NIST RMF Quick Start Guide
PREPARE STEP
Frequently Asked Questions (FAQs)

NIST Risk Management Framework (RMF) Prepare Step

The addition of the Prepare step is one of the key updates to the Risk Management Framework (NIST Special Publication 800-37, Revision 2 [SP 800-37r2]). The Prepare step was incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes. Tasks in the Prepare step directly support subsequent RMF steps and are largely derived from guidance in other NIST publications or are required by Office of Management and Budget (OMB) policy (or both). Thus, organizations may have already implemented many of the tasks in the Prepare step as part of organization-wide risk management. The Prepare step intends to reduce complexity as organizations implement the Risk Management Framework, promote IT modernization objectives, conserve security and privacy resources, prioritize security activities to focus protection strategies on the most critical assets and systems, and promote privacy protections for individuals. The organization- and system-level risk management activities conducted in the Prepare step are critical for preparing the organization to execute the remaining RMF steps. Without adequate risk management preparation at the organizational and system levels, security and privacy activities can become too costly, demand too many skilled security and privacy professionals, and produce ineffective solutions.

Contents

General Prepare Step FAQs

1. How does the Prepare step impact my organization's current Risk Management Framework implementation?

The Prepare step is not intended to require new or additional activities for security and privacy programs. Rather, it emphasizes the importance of having comprehensive, organization-wide governance and the appropriate resources in place to enable the execution of cost-effective and consistent risk management processes across the organization. Most tasks included in the Prepare step are derived from existing NIST guidance and/or OMB policy requirements and are foundational activities that support the implementation of subsequent Risk Management Framework steps. [Back to Table of Contents]

2. What is the Prepare step?

The purpose of the Prepare step is to carry out essential risk management tasks at the organization, mission and business process, and system levels to establish context and help prepare the organization to manage its security and privacy risks using the Risk Management Framework. Prepare step tasks are completed before the Categorize step and support all subsequent Risk Management Framework steps and tasks. Ultimately, the intention of the Prepare step is to provide the information and resources necessary to successfully manage information security and privacy risk to the organization and its missions from the operation and use of systems. [Back to Table of Contents]

3. What are some of the objectives and benefits of the Prepare step?

The objectives and benefits of the Prepare step include:

- Facilitating better communication between senior leaders and executives at the organization and mission and business process levels and system owners
- Facilitating organization-wide identification of common controls and the development of organizationally tailored control baselines, reducing the workload on individual system owners and the cost of system development and asset protection
- Reducing the complexity of the information technology and operations technology infrastructure using enterprise architecture concepts and models to consolidate, optimize, and standardize organizational systems, applications, and services
- Identifying, prioritizing, and focusing resources on the organization's high-value assets and high impact systems that require increased levels of protection and taking steps commensurate with the risk to such assets. [Back to Table of Contents]

4. What are the outcomes of the Prepare step?

An outcome is a result of a specific task identified in NIST SP 800-37 [SP 800-37r2]. For a listing of outcomes for each task in the Prepare step, refer to Table 1: *Prepare Tasks and Outcomes – Organization Level* and Table 2: *Prepare Tasks and Outcomes – System Level.* [Back to Table of Contents]

5. Who is responsible for conducting the Prepare step tasks?

Each task in the Prepare step identifies the primary role(s) responsible for ensuring the implementation and completion of the task, as well as supporting roles to assist or provide guidance or expertise for task implementation. Refer to the *RMF Roles and Responsibilities Crosswalk* chart for roles and responsibilities associated with the Prepare step tasks. For a description of roles and their associated responsibilities, see Appendix D: *Roles and Responsibilities*. [Back to Table of Contents]

6. Why is the Prepare step separated into organizational level and system level?

The preparatory activities are grouped into organization-level preparation and system-level preparation for ease of use and to clarify appropriate roles and responsibilities. [Back to Table of Contents]

