
1446 C-SCRM plans to the implementation of the RMF. Material has been added to address
1447 the use of information management tools and automation to support the development,
1448 management, maintenance, and protection of system plan information.

1449 In addition, the publication has been restructured, and the following content changes have
1450 been applied:

1451 • Technical content from other NIST publications is now included by reference rather than
1452 repeated.

1453 • The terms *general support system*, *major application*, and *minor application* have been
1454 deprecated to be consistent with OMB Circular A-130 (July 2016) [OMBA-130].

1455 • The term *system boundary* has been updated to *authorization boundary* for consistency
1456 with the terminology in [SP800-37].