

NIST Special Publication 800
NIST SP 800-100r1 ipd

Information Security Handbook

A Guide for Executive Leadership

Initial Public Draft

Isabel Van Wyk
Jeff Brewer
Jeffrey Marron
Jeremy Licata

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800.100r1.ipd>

NIST Special Publication 800
NIST SP 800-100r1 ipd

Information Security Handbook

A Guide for Executive Leadership

Initial Public Draft

Isabel Van Wyk

Jeff Brewer

Jeremy Licata

Computer Security Division

Information Technology Laboratory

Jeffrey Marron

Applied Cybersecurity Division

Information Technology Laboratory

This publication is available free of charge from:

<https://doi.org/10.6028/NIST.SP.800.100r1.ipd>

October 2026



U.S. Department of Commerce

Howard Lutnick, Secretary

National Institute of Standards and Technology

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

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at <https://csrc.nist.gov/publications>.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

[Copyright, Use, and Licensing Statements](#)

[NIST Technical Series Publication Identifier Syntax](#)

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]

Supersedes NIST Series XXX (Month Year) DOI [Will be added to final publication, if applicable.]

How to Cite this NIST Technical Series Publication

Van Wyk I, Brewer J, Marron J, Licata J (2026) Information Security Handbook: A Guide for Executive Leadership. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-100r1 ipd. <https://doi.org/10.6028/NIST.SP.800.100r1.ipd>

Author ORCID iDs

Isabel Van Wyk: 0000-0001-8566-6829

Jeff Brewer: 0009-0009-2159-3558

Jeffrey Marron: 0000-0002-7871-683X

Jeremy Licata: 0000-0001-8793-5471

Public Comment Period

October 21, 2026 – December 4, 2026

Submit Comments

sp800-100-comments@nist.gov

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

Additional Information

Additional information about this publication is available at <https://csrc.nist.gov/pubs/sp/800/100/r1/ipd>, including related content, potential updates, and document history.

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

1 **Abstract**

2 This document is a high-level guide to help executive leadership in both the public and private
3 sector understand key cybersecurity topics, including governance, risk management,
4 information exchange, security awareness and training, contingency planning, configuration
5 management, and incident response. It follows the general organization of the NIST
6 Cybersecurity Framework to emphasize the relationships between these core concepts and
7 points to other NIST publications for more detailed information and implementation guidance.

8 **Keywords**

9 Cybersecurity; cybersecurity supply chain risk management (C-SCRM); governance; NIST
10 Cybersecurity Framework (CSF); risk management.

11 **Reports on Computer Systems Technology**

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

Audience

This revision of SP 800-100 is intended for those who manage, support, and oversee information security and risk management but do not necessarily have technical responsibilities. This includes:

- Senior leadership and executives, such as Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs)
- Program managers
- Information system owners
- Other managers with security responsibilities but limited technical expertise

Readers are encouraged to reference the cited NIST publications for further detail and technical implementation guidelines.

Note to Reviewers

This revision of SP 800-100 substantially restructures the original document to provide high-level summaries on a variety of cybersecurity topics and new NIST frameworks. The previous version of this document was released in 2006 — two decades ago. Since that time, there have been dramatic changes in the regulatory environment, technological and cybersecurity landscape, and NIST's own body of guidance, including the introduction of the Cybersecurity Framework (CSF), the Risk Management Framework (RMF), and major updates to core publications (e.g., SP 800-53). As a result, the 2006 version of this document has become increasingly out of step with current practice, terminology, and best practices. This revision addresses that gap by realigning SP 800-100 with NIST's current frameworks and incorporating the many new concepts, processes, and roles that have emerged in cybersecurity since 2006.

NIST invites public feedback to maximize the document's effectiveness, relevance, and usability in helping executives understand key cybersecurity topics. To help guide this input, NIST has included specific questions below, though reviewers are welcomed to address additional topics in their comments. As you read this revision, please consider the following:

- What level of detail would be most appropriate for the intended audience throughout this publication? How might the current draft meet that level of detail?
- What topics should we add, remove, or revise to make the content more relevant for users?
- What additional references should be cited?
- How does the updated risk management section align with how your organization currently implements the RMF?
- Sec. 7 combines the CSF's Detect, Respond, and Recover Functions to discuss concepts that fall under all three. What topics, if any, are missing or misplaced?

Call for Patent Claims

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

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

- a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or
- b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:
 - i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
 - ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

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

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

Such statements should be addressed to: sp800-100-comments@nist.gov

85	Table of Contents	
86	1. Introduction	1
87	1.1. Purpose	1
88	1.2. Roles and Responsibilities	1
89	1.3. Document Organization	3
90	2. NIST Frameworks	4
91	2.1. Risk Management Framework (RMF)	4
92	2.2. Cybersecurity Framework (CSF 2.0)	6
93	2.3. NICE Framework	6
94	2.4. Privacy Framework	7
95	2.5. Secure Software Development Framework (SSDF)	8
96	2.6. Artificial Intelligence Risk Management Framework (AI RMF)	8
97	2.7. Cybersecurity Supply Chain Risk Management (C-SCRM)	9
98	2.8. Relationships Between Key NIST Frameworks	10
99	3. Governance	11
100	3.1. Risk Management Fundamentals	11
101	3.1.1. Enterprise Risk Management (ERM)	12
102	3.2. Establishing Cybersecurity Governance Roles and Responsibilities	14
103	3.3. Establishing and Updating Organizational Cybersecurity Governance Policy	15
104	3.4. Federal Governance Requirements	16
105	4. Identify	17
106	4.1. Asset Management	17
107	4.2. Risk Assessment	17
108	4.3. Information Exchange	18
109	4.4. Measurement and Metrics	18
110	5. Protect	20
111	5.1. Zero Trust Architecture	20
112	5.2. Awareness and Training	21
113	5.3. IT Contingency Planning	22
114	5.4. Configuration Management	23
115	6. Continuous Monitoring	25
116	6.1. ISCM Strategy	25
117	6.2. ISCM Roles and Responsibilities	26
118	7. Detect, Respond, and Recover	27
119	7.1. Incident Response Life Cycle Model	27

120	7.2. Incident Response Plan	28
121	References.....	30
122	Appendix A. List of Symbols, Abbreviations, and Acronyms.....	35
123	Appendix B. Glossary	38
124	Appendix C. Change Log	41
125	List of Figures	
126	Fig. 1. NICE Framework building blocks.....	7
127	Fig. 2. Levels of organization-wide risk management.....	13
128	Fig. 3. ISCM Process.....	25
129	Fig. 4. Incident response life cycle model [SP 800-61r3].....	28
130		

131 **Acknowledgments**

132 The authors would like to thank Pauline Bowen, Joan Hash, and Mark Wilson of NIST who
133 released the original version of SP 800-100 in 2006. Their work laid the foundation for this
134 handbook and continues to inform the content included in Revision 1. The authors would also
135 like to thank Vicki Pillitteri and Arminta Jenkins for their support and input in the development
136 of this revision.

1. Introduction

NIST Special Publication (SP) 800-100, *Information Security Handbook: A Guide for Executive Leadership*, provides high-level summaries of key cybersecurity topics in selected NIST frameworks and points to other NIST publications for more detailed information. Its goal is to help executive leadership in both public- and private-sector organizations understand the relationships between core concepts in cybersecurity using the familiar structure of the NIST Cybersecurity Framework (CSF) 2.0 [CSF 2.0]. The material in this handbook provides general information on key topics, including information security, privacy, cybersecurity supply chain risk management, and enterprise risk management (ERM). Organizations should refer to the cited publications for additional details and guidelines to address their own unique security postures and business requirements.

1.1. Purpose

This document provides high-level descriptions of cybersecurity concepts, actions, and procedures that those in information security and risk management roles (e.g., organizational leadership, Chief Information Officers [CIOs], Chief Information Security Officers [CISOs]) will be expected to implement and oversee in their respective organizations. Subsections that are dedicated to specific topics will point to NIST publications for more detailed information and technical implementation.

The topics in this document are organized based on the Functions and Categories of the CSF to facilitate a consistent approach to establishing and refining information security programs, and many of the topics apply to both public- and private-sector organizations.

1.2. Roles and Responsibilities

This section describes leadership roles and responsibilities that commonly support information security, risk management, and privacy across an organization by considering broader topics, such as governance, operational policy, and decision-making. Each organization may have slightly different roles and responsibilities filled by one or multiple individuals, depending on the size, type, and makeup of the organization.

- **Head of Agency (Chief Executive Officer)**

- Ensures that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the organization
- Ensures that information security processes are integrated with strategic and operational planning processes to secure the organization's mission
- Ensures that senior agency officials within the organization are given the necessary authority to secure the operations and assets under their control

- 172 ○ Ensures that the agency has trained personnel to support compliance with
173 information security policies, processes, standards, and guidelines
- 174 • **Chief Information Officer (CIO)**
 - 175 ○ Develops and oversees an organization-wide information security program and
176 related policies, procedures, and controls to address and comply with
177 information security requirements
 - 178 ○ Coordinates with other senior agency officials to provide annual reports to the
179 agency head on the effectiveness of the agency information security program,
180 including the progress of remedial actions
- 181 • **Chief Information Security Officer (CISO)**
 - 182 ○ Leads an organization-wide information security program, ensuring compliance
183 with relevant legislation and regulations
 - 184 ○ Identifies, assesses, and manages cybersecurity risks by initiating periodic risk
185 assessments and vulnerability analyses, establishing risk mitigation and incident
186 response plans, and overseeing remedial actions to address any deficiencies in
187 policies, procedures, or practices
 - 188 ○ Maintains risk-based and cost-effective information security policies,
189 procedures, and controls to address organizational goals and requirements
190 throughout the system life cycle
 - 191 ○ Ensures that all agency personnel, including contractors, receive appropriate
192 information security awareness training
 - 193 ○ Establishes plans for maintenance and crisis management to ensure the
194 continuity of operations for information systems that support organizational
195 assets and functions
- 196 • **Chief Enterprise Architect**
 - 197 ○ Leads the agency's Enterprise Architecture (EA) development and
198 implementation efforts
 - 199 ○ Collaborates with lines of business within the organization to ensure their proper
200 integration into the EA
 - 201 ○ Participates in agency strategic and performance planning activities to ensure
202 their proper integration into the EA
 - 203 ○ Works closely with program managers, the CISO, and the business owners to
204 ensure that all technical architecture requirements are adequately addressed by
205 applying the EA
- 206 • **Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO)**
 - 207 ○ Develops, promotes, and supports the organization's privacy program

- 208 ○ Leads organization-wide privacy risk management activities, including
- 209 identifying, assessing, and prioritizing privacy-related risks
- 210 ○ Ensures organization-wide privacy compliance for information security assets
- 211 and activities
- 212 ○ Encourages awareness of potential privacy issues and policies
- 213 ○ Reviews and implements privacy regulations and legislation
- 214 Additional roles and responsibilities related to specific program elements are further described
- 215 in later subsections.