7. Does the Prepare step require new or additional activities for security and privacy programs?

No, the Prepare step tasks are based on existing OMB policy requirements and risk management-related guidance from other NIST publications, including NIST SP 800-30 [SP 800-30], NIST SP 800-39 [SP 800-39], NIST SP 800-137 [SP 800-137], NIST SP 800-160 [SP 800-160], and NISTIR 8062 [IR 8062]. Each task in the Prepare step includes specific references to the task source and supporting publication. [Back to Table of Contents]

8. How does the Prepare step align with the NIST Cybersecurity Framework (CSF)?

To ensure effective and efficient Cybersecurity Framework implementation, several key areas within the RMF have been updated. Each task in the RMF includes references to applicable sections of the Cybersecurity Framework. For example, RMF Prepare – Organization Level step, Task P-2, *Risk Management Strategy*, aligns with the Cybersecurity Framework Core [*Identify Function*]; RMF Prepare—Organization Level step, Task P-4, *Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles*, aligns with the construct of *Cybersecurity Framework Profiles*. [Back to Table of Contents]

9. How does the Prepare step align with the NIST Privacy Framework?

The *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* [NIST PF] provides a simple "ready, set, go" method for establishing or improving a privacy program. The objective of its "*Ready*" phase may be compared to the RMF's *Prepare step* objective in assisting organizations with setting the groundwork for subsequent tasks and Categories/Subcategories to support their risk management processes. Some of the tasks in the Prepare step support certain outcomes in the NIST Privacy Framework and vice versa. The following table provides a mapping between Prepare step tasks and Privacy Framework Categories/Subcategories. For the complete mapping of SP 800-37, Revision 2, to the Privacy Framework, visit the Privacy Framework Resource Repository at https://www.nist.gov/privacy-framework/resource-repository. [Back to Table of Contents]

NIST SP 800-37 Prepare Step Tasks	NIST Privacy Framework Categories/Subcategories
Task P-1, Risk Management Roles	Governance Policies, Processes, and Procedures (**GV.PO-P3** and **GV.PO-P4**) Awareness and Training (**GV.AT-P2** and **GV.AT-P3**) Communication Policies, Processes, and Procedures (**CM.PO-P2**)
Task P-2, Risk Management Strategy	Risk Management Strategy (**GV.RM-P**) Data Processing Ecosystem Risk Management (**ID.DE-P1**)
Task P-3, Risk Assessment – Organization	Risk Assessment (**ID.RA-P**) Monitoring and Review (**GV.MT-P1**)
Task P-4 (optional), Organizationally Tailored Control Baselines and Cybersecurity Framework Profiles	Governance Policies, Processes, and Procedures (**GV.PO-P5**)
Task P-5, Common Control Identification	(none)
Task P-6 (Optional), Impact-Level Prioritization	(none)
Task P-7, Continuous Monitoring Strategy – Organization	(none)
Task P-8, Mission or Business Focus	Business Environment (**ID.BE-P2** and **ID.BE-P3**)
Task P-9, System Stakeholders	Inventory and Mapping (**ID.IM-P2**) Business Environment (**ID.BE-P1**) Risk Assessment (**ID.RA-P1** and **ID.RA-P2**)
Task P-10, Asset Identification	Inventory and Mapping (**ID.IM-P1** and **ID.IM-P2**)
Task P-11, Authorization Boundary	(none)
Task P-12, Information Types	Inventory and Mapping (**ID.IM-P6**)
Task P-13, Information Life Cycle	Inventory and Mapping (**ID.IM-P4** , **ID.IM-P5**, and **ID.IM-P8**) Data Processing Policies, Processes, and Procedures (**GV.PO-P5** and **GV.PO-P6**)
Task P-14, Risk Assessment – System	Risk Assessment (**ID.RA-P4** and **ID.RA-P5**) Monitoring and Review (**GV.MT-P1**)
Task P-15, Requirements Definition	Governance Policies, Processes, and Procedures (**GV.PO-P5** and **GV.PO-P6**)
Task P-16, Enterprise Architecture	Inventory and Mapping (**ID.IM-P7**) Governance Policies, Processes, and Procedures (**GV.PO-P6**)
Task P-17, Requirements Allocation	(none)
Task P-18, System Registration	(none)