216 **1.3. Document Organization**

217 The CSF's¹ Functions and some Categories inform the organization of this document, which is
218 structured as follows:

- 219 • Section 1 introduces the document.
- 220 • Section 2 provides an overview of key NIST frameworks and their relationships to one
- 221 another.
- 222 • Section 3 describes governance concepts, including fundamental elements of risk
- 223 management.
- 224 • Section 44 discusses concepts from the Identify Function of the CSF, including asset
- 225 management, risk assessment, information exchange, and security measurement and
- 226 metrics.
- 227 • Section 5555 discusses concepts from the Protect Function of the CSF, including
- 228 awareness and training programs, contingency planning, and configuration
- 229 management.
- 230 • Section 6 discusses continuous monitoring.
- 231 • Section 77 discusses incident detection, response, and recovery.

¹ This handbook is not intended to be a companion to the CSF.

2. NIST Frameworks

NIST has developed complementary frameworks to provide guidelines on risk management, workforce development, and privacy protections. These frameworks are designed to be flexible and scalable to meet the unique missions, requirements, and environments of both federal and non-federal organizations. The following subsections introduce seven NIST frameworks:

1. Risk Management Framework (see Sec. 2.1Error! Reference source not found.)
2. Cybersecurity Framework 2.0 (see Sec. 2.2Error! Reference source not found.)
3. NICE Framework (see Sec. 2.3Error! Reference source not found.)
4. Privacy Framework (see Sec. 2.4Error! Reference source not found.)
5. Secure Software Development Framework (see Sec. 2.5)
6. AI Risk Management Framework (see Sec. 2.62.62.62.6)
7. Cybersecurity supply chain risk management (C-SCRM) (see Sec. 2.7)

Additionally, Sec. 2.8Error! Reference source not found. provides an overview of how these frameworks intersect to strengthen organizational security and resilience.

2.1. Risk Management Framework (RMF)

SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [SP 800-37r2], provides a comprehensive, flexible, repeatable, and measurable seven-step process that organizations can use to manage their unique information security and privacy risks, and leverages a portfolio of additional resources to support implementation. The Risk Management Framework (RMF) can be applied to new and existing systems or technologies (e.g., IoT, control systems) and within any type of organization, regardless of size or sector. Key terminology and concepts in the RMF include:

- **Risk management strategy:** A strategy that addresses risk tolerance and how organizations plan to assess, respond to, and monitor risks.
- **Authorizing official:** A senior official or executive with the authority to formally assume responsibility and accountability for operating a system and the only organizational official who can accept security and privacy risks to organizational operations, organizational assets, and individuals.
- **Authorization boundary:** Components of a system to be authorized for operation (i.e., the scope of the “system” for RMF implementation).
- **Authorization to operate (ATO):** Periodic or ongoing determination by the authorizing official on whether the system can continue to operate based on the effectiveness of risk management efforts and organizational risk tolerance.
- **Risk tolerance:** The level of risk that an organization is willing to assume to achieve a potential desired result.

- **Security and Privacy Controls:** Descriptions of the safeguards for achieving security and privacy risk management objectives. [SP 800-53r5] provides a catalog of security and privacy controls divided into 20 topic areas referred to as families (e.g., Access Control, Configuration Management, Risk Assessment, Personally Identifiable Information (PII) Processing and Transparency, Supply Chain Risk Management). The current SP 800-53 catalog is maintained in the [Cybersecurity and Privacy Reference Tool \(CPRT\)](#).
- **Tailoring:** The process by which control baselines and controls are modified to meet organizational risks and constraints [SP 800-53B].

The risk-based approach of the RMF includes the following steps:

- **Prepare** for risk management with essential activities for program design and implementation. Related tasks include defining risk management roles, creating a risk management strategy and continuous monitoring strategy, determining the scope of the system's authorization boundary, and conducting risk assessments.
- **Categorize** systems and information based on an impact analysis. Related tasks include documenting a description of the system and identifying potential adverse impacts related to the confidentiality, integrity, and/or availability of information stored, processed, or transmitted by the system.
- **Select** [SP 800-53r5] controls to protect the system based on its security categorization and completed risk assessments. Related tasks include selecting the corresponding SP 800-53B security control and/or privacy baseline, tailoring the control baseline to align with organization specific security and privacy objectives, allocating additional controls to the system, documenting planned control implementation, and developing and implementing a system-level continuous monitoring strategy.
- **Implement** the controls, and document how the controls are deployed. Related tasks include documenting the as-implemented controls.
- **Assess** the control implementation to determine whether the controls are in place, operating as intended, and producing the desired results to manage risks. Related tasks include developing a control assessment plan, conducting control assessments, developing assessment reports, and developing a plan of action and milestones (POA&M) to track risks through remediation or acceptance.
- **Authorize** the system to operate; the system is put into operation after the authorizing official accepts residual risk and determine it is within the organizational risk tolerance. These tasks include assembling the authorization package for review by the authorizing official; reviewing, analyzing, and responding to risks; and having the authorizing official make an authorization decision.
- Continuously **monitor** the effectiveness of control implementations and identify any changes to the risks to the system. These tasks include monitoring system environment for new components, identifying configuration changes to existing system components, conducting ongoing control assessments, implementing risk responses, reporting on

vulnerabilities and weaknesses in the system, and updating the authorization package to reflect the ongoing state of the protections for system operations.

[SP 800-37r2] provides more detailed information about the RMF. Additional RMF-related resources are available at <https://nist.gov/rmf>.

2.2. Cybersecurity Framework (CSF 2.0)

The Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors — including industry, government, academia, and nonprofit — manage and reduce their cybersecurity risks alongside their other organizational risks (e.g., financial, supply chain, reputational, regulatory). The CSF describes desired cybersecurity outcomes that are sector-, country-, and technology-neutral to give organizations the flexibility to prioritize the cybersecurity outcomes that best address their unique risks, technologies, and business/mission considerations.

The CSF includes the following components:

- **CSF Core:** A taxonomy of high-level cybersecurity outcomes that are organized hierarchically into Functions, Categories, and Subcategories that detail each outcome. The Core describes *what* desired outcomes an organization can aspire to. Additional CSF resources and existing controls catalogs can assist organizations in determining *how* to achieve the desired outcomes.
- **CSF Organizational and Community Profiles:** An Organizational Profile is a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes. Profiles can help an organization prioritize the CSF Core outcomes to achieve its target state. A Community Profile is a baseline of CSF outcomes that is created and published to address shared interests and goals among organizations. It is typically developed for a particular industry sector or subsector, technology, threat type, or other use case. An organization can use as-is or tailor a Community Profile as the basis for its own Target Profile.
- **CSF Tiers:** Provide context for how an organization views cybersecurity risks and the processes in place to manage those risks. Tiers can also be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices.

2.3. NICE Framework

The National Initiative for Cybersecurity Education (NICE) was created by the Cybersecurity Enhancement Act of 2014 [CEA] to establish a national cybersecurity and education program. Its mission is to promote a holistic approach to cybersecurity education, training, and workforce development in both federal agencies and the private sector. In 2017, NICE created the Workforce Framework for Cybersecurity (NICE Framework), which helps organizations describe their cybersecurity efforts through three conceptual building blocks: tasks, knowledge, and

skills (TKS). These concepts directly inform the development of TKS statements to articulate specific organizational objectives [NICE]:

1. Task statements describe cybersecurity work activities.
2. Knowledge statements describe the required understanding for accomplishing tasks.
3. Skill statements describe the required abilities for accomplishing tasks.

In short, tasks describe the work being done, while knowledge and skills refer to the learner, as shown in Fig. 1.

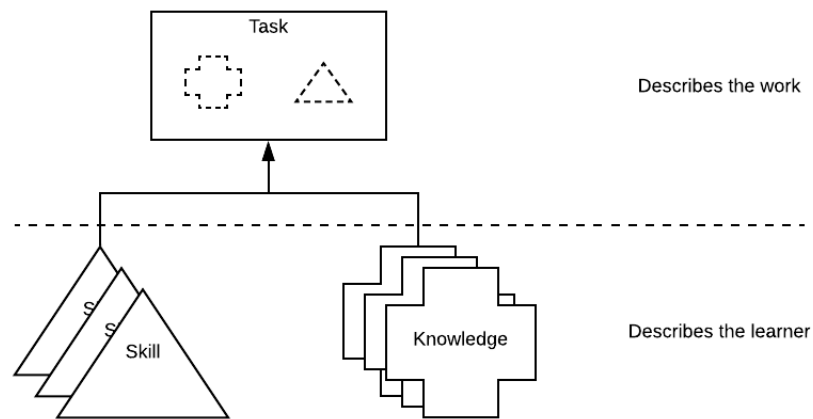


Fig. 1. NICE Framework building blocks

The NICE Framework was designed to evolve with changing technologies and risks and grants organizations the ability to adapt to their unique contexts. It also standardizes communication and terminology in a way that aligns with related frameworks.

SP 800-181r1, *Workforce Framework for Cybersecurity (NICE Framework)* [NICE], introduces competencies to enable organizations to assess their learners by grouping associated TKS statements. Competencies map to job roles, workforce needs, and training programs to support interoperability.

2.4. Privacy Framework

The NIST Privacy Framework provides a common language for understanding, managing, and communicating privacy risk with both private and public stakeholders. Designed as a voluntary tool, it is intended for broad applicability across organizations of all sizes and is agnostic to any particular technology, sector, law, or jurisdiction. The Framework is adaptable to any organization's role in the data processing ecosystem and assists in the identification and prioritization of actions for reducing privacy risks. Ultimately, it serves as a valuable tool for aligning policy, business, and technological approaches to effectively manage risks. Use of the NIST Privacy Framework can help:

- Establish or improve a Privacy Program

- Strengthen accountability
- Prioritize and transform privacy outcomes by integrating privacy into the system development life cycle (SDLC)
- Align privacy risk management by communicating requirements to internal and external stakeholders
- Inform decision-makers about buying decisions

Even when fully compliant with applicable laws and regulations, unintended consequences can affect an organization's brand, finances, and prospects for growth. Privacy risk assessments can help organizations analyze their practices, detect gaps, and identify areas for improvement. By utilizing a risk- and outcome-driven approach, the NIST Privacy Framework supports the development of innovative and effective solutions that enhance outcomes for individuals and organizations, while ensuring relevance in the face of evolving technology. Additional detailed information regarding the NIST Privacy Framework can be found at [Privacy Framework](#).

2.5. Secure Software Development Framework (SSDF)

The Secure Software Development Framework (SSDF) defines high-level practices that organizations can integrate into existing software development procedures, including acquisition and collaboration with third-party suppliers. These practices are organized into four general categories:

1. **Prepare the Organization (PO):** Ensuring that an organization's people, processes, and technologies are prepared to perform secure software development
2. **Protect the Software (PS):** Protecting components of software from tampering and unauthorized access
3. **Produce Well-Secured Software (PW):** Producing well-secured software with minimal security vulnerabilities
4. **Respond to Vulnerabilities (RV):** Identifying residual vulnerabilities and addressing them appropriately to prevent future occurrences

The SSDF does not prescribe implementation but focuses on intended outcomes, which allows organizations to tailor these practices to their unique environments and needs.

SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* [SP 800-218], describes these categories in greater detail, including tasks, notional implementation examples, and additional references.

2.6. Artificial Intelligence Risk Management Framework (AI RMF)

NIST's Artificial Intelligence Risk Management Framework (AI RMF) is a flexible, sector- and use-case-agnostic resource that aligns with related NIST guidelines and adapts to evolving technological landscapes. It is designed to help organizations foster the responsible design,

development, deployment, and use of trustworthy AI systems. The AI RMF Core then describes specific functions that help organizations address AI-related risks: Govern, Map, Measure, and Manage. These functions include detailed categories, actions, and outcomes.

Use of the AI RMF can lead to:

- Improved awareness of the relationships and trade-offs among trustworthiness characteristics, including approaches that consider community and organizational dynamics, human behavior, and AI risks
- Clear processes for making system commissioning and deployment decisions
- Policies, practices, and procedures for improving organizational accountability and transparency related to AI systems
- Enhanced organizational culture that considers both the benefits of innovation and the identification and management of AI risks
- Better information sharing within and across organizations about risks, decision-making processes, responsibilities, common pitfalls, measurement practices, and approaches for continuous improvement
- Greater contextual knowledge for increased awareness of downstream risks
- Strengthened engagement with interested parties and relevant AI actors
- Improved ability to measure AI system performance and risks

NIST Artificial Intelligence (AI) 100-1, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* [AI RMF], describes the trustworthiness characteristics in detail and provides examples of outcomes and actions for the Core functions.

2.7. Cybersecurity Supply Chain Risk Management (C-SCRM)

Cybersecurity supply chain risk management (C-SCRM), while not technically a NIST framework, describes a systematic process for managing exposure to cybersecurity risks throughout supply chains and developing appropriate response strategies, policies, processes, and procedures [CSF 2.0]. All technologies rely on a complex, globally distributed, and interconnected supply chain ecosystem of public- and private-sector entities that interact throughout the life cycle of a product or service. Effective C-SCRM requires both internal and external stakeholder engagement to actively collaborate, communicate, and take collective action to secure favorable C-SCRM outcomes and understand the potential ramifications of cybersecurity risks throughout the supply chain.

C-SCRM is integrated into enterprise-wide risk management processes (e.g., acquisition, system development life cycle) so that organizations can identify priorities and develop solutions. As the exposure to supply chain risks differs across and within enterprises, business- and mission-specific strategies and policies should set the tone and direction for C-SCRM across the enterprise [SP 800-161r1].

2.8. Relationships Between Key NIST Frameworks

Together, these frameworks and processes form a complementary ecosystem for addressing distinct but associated risk domains based on common structural principles. Since they are designed to be technology and sector-neutral, they can be layered onto one another and tailored to organizational needs. Moreover, they explicitly reference one another's components to ensure a well-rounded approach to defining outcomes, processes, and workforce capabilities.

The operational foundation of these NIST frameworks is the RMF, which describes procedural guidelines on governance and risk management. Its seven-step life cycle can be applied to both new and existing systems in any organization, regardless of size or sector. It also directly aligns with and references other key NIST frameworks and resources. For example, the RMF's "Select" step explicitly draws from the control catalog in [SP 800-53r5], and the "Implementation" step is hardened by SSDP practices, which in turn intersect with C-SCRM (e.g., third-party collaboration, acquisition). The RMF describes a repeatable implementation process for achieving the target states defined in other frameworks.

The CSF's Functions, Categories, and Subcategories then layer on the RMF to describe cybersecurity outcomes. For example, an organization can use the CSF's Organizational Profiles to set its target cybersecurity posture and then implement the RMF's process to achieve that posture. This enables strategic, organization-wide prioritization that considers financial, supply chain, and reputational risks. The Privacy Framework also supplements the RMF to specifically address the privacy risks that can arise, even when an organization is fully compliant with applicable laws and regulations. It feeds into the control selections [SP 800-53r5] for the RMF to give organizations a privacy-specific vocabulary that mirrors how the CSF addresses cybersecurity. The AI RMF is another domain-specific extension of the RMF that addresses AI-specific risks and trustworthiness characteristics. Like the CSF's Organizational Profiles and the Privacy Framework's prioritization mechanisms, the AI RMF's functions define the target states and priorities that the RMF's life cycle helps implement.

While the RMF, CSF, Privacy Framework, and AI RMF focus on outcomes and processes, the NICE Framework addresses how people carry out those activities. Its Task, Knowledge, and Skill (TKS) model describes the work that needs to be done, the knowledge and skills required to do it, and the language for communicating about it. Its focus on workforce development supports the implementation of every other framework.

Together, these flexible, agnostic frameworks help executive leadership understand the people, processes, and technologies that are needed to help system-level management align security activities with mission objectives.

3. Governance

Governance refers to the set of responsibilities and practices that are exercised by organizations with the express goal of[SP 800-39]:

- Setting the criteria and expectations by which risk management will be conducted [IR 8286Cr1] (see Sec. 3.1.1),
- Establishing cybersecurity governance roles and responsibilities (see Sec. 3.2), and
- Establishing and updating organizational cybersecurity governance policies (see Sec. 3.3).

Governance activities ensure that organizational missions and objectives are met, resources are used in a responsible manner, and protections and safeguards are incorporated into the organization's broader security, privacy, and cybersecurity strategies. Section 3.4 identifies specific federal governance requirements that may be useful for other organizations.

In addition to cybersecurity risk management (CSRM), privacy risk management (see Sec. 2.4) and cybersecurity supply chain risk management (see Sec. 2.7) are critical elements of organizational governance.

3.1. Risk Management Fundamentals

While striving to realize business and mission objectives, organizational leadership is expected to manage a variety of risks (e.g., legal, financial, reputational, regulatory) across the enterprise under the umbrella of governance, including clearly expressing expectations for how risk is managed [IR 8286Ar1]. Executives prioritize risk management as a core component of investment strategies to ensure that adequate resources are allocated based on risk management priorities. By employing practices and procedures that are designed to foster informed decision-making, senior leadership facilitates the protection of information assets that support the organizational mission.

Key Risk Management Concepts and Definitions

According to SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, the components of risk management include:

- **Framing risk:** Establish a risk context by providing a common perspective on how organizations manage risks. A business impact analysis (BIA) can provide information about asset valuation and criticality that factor into understanding the risk impact and adequately resourcing risk responses.
- **Assessing risk:** Identify, prioritize, and estimate the likelihood that a threat event will occur and the consequences of an adverse impact to the organization and operations. Risks can be cataloged in a risk register to support organization-wide understanding of identified risks across the entire asset portfolio.
- **Responding to risk:** Identify, evaluate, decide on, and implement appropriate courses of action to accept, avoid, mitigate, share, or transfer risk.

- **Monitoring risk:** Verify that planned risk response measures are implemented and determine the ongoing effectiveness of the risk response over time.

A key output from these components is the risk management strategy, which addresses risk appetite, risk tolerance, assumptions, constraints, and how the organization intends to assess, respond to, and monitor risks. The risk management strategy also considers the following:

- **Risk appetite:** Defined at the highest level of the organization and provides a guide to the types and amount of risk that senior leaders are willing to accept in pursuit of mission objectives [IR 8286Ar1]
- **Risk tolerance:** Represents the specific level of risk deemed acceptable within the risk appetite set by senior leadership. Organizations may choose to express risk tolerance qualitatively (e.g., Very Low, Low, Moderate, High, or Very High) [IR 8286Ar1]

Risk appetite and risk tolerance are related but distinct. While risk appetite statements define the overarching risk guidance, risk tolerance statements define the specific application of that direction. This means that risk tolerance statements are always more specific than the corresponding risk appetite statements. Together, risk appetite and risk tolerance statements represent and communicate risk limits that can assist organizations in managing risk [IR 8286Ar1].

3.1.1. Enterprise Risk Management (ERM)

Enterprise risk management (ERM) is a structured approach to identifying, assessing, and responding to risks throughout the entire portfolio of organizational systems and services, including security, privacy, and supply chain risks [IR 8286r1]. This holistic view enables organization leadership to determine the probability that these risks will occur and estimate their potential impacts. Effective strategic planning requires understanding organizational context, including:

- The organization's mission, purpose, and high-level business objectives and how they inform enterprise risk management
- The organization's stakeholders and the critical organizational outcomes or services they depend on
- Relevant laws, regulations, and contractual requirements that influence the organization's operations and cybersecurity risk management
- Externally provided capabilities or services that the organization needs to achieve its mission

Managing information security risk across an organization involves multiple levels of risk management [SP 800-39] that each have a different risk focus, as shown in Fig. 2.

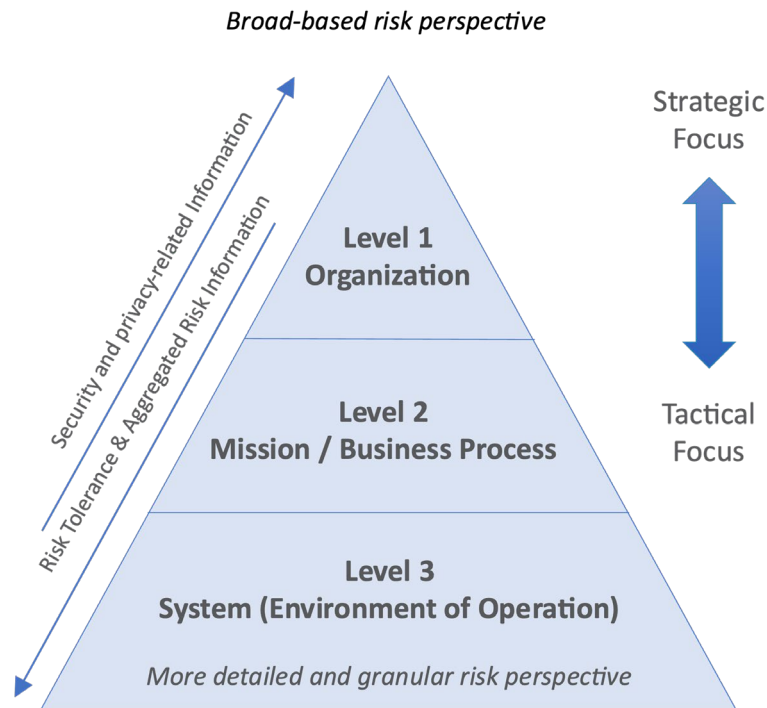


Fig. 2. Levels of organization-wide risk management

- **Level 1** addresses risk from an organizational perspective to provide the context for all risk management activities. Risk management activities at Level 1 include prioritizing mission and business functions, identifying investment strategies and funding decisions, identifying responsible entities for risk management (including cyber supply chain risk management [C-SCRM]), developing the enterprise architecture, developing an organizational risk management strategy, defining risk tolerance, and developing an overarching C-SCRM strategy, policy, and high-level implementation plan.
- **Level 2** addresses risk from a mission and business process perspective and is informed by the risk context, decisions, and activities at Level 1. Risk management activities at Level 2 include defining and prioritizing mission and business functions that are consistent with the strategic goals identified at Level 1, incorporating cybersecurity requirements into the mission and business processes, establishing an enterprise architecture that addresses information security and privacy, and performing activities in accordance with the C-SCRM strategy and policies developed at Level 1. Specific C-SCRM program requirements are also defined and managed at Level 2, including cost, schedule, performance, security, and other critical non-functional requirements.
- **Level 3** addresses risk from a system perspective and is guided by the risk context, decisions, and activities at Levels 1 and 2. Risk management activities at Level 3 include categorizing systems, managing the selection and implementation of security controls, and continuously monitoring the controls to manage risks in accordance with the organizational risk management strategy. At Level 3, procurements are conducted and

system-related C-SCRM activities are executed as part of the SDLC, including the development of a C-SCRM plan for the system.