10. Are other resources available to help my organization implement the Prepare step?

Each task in the Prepare step includes references to relevant supporting publications that provide additional guidance for task completion. Refer to the NIST FISMA Implementation Project website (https://nist.gov/rmf) for additional resources. [Back to Table of Contents]

11. Why are some tasks in the Prepare step optional?

Prepare Task P-4, *Organizationally Tailored Control Baselines and Cybersecurity Framework Profiles*, and Task P-6, *Impact-Level Prioritization*, are optional. Organizational level Task P-4 is optional because organizations determine the applicability and need for specialized sets of controls (e.g., tailored control baselines) for organization-wide use. Organizations can, at their discretion, use the tailored control baseline concept when there is divergence from the fundamental assumptions used to create the initial control baselines in NIST Special Publication 800-53B [SP 800-53B]. This would include, for example, situations when the organization has specific security and privacy risks, specific mission or business needs, or plans to operate in environments that are not addressed in the initial baselines. Organizationally tailored control baselines can also be developed to streamline the tailoring process across the organization. For example, an organization could develop a tailored baseline that applies to all moderate impact applications within the organization. Organizational level Task P-6 is optional because organizations may determine that additional granularity in their impact designations facilitates risk-based decision making, including the allocation of resources. Organizations can use organizational-level task P-6 to prioritize systems within each impact level. For example, an organization may want to prioritize moderate impact systems by assigning each moderate impact system to one of three more granular moderate impact level subcategories: *low-moderate* systems, *moderate-moderate* systems, and *high-moderate* systems. [Back to Table of Contents]

12. Where does the Prepare step fit into the existing steps of the RMF?

The Prepare step should be completed before the remaining steps or tasks are undertaken since its tasks support subsequent tasks. Organizations implementing the Risk Management Framework for the first time typically carry out the steps in sequential order, starting with the Prepare step. If the system is already in the operations and maintenance phase of the system development life cycle as part of the continuous monitoring step, Prepare step tasks still need to be undertaken for effective risk management. The idea is to ensure that Prepare step tasks are performed even by systems in operations. [Back to Table of Contents]

13. When are security and privacy requirements considered within the system development life cycle?

All federal systems – including operational systems, systems under development, and systems undergoing modifications or upgrades – are in some phase of a system development life cycle. Requirements definition is a critical part of any system development process and begins very early in the life cycle, typically in the initiation phase. Security and privacy requirements are a subset of the overall functional and nonfunctional requirements levied on a system and are incorporated into the system development life cycle simultaneously with the functional and nonfunctional requirements. Without the early integration of security and privacy requirements, significant expenses may be incurred by the organization later in the life cycle to address security and privacy considerations that could have been included in the initial design. When security and privacy requirements are considered as an integral subset of other system requirements, the resulting system has fewer weaknesses and, therefore, fewer vulnerabilities that can be exploited in the future. [Back to Table of Contents]

Prepare Step Fundamentals FAQs

14. What is a risk management strategy, and why is it necessary?

The risk management strategy guides and informs risk-based decisions, including how security and privacy risk is framed, assessed, responded to, and monitored. The risk management strategy makes explicit the threats, assumptions, constraints, priorities, trade-offs, and risk tolerance used for making investment and operational decisions. The strategy includes the strategic-level decisions and considerations for how senior leaders and executives are to manage security, privacy, and supply chain risks to organizational operations and assets, individuals, other organizations, and the Nation. The risk management strategy includes an expression of organizational risk tolerance; acceptable risk assessment methodologies and risk response strategies; a process for consistently evaluating the security,[1] privacy,[2] and supply chain[3] risks across the organization with respect to risk tolerance; and approaches for monitoring risk over time. Security risk management strategy is addressed in NIST SP 800-39 [SP 800-39]. Foundational privacy risk management concepts and considerations that can inform organizations' strategies are provided in NISTIR 8062 [IR 8062]. Supply chain risk management strategy is addressed in NIST SP 800-161 [SP 800-161]. [Back to Table of Contents]