Management at each organizational level (Fig. 2) implements procedures to ensure that risks are framed, assessed, responded to, and monitored in order to maintain an acceptable level of risk within identified risk tolerances. As the risk landscape evolves (e.g., due to technological or environmental changes), leadership and management integrate information security activities into strategic planning processes and clearly document the following:

- Comprehensive risk management goals and objectives and how they relate to the organization's mission
- A high-level plan for achieving information security, privacy, and supply chain risk management goals, including specific short- and mid-term objectives and performance targets
- Strategies for allocating an organization's limited resources to achieve identified goals and objectives
- Performance measures to continuously monitor the accomplishment of identified goals and progress toward stated targets

To learn more about ERM, see the Interagency Report (IR) 8286 series of publications. For more information about risk management strategies, see [SP 800-39] and the Prepare step in [SP 800-37r2]. For information about managing cybersecurity supply chain risks, see SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* [SP 800-161r1], and SP 800-18r2, *Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems* [SP 800-18r2].

3.2. Establishing Cybersecurity Governance Roles and Responsibilities

Organizational leadership is responsible for:

- Establishing cybersecurity and governance roles, as well as communicating the responsibilities and corresponding authorities for those roles
- Allocating appropriate resources to ensure that responsibilities can be met

Many common organizational cybersecurity roles and responsibilities are listed in Sec. 1.2 for reference. Relevant governance roles, and their associated responsibilities [IR 8286Cr1], may include:

- Enterprise-Level Oversight
 - Ensure organizational alignment with strategic priorities
 - Enforce management accountability for achieving organizational objectives
- Enterprise-Level Risk Governance
 - Maintain oversight of the enterprise risk management function

- 604 ○ Determine risk reporting requirements and ensure reporting to external
605 stakeholders
- 606 • Enterprise-Level Risk Management
- 607 ○ Implement the organizational risk management program
- 608 ○ Aggregate risks reported by various risk owners, including third-party suppliers
- 609 ○ Provide regular, comprehensive risk reports to organizational executives
- 610 ○ Consult with organizational leaders to establish enterprise risk appetite and
611 tolerance
- 612 • Organizational-Level Risk Governance
- 613 ○ Establish and communicate organizational risk management policies
- 614 ○ Ensure organizational-level risk is communicated to the enterprise-level
- 615 ○ Ensure organizational personnel are made aware of applicable policies and
616 procedures
- 617 • System-Level Risk Management
- 618 ○ Document and track identified risks, including those inherited from third-party
619 suppliers
- 620 ○ Ensure identified risks and risk responses are monitored and reported to
621 organizational-level risk management

622 **3.3. Establishing and Updating Organizational Cybersecurity Governance Policy**

623 Information security governance requires a documented policy based on appropriate
624 legislation, applicable standards and guidance, and internal organizational requirements. The
625 policy should address the fundamental components of the information security governance
626 structure, including:

- 627 • Information security roles and responsibilities (see Sec. 1.2)
- 628 • A statement of the security controls baseline and procedures for tailoring the baseline
629 (see Sec. 3.1)
- 630 • Rules of behavior that agency users are expected to follow with appropriate
631 repercussions for noncompliance

632 The organizational cybersecurity policy may also address measurement and metrics (see Sec.
633 4.4), awareness and training (see Sec. 5.2), contingency planning (see Sec. 5.3), configuration
634 management (see Sec. 5.4), continuous monitoring (see Sec. 6), and incident response (see Sec.
635 7.2). Organizations implement a policy review and revision cycle to ensure that their
636 information security policy is regularly updated to accommodate the changing information
637 security environment, the organization's mission, and operational requirements. As part of the
638 initial development and periodic review of the information security policy, organizations ensure

that internal policies are aligned for effective implementation and convergent security objectives, such as access control initiatives.

3.4. Federal Governance Requirements

The following legislation and federal-wide policy inform the protection of information systems and data in federal organizations but may also be useful for private (i.e., non-federal) organizations:

- Federal Information Security Modernization Act of 2014 [FISMA] updates the 2002 law, strengthening federal government cybersecurity by requiring risk-based, cost-effective security for federal information systems, introducing continuous diagnostics, and streamlining reporting.
- The 2014 Federal Information Technology Acquisition Reform Act [FITARA] reforms how federal agencies acquire and manage IT, aiming to reduce waste and duplication while improving transparency.
- The Federal Managers Financial Integrity Act [FMFIA] of 1982 requires accountability for financial and program managers, including the financial results of the actions they take, the control and use of the Federal Government's financial resources, and the protection of federal assets.
- The Federal Financial Management Improvement Act [FFMIA] of 1996 focuses specifically on the technical and managerial control of financial management systems.
- OMB Circular A-130, *Managing Information as a Strategic Resource* [OMB A-130][OMB A-130], establishes executive policies for managing federal information security programs and resources, including security, privacy, records management, and information governance. The provisions of OMB A-130 are considered mandatory requirements for the federal executive branch and serve as regulatory requirements for other entities, particularly those interconnecting with federal program.
- OMB Circular A-123, *Management's Responsibility for Internal Control* [OMB A-123], "ensures federal agencies are accountable for their operations and finances, foster transparency, and responsibly manage and safeguard taxpayer funds." The provisions of OMB A-123 support the enforcement of FITARA, FMFIA, and FFMIA legislation.
- The GPRA Modernization Act of 2010 [GPRAMA] is the basis for Federal Government performance management. GPRAMA seeks to improve federal management, transparency, and efficiency by requiring federal agencies to set 4-year strategic plans, 2-year Agency Priority Goals (APGs), and quarterly, data-driven performance reviews. It is an update to the Government Performance and Results Act [GPRA] of 1993, which established the foundation for budget decision-making to achieve strategic goals and meet agency mission objectives.

The Clinger-Cohen Act of 1996 [AI RMF] National Institute of Standards and Technology
(2023) Artificial Intelligence Risk Management Framework (AI RMF 1.0).

- 677 (National Institute of Standards and Technology, Gaithersburg, MD), NIST
678 Artificial Intelligence (AI) NIST AI 100-1. [https://doi.org/10.6028/NIST.AI.100-](https://doi.org/10.6028/NIST.AI.100-1)
679 1
- 680 • [CCA] set requirements for Capital Planning and Investment Control (CPIC) and the role
681 of CIO in federal agencies.

4. Identify

The CSF Identify Function focuses on understanding the organization's current cybersecurity risks by, for example:

- Identifying and managing assets ([SP 800-53r5] CM-08, *System Component Inventory*)
- Conducting risk assessments ([SP 800-53r5] RA-03, *Risk Assessment*) and identifying exploitable vulnerabilities ([SP 800-53r5] RA-05, *Vulnerability Monitoring and Scanning*)
- Planning and documenting the flow of organizational information ([SP 800-53r5] AC-04, *Information Flow Enforcement*; CA-03, *Information Exchange*)
- Utilizing measurements and metrics to improve cybersecurity risk management processes ([SP 800-53r5] AU-06, *Audit Record Review, Analysis, and Reporting*).

4.1. Asset Management

A key element of asset management is maintaining an accurate inventory of all organizational assets (e.g., hardware, software, data, facilities). The inventory may also include services provided by external parties as well as documentation of organizational data flows. Asset inventory is not a one-time task. Processes should be established to regularly maintain an accurate inventory of organizational assets.

Identified assets may also need to be managed throughout their life cycles, from development and acquisition to disposal. An important component of managing assets is configuration management (see Sec. 5.4), which is a process for monitoring and managing the configuration settings of assets to maintain system integrity and prevent unauthorized changes to assets. Organizations may benefit from establishing processes for updating the asset inventory to record authorized changes to systems, provide required maintenance to assets, and securely dispose of assets when they have reached end of life. For more information about asset management, see SP 1800-5, *IT Asset Management* [SP 1800-5].

4.2. Risk Assessment

Risk assessments are a critical component of an organization's risk management process (see Sec 3.1). Risk assessments help identify, estimate, and prioritize risks to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of information systems. Risk assessments inform decision-makers and support risk responses by identifying relevant threats, vulnerabilities, the potential impacts of exploiting vulnerabilities, and the likelihood that harm will occur. The result is a determination of risk to the organization [SP 800-30r1].

To be effective and useful, organizations should conduct risk assessments on an ongoing basis and at various stages of a system's life cycle. Risk assessments are composed of 4 steps:

1. Prepare for the assessment — Identify the purpose, scope, and constraints of the assessment as well as the methodology to be used.
2. Conduct the assessment — Analyze threats, vulnerabilities, impacts, and likelihoods to produce a list of information security risks that can be prioritized by risk level and used to inform risk response decisions.
3. Communicate assessment results — Ensure that decision-makers across the organization have the appropriate risk-related information needed to inform and guide risk decisions.
4. Maintain the assessment — Maintain risk assessments to incorporate any changes detected through risk monitoring.

The results of risk assessment help organizations respond to (i.e., identify, evaluate, decide on, and implement appropriate courses of action to accept, avoid, mitigate, share, or transfer risks) and monitor risks (i.e., verify that planned risk response measures are implemented and determine the ongoing effectiveness of the risk response over time). For more information about risk assessments, see SP 800-30r1, *Guide to Conducting Risk Assessments* [SP 800-30r1].

4.3. Information Exchange

Information exchange refers to accessing or transferring data outside of authorization boundaries to accomplish a mission or business function. Significant benefits can be achieved through the exchange of information, such as decreased operating costs, greater functionality, improved efficiency, centralized data access, the reduction of duplicative datasets, and enhanced relationships between collaborating organizations.

An important component of information exchange is system interconnection, which is defined as a direct connection between two or more systems in different authorization boundaries for the purpose of exchanging information and/or allowing access to information, information services, and resources. Organizations establish formal agreements that specify the technical and security requirements of the interconnection, define the responsibilities of the participating organizations, identify the risks inherited from the participating organization, and specify the rules that govern these interconnections.

SP 800-47, *Managing the Security of Information Exchanges* [SP 800-47r1], provides guidelines for planning, establishing, maintaining, and discontinuing information exchange and access between systems that are owned and operated by different organizations or that cross authorization boundaries.

4.4. Measurement and Metrics

Information security measurement helps organizations describe and quantify information security, identify gaps, and make informed decisions to accomplish strategic goals and

objectives. The process involves gathering numerically expressed data (i.e., measures) and conducting quantitative assessments to determine whether the organization is meeting its information security goals. A robust information security measurement program provides the structure for collecting, analyzing, and reporting relevant data to inform decisions that directly affect the information security posture of an organization, including its budget and personnel. Continuous feedback supports regular communication with high-level members of the organization regarding information security performance and risks.

Organizations also utilize metrics to track progress, facilitate decision-making, and improve performance with respect to a set target. The information gained from measurement may be used to identify and define new metrics, which in turn drive subsequent assessments. Organizations can evaluate metrics over a continuous period to identify long-term trends in organization-, program-, and system-level information security plans, policies, procedures, and goals.

For more detailed information on measurement and metrics, see SP 800-55v1 (Volume 1), *Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures* [SP 800-53B] Joint Task Force (2020) Control Baselines for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53B, Includes updates as of October 2020.
<https://doi.org/10.6028/NIST.SP.800-53B>
[SP 800-55v1], and SP 800-55v2, *Measurement Guide for Information Security: Volume 2 — Developing an Information Security Measurement Program* [SP 800-55v2].

5. Protect

In addition to governance strategies, organizations can implement operational safeguards to protect critical assets by considering the people, processes, and practices needed to sustain operational resilience and reduce the impacts of adverse events. This section provides high-level overviews of several critical operational domains:

- Zero trust architecture (see Sec. 5.1), which protects systems and data by assuming no implicit trust in users, devices, or services
- Awareness and training (see Sec. 5.2), which ensures that all personnel understand their roles and responsibilities
- Contingency planning (see Sec. 5.3), which establishes clear procedures for responding to disruptions
- Configuration management (see Sec. 5.4), which defines how the system is configured and how changes are controlled to prevent new vulnerabilities or disruptions to system operations

5.1. Zero Trust Architecture

Zero trust architecture (ZTA) is a cybersecurity paradigm that eliminates implicit trust by assuming that threats exist both inside and outside of traditional network boundaries. It focuses on protecting resources (e.g., assets, services, workflows) rather than network segments through strict per-request authentication and authorization for all users and devices. ZTA replaces the concept of implicit trust with a requirement for continuous verification, segmentation, and the principle of least privilege [SP 800-207]. It is a strategic approach to aligning with the RMF and CSF 2.0 outcomes by adhering to seven core tenets:

1. All data sources, services, and devices are considered resources and must therefore be protected, regardless of their location or ownership.
2. All communication must meet the same security requirements, even if they originate from an enterprise-owned network.
3. Access to resources should be based on least privilege and granted on a per-session basis after a requester has been authenticated.
4. Access decisions should be based on a dynamic policy that considers a client's identity, the state of the asset (e.g., software versions, previously observed behavior), and environmental context (e.g., reports of active attacks).
5. Organizations should continuously monitor and evaluate the security posture of an asset (e.g., device, data, infrastructure) before granting a resource request.
6. Authentication and authorization should be continuously evaluated and enforced before access is granted.

7. Organizations should collect and analyze data on their security posture, network activity, and access requests to improve access decisions.

SP 800-207, *Zero Trust Architecture* [SP 800-207], describes a variety of deployment scenarios, threats, and other considerations for integrating zero trust principles in alignment with NIST Frameworks (see Sec. 2).

5.2. Awareness and Training

Security awareness and training programs are critical for disseminating security information across an organization and providing the workforce with the tools they need to protect vital information resources. These programs ensure that personnel at all levels of the organization understand their information security responsibilities to properly identify, respond to, and manage risks. While such programs vary across organizations, they share fundamental elements that can be used to create a Cybersecurity and Privacy Learning Program (CPLP), which encompasses cybersecurity and privacy awareness, training, and education [SP 800-50r1].

Typical CPLP activities that are implemented throughout the program's life cycle include awareness promotion, experiential learning, and training[SP 800-50r1]. SP 800-37r2 (Revision 2), *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [SP 800-37r2][SP 800-37r2], identifies the typical roles associated with cybersecurity and privacy training programs. The NICE Framework [SP 800-181r1]also offers guidance for identifying those with responsibilities for managing the CPLP. Depending on the organization, a single person may serve multiple functions, or multiple people may have overlapping responsibilities[SP 800-50r1]. The roles and responsibilities for key positions in a CPLP should be documented in the program plan. Many of the roles associated with awareness and training will likely have been identified during information security governance activities (see Sec. 1.2).

Additionally, the NICE Framework (see Sec. 2.3) recommends creating and referencing TKS statements that describe both the work that needs to be accomplished and the users who will complete it[SP 800-181r1]. TKS statements become a core element of NICE Framework Competencies, which describe tasks, track workforce capabilities, and identify team requirements. The goal of a CPLP is to ensure that all personnel are aware of their roles and responsibilities for protecting information and assets and can take appropriate actions to respond to a variety of cybersecurity and privacy risks. This may include requiring personnel to agree to Rules of Behavior (RoB) that establish standards of conduct for accessing an organization's information systems. Security and privacy training can directly map to RoB provisions to educate personnel on specific behaviors to integrate into day-to-day activities.

The Federal Information Security Modernization Act [FISMA] requires federal agencies to implement awareness activities and role-based training as security controls to minimize the inherent risks that result from the people who use, manage, operate, and maintain information systems and networks. SP 800-50r1, *Building a Cybersecurity and Privacy Learning Program* [SP 800-50r1], provides detailed guidelines for federal and non-federal organizations to develop a CPLP that works within a larger organizational program to address risks, including physical

privacy and security threats, insider threats, and other related human risk management concerns[SP 800-50r1].

5.3. IT Contingency Planning

Information technology (IT) contingency planning refers to the process of recovering information system services and data after a disruption of operations due to natural, technological, or human-driven events. Organizations establish policies and procedures for interim measures that help ensure the safety and security of personnel and property; inform crisis communication with personnel, law enforcement, and the public; and mitigate long-term impacts.

Contingency planning typically requires a suite of specific plans to effectively respond to and recover from disruptive events. Each type of plan has its own scope, purpose, and activities that vary depending on the organization. SP 800-34r1, *Contingency Planning Guide for Federal Information Systems*[SP 800-34r1] [SP 800-34r1], describes the types of plans that organizations can utilize to protect their systems. The following common plans are listed in alphabetical order[SP 800-34r1]:

- **Business continuity plan (BCP):** Focuses on sustaining the organization's mission and business processes (e.g., payroll, customer service). BCPs are typically used by non-federal organizations.
- **Continuity of operations (COOP) plan:** Focuses on restoring the organization's mission-essential functions (MEF) at an alternate site for up to 30 days before a return to normal operations. COOP plans are typically used by government organizations and may be mandated by FCD 1, *Federal Executive Branch National Continuity Program and Requirements* [FCD1].
- **Crisis communications plan:** Documents procedures for internal and external communications after a disruption. These procedures may include guidance on dissemination reports and statements (e.g., templates) and the designation of a specific individual to provide information to the public.
- **Critical infrastructure protection (CIP) plan:** Describes policies and procedures for protecting and recovering vital national assets (i.e., critical infrastructure) and mitigating risks and vulnerabilities. The CIP plan defines roles and responsibilities and implements the risk management framework of the National Infrastructure Protection Plan (NIPP) [NIPP].
- **Disaster recovery plan (DRP):** Focuses on addressing major disruptions that affect the primary facility's infrastructure and restoring operability at an alternate site. A DRP is site-specific and includes procedures for moving operations to a temporary location. It may be part of a BCP or COOP plan.
- **Information system contingency plan (ISCP):** Establishes procedures for assessing and recovering a system after disruption. The ISCP identifies roles and responsibilities; details assessment, recovery, and testing procedures; and includes inventory

information. The ISCP is intended for system recovery regardless of location and can be implemented at the primary site or after the DRP has successfully transferred systems to an alternate location.

- **Occupant emergency plan (OEP):** Outlines first-response procedures in the event of an incident that threatens the health or safety of personnel, the environment, or property (e.g., fire, medical emergency, bomb threat). An OEP is site-specific and includes shelter-in-place and evacuation procedures. While it is executed as a first response, it may be included in a BCP or COOP.

5.4. Configuration Management

Configuration management (CM) identifies the processes for establishing the initial configuration of a system (i.e., baseline configuration), controlling changes to the configuration, and monitoring the configurations throughout the system's life cycle. Organization-level, security-focused policies support system-level plans to provide a comprehensive strategy for managing the configuration of components that are required for system operations.

The configuration of a system may change in response to:

- New threats and evolving tactics by existing threat actors
- Updates to system security, privacy, or supply chain risk management requirements resulting from changes to mission objectives, business functions, regulations, standards, and suppliers
- Improvements to hardware and software capabilities
- The identification of flaws and vulnerabilities in components of the existing environment of operations

Changes can be initiated by numerous individuals (e.g., users, system owners) or identified through audit findings or other reviews. An impact analysis can identify the effects that the change may have on the system or other interrelated systems. As changes are made to baseline configurations, the new baseline becomes the current version. The previous baseline is no longer valid but is retained for traceability during configuration reviews and control assessments. For example, if there are issues with a production release, the retention of previous versions of the configuration allows system operators to roll back or restore a previous secure and functional version of the baseline configuration.

The system owner serves as the authority for all CM processes and is responsible for developing functional requirements and verifying that the requirements are implemented appropriately. Reviews of the configuration baseline against the implemented configurations can identify gaps in the CM processes, including changes that were not approved, that have not been implemented correctly, or whose impact was greater than originally discussed during the analysis and approval of the change.

The organization can also identify additional roles for the approval process based on the configuration item, the type of change, and the criticality of the change (e.g., mission-critical,

926 moderate-impact, low-impact). A Configuration Control Review Board (CCRB) with various
927 organization- and system-level risk management related roles may be responsible for discussing
928 and resolving change requests that require additional funding or resources, ensuring that
929 change requests do not adversely affect any systems or services, and evaluating CM metric
930 information on other related issues.

931 SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems* [SP
932 800-128], provides detailed guidelines for developing a configuration management process that
933 identifies configuration items, establishes approved baseline configurations, and defines
934 security-focused configuration control processes to ensure that changes do not adversely affect
935 the security of the system or the organization.

936

6. Continuous Monitoring

Information security continuous monitoring (ISCM) analyzes the effectiveness of security and privacy controls in accordance with organizational risk tolerance. It incorporates processes to help risk managers:

- Maintain situational awareness of all systems across the organization
- Understand security, privacy, and cybersecurity supply chain threats
- Review the status and effectiveness of all implemented security, privacy, and supply chain risk management controls
- Provide actionable communication on the risk management status across all tiers of the organization
- Ensure that organizational officials actively manage risks

SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* [SP 800-137], provides more detailed information on developing a continuous monitoring strategy and implementing a program.

6.1. ISCM Strategy

A well-designed ISCM strategy encompasses control assessment, status monitoring, and status reporting in support of timely risk-based decision-making throughout the organization. The process for developing an ISCM strategy and implementing an ISCM program involves six stages, as shown in Fig. 3.

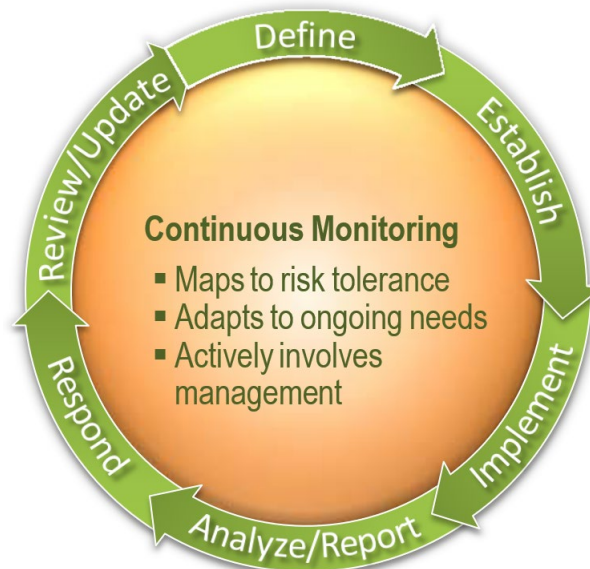


Fig. 3. ISCM Process

1. **Define:** Define a strategy that addresses ISCM requirements and activities at each organizational level (i.e., organization, mission/business processes, and information systems).
2. **Establish:** Determine the metrics, control assessment frequencies, and the ISCM technical architecture. Automate the collection, analysis, and reporting of data where possible as part of the ISCM technical architecture.
3. **Implement:** Collect the security-related information required for metrics, assessments, and reporting.
4. **Analyze:** Analyze the data collected. Report on the effectiveness of the security controls in accordance with organizational requirements. Report on security status monitoring based on predefined measurements and metrics.
5. **Respond:** Address findings with implemented controls following organizational risk response strategies. This may include mitigation, acceptance, transference/sharing, or avoidance/rejection.
6. **Review/Update:** Continually refine the ISCM strategy as the organization's security program matures and/or as objectives, operational environments, and threats change.

6.2. ISCM Roles and Responsibilities

Maintaining an up-to-date view of risk management activities requires involvement across the entire organization, including:

- **Risk executive (function):** Oversees the organization's ISCM strategy and program, reviews status reports from the ISCM process as input to the information security risk posture and risk tolerance decisions, and provides input on the ISCM strategy and requirements
 - **Authorizing official (AO):** Responsible for ensuring that the organization's ISCM program is applied with respect to a given information system
 - **Information system owner (ISO):** Establishes processes and procedures that support the system-level implementation of the organization's ISCM program
 - **Information system security officer (ISSO):** Supports the organization's ISCM program by assisting the ISO in completing ISCM responsibilities and by participating in the configuration management process
- Security control assessor:** Provides input into the types of security-related information gathered as part of ISCM and assesses information system or program management security controls for the organization's ISCM program

7. Detect, Respond, and Recover

An effective risk management program requires the ability to detect and effectively respond to incidents that may compromise organizational systems. These efforts involve the coordination of many people with specific roles and clear responsibilities[SP 800-61r3], including leadership (see Sec. 1.2), incident handlers, technology professionals, asset owners, and personnel in legal offices, public affairs, human resources, and physical security and facilities management. A well-defined incident response plan (see Sec. 7.2) enables organizations to define their capability to detect incidents, minimize loss and destruction, identify weaknesses, and restore operations as quickly as possible.

SP 800-61r3, *Incident Response Recommendations and Considerations for Cyber Risk Management* [SP 800-61r3], describes an incident response model that considers the increased frequency, breadth, and capabilities of modern cybersecurity incidents and recognizes the need to integrate response activities across the organization.

SP 800-160v2r1, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* [SP 800-160v2r1], provides guidelines on developing the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

7.1. Incident Response Life Cycle Model

The incident response life cycle model has three primary stages[SP 800-61r3]:

1. **Detect:** Event and activity logs generated by system assets, network service activities, and personnel activity are analyzed to find anomalies, indicators of compromise, and other potentially adverse events. System auditing capabilities provide the information necessary to establish a baseline for normal operations and deviation thresholds that may indicate aberrant system behavior. System monitoring and vulnerability management (e.g., endpoint detection and response [EDR], security information and event management [SIEM], security orchestration, automation, and response [SOAR], network detection and response [NDR]) tools enable the capture of information about the operating state of system assets, including the identification of exploitable software defects or hardware vulnerabilities, or ongoing attack activities from an advanced persistent threat (APT).
2. **Respond:** When an adverse event is identified, system personnel focus on containing the threat by analyzing its impact and mitigating damage. Detection and response tools may automatically respond to a detected event based on the limits of the tool capability. This includes maintaining active communication with stakeholders, deploying countermeasures, and coordinating efforts with internal teams and external partners.
3. **Recover:** After a cybersecurity incident, critical functions are recovered and activities are returned to normal operations. This typically includes confirming that systems are functioning properly and remediating vulnerabilities to prevent the recurrence of similar adverse events.

1030 The incident response life cycle model in Fig. 4 emphasizes the iterative nature of responding to
1031 and recovering from cybersecurity incidents and calls for continuous improvement.

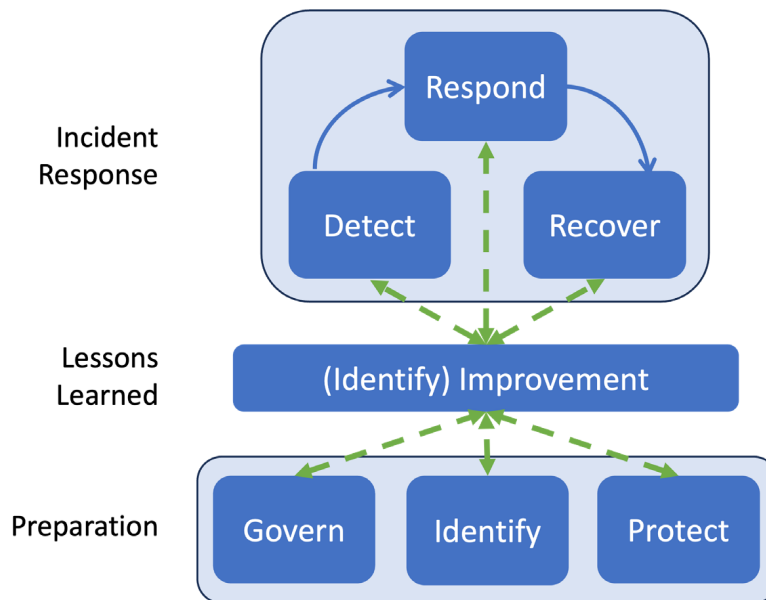


Fig. 4. Incident response life cycle model [SP 800-61r3]

1034 Post-incident activities feed into the preparation stage of incident response to ensure that
1035 organizations account for rapidly evolving threats. This life cycle model greatly emphasizes the
1036 importance of improvement at every stage, including preparation activities. Post-incident
1037 analyses and lessons learned should be incorporated into the organization's practices to
1038 improve detection, response, and recovery capabilities in the future, and response plans should
1039 be updated accordingly.

1040 7.2. Incident Response Plan

1041 While not required, non-federal organizations may benefit from following federal guidance on
1042 incident response. For example, FISMA specifically directs federal agencies to develop and
1043 implement procedures for detecting, reporting, and responding to security incidents [FISMA].
1044 Federal civilian agencies are responsible for reporting all computer security incidents to the
1045 United States Computer Emergency Readiness Team (US-CERT) in the Department of Homeland
1046 Security and for documenting the corrective actions taken and their impact. Policy guidance
1047 issued by the Office of Management and Budget (OMB) in Circular No. A-130, Appendix III
1048 [OMB A-130], requires federal agencies to help users after a system security incident occurs
1049 and to share information concerning common vulnerabilities and threats. Additionally, OMB
1050 Memorandum M-17-12 [OMB M-17-12] requires federal agencies to develop and implement
1051 policies on preparing for and responding to breaches of PII.

1052 An incident response plan documents the organization's structured and systematic approach to
1053 managing cybersecurity incidents[SP 800-61r3]. It includes statements that clearly define its
1054 purpose and objectives, scope, the roles and responsibilities of both internal and external
1055 stakeholders, the types of incidents to be addressed, categorization criteria, response priorities,

communication protocols, and performance measures. Response procedures should describe detailed steps for responding to the most common types of incidents and threats. These procedures may be formatted in a cybersecurity playbook that is organized based on incident categories, such as malware attacks, phishing attempts, data breaches, or insider threats. The Cybersecurity and Infrastructure Security Agency (CISA) provides incident response playbook examples that can be tailored based on the organization's mission and business goals [CISAPB], and [OMB M-17-12] describes procedures for notifying affected individuals and organizations.

Once the plan has been developed, it can be integrated into broader organizational policies and practices in alignment with existing contingency plans (Sec. 5.3) and legal requirements. Successful implementation will require several key elements, including management support, the appropriate tools and technologies for identifying and analyzing potential incidents, regular awareness and training activities (Sec. 5.2), plan testing [CSF 2.0], and ongoing reviews to update the response plan based on emerging threats, lessons learned from past incidents, and organizational changes. Response plan implementation is a dynamic process that requires organizational flexibility to adapt to evolving threats and ensure rapid recovery after an incident.

1072 References

- 1073 [AI RMF] National Institute of Standards and Technology (2023) Artificial Intelligence
1074 Risk Management Framework (AI RMF 1.0). (National Institute of Standards
1075 and Technology, Gaithersburg, MD), NIST Artificial Intelligence (AI) NIST AI
1076 100-1. <https://doi.org/10.6028/NIST.AI.100-1>
- 1077 [CCA] Clinger–Cohen Act of 1996, 40 USC 1401(3).
1078 [https://www.govinfo.gov/content/pkg/USCODE-2011-title40/html/USCODE-](https://www.govinfo.gov/content/pkg/USCODE-2011-title40/html/USCODE-2011-title40-subtitleIII.htm)
1079 [2011-title40-subtitleIII.htm](https://www.govinfo.gov/content/pkg/USCODE-2011-title40/html/USCODE-2011-title40-subtitleIII.htm)
- 1080 [CEA] Cybersecurity Enhancement Act of 2014, Pub. L. 113-274, 128 Stat. 2971.
1081 Available at [https://www.congress.gov/bill/113th-congress/senate-](https://www.congress.gov/bill/113th-congress/senate-bill/1353/text)
1082 [bill/1353/text](https://www.congress.gov/bill/113th-congress/senate-bill/1353/text)
- 1083 [CISAPB] Cybersecurity and Infrastructure Security Agency (2021) Cybersecurity
1084 Incident & Vulnerability Response Playbooks: Operational Procedures for
1085 Planning and Conducting Cybersecurity Incident and Vulnerability Response
1086 Activities in FCEB Information Systems. (Cybersecurity and Infrastructure
1087 Security Agency, Arlington, VA). Available at
1088 [https://www.cisa.gov/sites/default/files/publications/Federal_Government](https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf)
1089 [Cybersecurity Incident and Vulnerability Response Playbooks 508C.pdf](https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf)
- 1090 [CSF 2.0] NIST (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute
1091 of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White
1092 Paper (CSWP) NIST CSWP 29. <https://doi.org/10.6028/NIST.CSWP.29>
- 1093 [FCD1] U.S. Department of Homeland Security (2017) Federal Continuity Directive 1:
1094 Federal Executive Branch National Continuity Program and Requirements.
1095 Available at [https://www.gpo.gov/docs/default-source/accessibility-privacy-](https://www.gpo.gov/docs/default-source/accessibility-privacy-coop-files/January2017FCD1-2.pdf)
1096 [coop-files/January2017FCD1-2.pdf](https://www.gpo.gov/docs/default-source/accessibility-privacy-coop-files/January2017FCD1-2.pdf)
- 1097 [FFMIA] Federal Financial Management Improvement Act of 1996, Pub. L. 104-208,
1098 110 Stat. 3009. Available at
1099 <https://www.congress.gov/104/plaws/publ208/PLAW-104publ208.pdf>
- 1100 [FIPS 200] National Institute of Standards and Technology (2001) Security Requirements
1101 for Cryptographic Modules. (Department of Commerce, Washington, D.C.),
1102 Federal Information Processing Standards Publications (FIPS PUBS) NIST FIPS
1103 200. <https://doi.org/10.6028/NIST.FIPS.200>
- 1104 [FISMA] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128
1105 Stat. 3073. Available at [https://www.govinfo.gov/app/details/PLAW-](https://www.govinfo.gov/app/details/PLAW-113publ283)
1106 [113publ283](https://www.govinfo.gov/app/details/PLAW-113publ283)
- 1107 [FITARA] Federal Information Technology Acquisition Reform Act, H.R. 1232. Available
1108 at <https://www.congress.gov/bill/113th-congress/house-bill/1232>
- 1109 [FMFIA] Federal Managers Financial Integrity Act of 1982, Pub. L. 97-255, 96 Stat. 814.
1110 Available at [https://www.congress.gov/bill/97th-congress/house-](https://www.congress.gov/bill/97th-congress/house-bill/1526/text)
1111 [bill/1526/text](https://www.congress.gov/bill/97th-congress/house-bill/1526/text)
- 1112 [GPRA] Government Performance Results Act of 1993, Pub. L. 103-62, 107 Stat. 285.
1113 Available at [https://www.govinfo.gov/app/details/STATUTE-107/STATUTE-](https://www.govinfo.gov/app/details/STATUTE-107/STATUTE-107-Pg285)
1114 [107-Pg285](https://www.govinfo.gov/app/details/STATUTE-107/STATUTE-107-Pg285)

1115 [GPRAMA] GPRAMA Modernization Act of 2010, Pub. L. 111-352, 124 Stat. 3866. Available
1116 at <https://www.congress.gov/111/plaws/publ352/PLAW-111publ352.pdf>

1117 [IR 8286r1] Quinn S, Chua J, Ivy N, Gardner RK, Kent K, Smith M, Witte G (2025)
1118 Integrating Cybersecurity and Enterprise Risk Management (ERM). (National
1119 Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency
1120 Report (IR) NIST IR 8286r1. <https://doi.org/10.6028/NIST.IR.8286r1>

1121 [IR 8286Ar1] Quinn SD, Ivy N, Barrett M, Feldman L, Witte GA, Gardner RK (2025)
1122 Identifying and Estimating Cybersecurity Risk for Enterprise Risk
1123 Management. (National Institute of Standards and Technology, Gaithersburg,
1124 MD), NIST Interagency Report (IR) NIST IR 8286Ar1.
1125 <https://doi.org/10.6028/NIST.IR.8286Ar1>

1126 [IR 8286Cr1] Quinn SD, Ivy N, Barrett M, Gardner RK, Smith MC, Witte GA (2025) Staging
1127 Cybersecurity Risks for Enterprise Risk Management and Governance
1128 Oversight. (National Institute of Standards and Technology, Gaithersburg,
1129 MD), NIST Interagency Report (IR) NIST IR 8286Cr1.
1130 <https://doi.org/10.6028/NIST.IR.8286Cr1>

1131 [NICE] Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce
1132 Framework for Cybersecurity (NICE Framework). (National Institute of
1133 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
1134 NIST SP 800-181r1. <https://doi.org/10.6028/NIST.SP.800-181r1>

1135 [NIPP] Cybersecurity and Infrastructure Security Agency (2013) National
1136 Infrastructure Protection Plan. (Cybersecurity and Infrastructure Security
1137 Agency, Arlington, VA). Available at
1138 https://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf

1139 [OMB A-123] Office of Management and Budget (2026) Management's Responsibility for
1140 Enterprise Risk Management and Internal Control. (The White House,
1141 Washington, DC), OMB Circular A-123, March 10, 2026. Available at
1142 [https://www.whitehouse.gov/wp-content/uploads/2026/03/OMB-Circular-](https://www.whitehouse.gov/wp-content/uploads/2026/03/OMB-Circular-No.-A-123-2026.pdf)
1143 [No.-A-123-2026.pdf](https://www.whitehouse.gov/wp-content/uploads/2026/03/OMB-Circular-No.-A-123-2026.pdf)

1144 [OMB A-130] Office of Management and Budget (2016) Managing Information as a
1145 Strategic Resource. (The White House, Washington, DC), OMB Circular A-130,
1146 July 28, 2016. Available at [https://www.whitehouse.gov/wp-](https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf)
1147 [content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf](https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf)

1148 [OMB M-17-12] Office of Management and Budget (2017) Preparing for and Responding to a
1149 Breach of Personally Identifiable Information. (The White House,
1150 Washington, DC), OMB Memorandum M-17-12, January 3, 2017. Available at
1151 [https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda](https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf)
1152 [/2017/m-17-12_0.pdf](https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf)

1153 [SP 800-18r2] Licata J, McWhite R, Calloway L, Gilbert D, Anderson M, Snyder J, Miller J
1154 (2025) Developing Security, Privacy, and Cybersecurity Supply Chain Risk
1155 Management Plans for Systems. (National Institute of Standards and
1156 Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-
1157 18r2 ipd. <https://doi.org/10.6028/NIST.SP.800-18r2.ipd>

- 1158 [SP 800-30r1] Joint Task Force (2012) Guide for Conducting Risk Assessments. (National
1159 Institute of Standards and Technology, Gaithersburg, MD), NIST Special
1160 Publication (SP) NIST SP 800-30r1. <https://doi.org/10.6028/NIST.SP.800-30r1>
- 1161 [SP 800-34r1] Swanson M, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency
1162 Planning Guide for Federal Information Systems. (National Institute of
1163 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
1164 NIST SP 800-34r1. <https://doi.org/10.6028/NIST.SP.800-34r1>
- 1165 [SP 800-37r2] Joint Task Force (2018) Risk Management Framework for Information
1166 Systems and Organizations: A System Life Cycle Approach for Security and
1167 Privacy. (National Institute of Standards and Technology, Gaithersburg, MD),
1168 NIST Special Publication (SP) NIST SP 800-37r2.
1169 <https://doi.org/10.6028/NIST.SP.800-37r2>
- 1170 [SP 800-39] Joint Task Force (2011) Managing Information Security Risk: Organization,
1171 Mission, and Information System View. (National Institute of Standards and
1172 Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-39.
1173 <https://doi.org/10.6028/NIST.SP.800-39>
- 1174 [SP 800-47r1] Dempsey K, Pillitteri VY, Regenscheid A (2021) Managing the Security of
1175 Information Exchanges. (National Institute of Standards and Technology,
1176 Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-47r1.
1177 <https://doi.org/10.6028/NIST.SP.800-47r1>
- 1178 [SP 800-50r1] Merritt M, Hansche S, Ellis B, Sanchez-Cherry K, Snyder JN, Walden D (2024)
1179 Building a Cybersecurity and Privacy Learning Program. (National Institute of
1180 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
1181 NIST SP 800-50r1. <https://doi.org/10.6028/NIST.SP.800-50r1>
- 1182 [SP 800-53r5] Joint Task Force (2020) Security and Privacy Controls for Information Systems
1183 and Organizations. (National Institute of Standards and Technology,
1184 Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53r5-upd1,
1185 Includes updates as of September 2020.
1186 <https://doi.org/10.6028/NIST.SP.800-53r5>
- 1187 [SP 800-53B] Joint Task Force (2020) Control Baselines for Information Systems and
1188 Organizations. (National Institute of Standards and Technology,
1189 Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53B, Includes
1190 updates as of October 2020. <https://doi.org/10.6028/NIST.SP.800-53B>
- 1191 [SP 800-55v1] Schroeder K, Trinh H, Pillitteri V (2024) Measurement Guide for Information
1192 Security: Volume 1 — Identifying and Selecting Measures. (National Institute
1193 of Standards and Technology, Gaithersburg, MD), NIST Special Publication
1194 (SP) NIST SP 800-55v1. <https://doi.org/10.6028/NIST.SP.800-55v1>
- 1195 [SP 800-55v2] Schroeder K, Trinh H, Pillitteri V (2024) Measurement Guide for Information
1196 Security: Volume 2 — Developing an Information Security Measurement
1197 Program. (National Institute of Standards and Technology, Gaithersburg,
1198 MD), NIST Special Publication (SP) NIST SP 800-55v2.
1199 <https://doi.org/10.6028/NIST.SP.800-55v2>
- 1200 [SP 800-61r3] Nelson A, Rekhi S, Souppaya M, Scarfone K (2024) Incident Response
1201 Recommendations and Considerations for Cybersecurity Risk Management: A

1202 CSF 2.0 Community Profile. (National Institute of Standards and Technology,
1203 Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-61r3.
1204 <https://doi.org/10.6028/NIST.SP.800-61r3>

1205 [SP 800-84] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006), Guide to Test,
1206 Training, and Exercise Programs for IT Plans and Capabilities, 1.0 (National
1207 Institute of Standards and Technology, Gaithersburg, MD), NIST Special
1208 Publication (SP) NIST SP 800-84. <https://doi.org/10.6028/NIST.SP.800-84>

1209 [SP 800-128] Johnson A, Dempsey K, Ross R, Gupta S, Bailey D (2011) Guide for Security-
1210 Focused Configuration Management of Information Systems. (National
1211 Institute of Standards and Technology, Gaithersburg, MD), NIST Special
1212 Publication (SP) NIST SP 800-128. <https://doi.org/10.6028/NIST.SP.800-128>

1213 [SP 800-137] Dempsey K, Chawla N, Johnson L, Johnston R, Jones A, Orebaugh A, Scholl M,
1214 Stine K (2011) Information Security Continuous Monitoring (ISCM) for
1215 Federal Information Systems and Organizations. (National Institute of
1216 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
1217 NIST SP 800-137. <https://doi.org/10.6028/NIST.SP.800-137>

1218 [SP 800-160v1r1] Ross R, McEvilly M, Winstead M (2022) Engineering Trustworthy Secure
1219 Systems. (National Institute of Standards and Technology, Gaithersburg, MD),
1220 NIST Special Publication (SP) NIST SP 800-160v1r1.
1221 <https://doi.org/10.6028/NIST.SP.800-160v1r1>

1222 [SP 800-160v2r1] Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2021) Developing
1223 Cyber-Resilient Systems: A Systems Security Engineering Approach. (National
1224 Institute of Standards and Technology, Gaithersburg, MD), NIST Special
1225 Publication (SP) NIST SP 800-160v2r1. <https://doi.org/10.6028/NIST.SP.800-160v2r1>

1226 [SP 800-161r1] Boyens J, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M (2022)
1227 Cybersecurity Supply Chain Risk Management Practices for Systems and
1228 Organizations. (National Institute of Standards and Technology,
1229 Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-161r1-upd1,
1230 Includes updates as of November 2024.
1231 <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>

1232 [SP 800-181r1] Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce
1233 Framework for Cybersecurity (NICE Framework). (National Institute of
1234 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
1235 NIST SP 800-181r1. <https://doi.org/10.6028/NIST.SP.800-181r1>

1236 [SP 800-207] Rose S, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture.
1237 (National Institute of Standards and Technology, Gaithersburg, MD), NIST
1238 Special Publication (SP) NIST SP 800-207.
1239 <https://doi.org/10.6028/NIST.SP.800-207>

1240 [SP 800-218] Souppaya M, Scarfone K, Dodson D (2022) Secure Software Development
1241 Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of
1242 Software Vulnerabilities. (National Institute of Standards and Technology,
1243 Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-218.
1244 <https://doi.org/10.6028/NIST.SP.800-218>

1245

1246 [SP 1800-5] Stone M, Irrechukwu C, Perper H, Wynne D (2018) IT Asset Management.
1247 (National Institute of Standards and Technology, Gaithersburg, MD), NIST
1248 Special Publication (SP) NIST SP 1800-5.
1249 <https://doi.org/10.6028/NIST.SP.1800-5>

1250 **Appendix A. List of Symbols, Abbreviations, and Acronyms**

1251 **APG**

1252 Agency Priority Goals

1253 **BIA**

1254 Business Impact Analysis

1255 **BCP**

1256 Business Continuity Plan

1257 **CCA**

1258 Clinger-Cohen Act of 1996

1259 **CCRB**

1260 Configuration Control Review Board

1261 **CIO**

1262 Chief Information Officer

1263 **CIP**

1264 Critical Infrastructure Protection

1265 **CISA**

1266 Cybersecurity and Infrastructure Security Agency

1267 **CISO**

1268 Chief Information Security Officer

1269 **CM**

1270 Configuration Management

1271 **CMVP**

1272 Cryptographic Module Validation Program

1273 **COOP**

1274 Continuity of Operations

1275 **CPIC**

1276 Capital Planning and Investment Control

1277 **CPLP**

1278 Cybersecurity and Privacy Learning Program

1279 **CPRT**

1280 Cybersecurity and Privacy Reference Tool

1281 **C-SCRM**

1282 Cybersecurity Supply Chain Risk Management

1283 **CSO**

1284 Chief Security Officer

1285 **DRP**

1286 Disaster Recovery Plan

1287	EA
1288	Enterprise Architecture
1289	FEA
1290	Federal Enterprise Architecture
1291	FFMIA
1292	Federal Financial Management Improvement Act
1293	FIPS
1294	Federal Information Processing Standard
1295	FISMA
1296	Federal Information Security Modernization Act
1297	FITARA
1298	Federal Information Technology Acquisition Reform Act
1299	GPRA
1300	Government Performance and Results Act
1301	GPRAMA
1302	GPRA Modernization Act of 2010
1303	IDP
1304	Individual Development Plan
1305	IDS
1306	Intrusion Detection System
1307	ISCP
1308	Information System Contingency Plan
1309	ISSO
1310	Information System Security Officer
1311	IT
1312	Information Technology
1313	ITL
1314	Information Technology Laboratory
1315	NICE
1316	National Initiative for Cybersecurity Education
1317	NIST
1318	National Institute of Standards and Technology
1319	NVD
1320	National Vulnerability Database
1321	OEP
1322	Occupant Emergency Plan
1323	OMB
1324	Office of Management and Budget

1325	OPM
1326	Office of Personnel Management
1327	POA&M
1328	Plan of Action and Milestones
1329	RTO
1330	Recovery Time Objective
1331	SDLC
1332	System Development Life Cycle
1333	SIEM
1334	Security Information and Event Management
1335	SP
1336	Special Publication
1337	TKS
1338	Task, Knowledge, and Skill
1339	TT&E
1340	Testing, Training, and Exercises
1341	US-CERT
1342	United States Computer Emergency Readiness Team

1343 **Appendix B. Glossary**

1344 **authorizing official**

1345 Senior (federal) official or executive with the authority to formally assume responsibility for operating an
1346 information system at an acceptable level of risk to organizational operations (including mission, functions, image,
1347 or reputation), organizational assets, individuals, other organizations, and the Nation.

1348 **authorization boundary**

1349 All components of an information system to be authorized for operation by an authorizing official and excludes
1350 separately authorized systems, to which the information system is connected.

1351 **authorization to operate**

1352 Official management decision given by a senior Federal official or officials to authorize operation of an information
1353 system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation),
1354 agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set
1355 of security and privacy controls. [SP 800-53r5]

1356 **configuration management**

1357 A collection of activities focused on establishing and maintaining the integrity of information technology products
1358 and systems, through control of processes for initializing, changing, and monitoring the configurations of those
1359 products and systems throughout the system development life cycle. [SP 800-128]

1360 **continuous monitoring**

1361 Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk
1362 management decisions.

1363 **Cybersecurity Supply Chain Risk Management (C-SCRM)**

1364 A systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the
1365 supply chain and developing risk response strategies to the risks presented by the supplier, the supplied products
1366 and services, or the supply chain.

1367 **enterprise architecture**

1368 The description of an enterprise's entire set of information systems: how they are configured, how they are
1369 integrated, how they interface to the external environment at the enterprise's boundary, how they are operated
1370 to support the enterprise mission, and how they contribute to the enterprise's overall security posture.

1371 **federal enterprise architecture**

1372 A business-based framework for government-wide improvement developed by the Office of Management and
1373 Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered,
1374 results-oriented, and market-based.

1375 **governance**

1376 Activities for managing risks through strategic planning, including establishing and adjusting a risk management
1377 strategy, understanding organizational context, identifying roles and responsibilities, documenting policies, and
1378 managing the organization's supply chain. [CSF 2.0]

1379 **impact**

1380 The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of
1381 information, unauthorized modification of information, unauthorized destruction of information, or loss of
1382 information or information system availability.

1383 **incident response plan**

1384 The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit
1385 consequences of a malicious cyber attacks against an organization's information system(s). [SP 800-34r1]

1386	likelihood
1387	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a
1388	given vulnerability or a set of vulnerabilities.
1389	measurement
1390	The process of obtaining quantitative values using quantitative methods.
1391	measures
1392	Quantifiable and objective values that result from measurement.
1393	metrics
1394	Measures and assessment results designed to track progress, facilitate decision-making, and improve performance
1395	with respect to a set target.
1396	quantitative assessment
1397	The use of a set of methods, principles, or rules for assessing risk based on numbers where the meanings and
1398	proportionality of values are maintained inside and outside of the context of the assessment.
1399	risk appetite
1400	The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.
1401	risk executive (function)
1402	An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for
1403	individual information systems, to include the authorization decisions for those systems, are viewed from an
1404	organization-wide perspective with regard to the overall strategic goals and objectives of the organization in
1405	carrying out its missions and business functions; and (ii) managing risk from individual information systems is
1406	consistent across the organization, reflects organizational risk tolerance, and is considered along with other
1407	organizational risks affecting mission/business success.
1408	risk management strategy
1409	Strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit
1410	and transparent the risk perceptions that organizations routinely use in making both investment and operational
1411	decisions.
1412	risk tolerance
1413	The level of risk an entity is willing to assume to achieve a potential desired result.
1414	system development life cycle
1415	The scope of activities associated with a system, encompassing the system’s initiation, development and
1416	acquisition, implementation, operation and maintenance, and ultimately its disposal.
1417	tailoring
1418	The process by which security control baselines are modified by identifying and designating common controls;
1419	applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined
1420	control parameters; supplementing baselines with additional controls or control enhancements; and providing
1421	additional specification information for control implementation. The tailoring process may also be applied to
1422	privacy controls. [SP 800-37r2]
1423	threat
1424	Any circumstance or event with the potential to adversely impact organizational operations (including mission,
1425	functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an
1426	information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of
1427	service.

1428 **vulnerability**

1429 Weakness in an information system, system security procedures, internal controls, or implementation that could
1430 be exploited or triggered by a threat source.

1431 **zero trust architecture**

1432 An enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships,
1433 workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical
1434 and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture
1435 plan. [SP 800-207]

1436 **Appendix C. Change Log**

1437 This revision of SP 800-100 includes significant changes to the original document, such as:

- 1438 • Reorganization of sections, subsections, and topics to generally follow the CSF 2.0,
1439 namely the Functions and Categories
- 1440 • Reduced the emphasis on a federal government executive audience to make the
1441 publication relevant to executives in a wide variety of organizations
- 1442 • Revised the Governance section to incorporate risk management strategy and
1443 cybersecurity supply chain risk management (C-SCRM)
- 1444 • High-level descriptions of NIST frameworks, including the Risk Management Framework,
1445 Cybersecurity Framework 2.0, NICE Framework, and Privacy Framework
- 1446 • Updated references to NIST publications and relevant legislation

1447

1448