15. What is a risk assessment?

Assessing risk is one of the four components of risk management addressed in the organization's risk management strategy. Risk assessments are used to identify, estimate, and prioritize risk 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 systems. The purpose of security risk assessments is to inform decision makers and support risk responses by identifying (i) relevant threats to organizations or threats directed through organizations against other organizations; (ii) vulnerabilities, both internal and external to organizations; (iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring). NIST SP 800-30 [SP 800-30] provides guidance on conducting risk assessments. Privacy risk assessments are conducted to determine the likelihood that a given operation the system is taking when processing PII could create an adverse effect on individuals and the potential impact on those individuals. NISTIR 8062 [IR 8062] introduces privacy risk management and a privacy risk model for privacy risk assessments. Organizations can use the NIST Privacy Risk Assessment Methodology (PRAM) tool to apply the risk model from NISTIR 8062 and analyze, assess, and prioritize privacy risks. [Back to Table of Contents]

16. What is a Cybersecurity Framework or Privacy Framework profile?

A Profile is a selection of outcomes from the Cybersecurity Framework or Privacy Framework Core based on mission and business functions, security and privacy requirements, and risk determinations. Many of the tasks in the organizational preparation step provide an organization-level view of these considerations (i.e., functions, security and privacy requirements, and risk determinations) and can serve as inputs to a Profile. The resulting prioritized list of cybersecurity and privacy outcomes developed at the organization and mission and business process levels can be helpful in facilitating consistent, risk-based decisions at the system level during the execution of the RMF steps. Profiles can also be used to guide and inform the development of the tailored control baselines described in NIST SP 800-37 [SP 800-37r2] and NIST SP 800-53B [SP 800-53B]. For more information about the Cybersecurity Framework, see [NIST CSF]. For more information about the Privacy Framework, see [NIST PF]. [Back to Table of Contents]

[1] Security risk management strategy is addressed in NIST SP 800-39 [SP 800-39].
[2] Privacy risk management strategy is addressed in NISTIR 8062 [IR 8062].
[3] Supply chain risk management strategy is addressed in NIST SP 800-161 [SP 800-161].

17. What is a common control?

Controls are safeguards to protect the *security* of information and systems as well as the *privacy* of individuals. Common controls are controls provided by a system or non-system entity other than the system-of-interest that can be inherited by one or more organizational systems. Common controls promote more cost-effective and consistent information security across the organization and can also simplify risk management activities. These controls can include, for example, physical and environmental protection controls, boundary protection and monitoring controls, personnel security controls, policies and procedures, acquisition controls, account and identity management controls, audit log and accountability controls, or complaint management controls for receiving privacy-related inquiries from the public. Organizations identify and make available to system owners the set of common controls available for inheritance by organizational systems and allocate those controls to the organizational entities designated as common control providers for implementation and monitoring.

From a system standpoint, inheriting common controls can result in fewer controls to implement (and maintain) and, thus, fewer expenses. Many common controls, however, are actually hybrid controls in which the organization or system offering the controls only provides part of the controls. The system is then responsible for implementing the remaining portion of the common controls. Take, for example, PE-3 PHYSICAL ACCESS CONTROL. A system may be a tenant within a facility managed and operated by a separate organization responsible for the facility, including controlling access to the facility, but the system may still be responsible for the remaining control items that are not offered by the common control provider.

Organizations or entities that offer common controls for inheritance need to ensure that control implementation details are communicated to inheriting systems and that any additional guidance for implementation are provided (e.g., in the case of hybrid controls). Such guidance is beneficial to inheriting systems as well as to control assessors. Any changes to control offerings, including how common controls are implemented, also need to be communicated. Whether common control providers offer controls to the entire organization or to specific systems, it is the responsibility and interest of the inheriting system to ensure that it is informed of any changes to control offerings. There may be cases in which organizations post information on changes to their common control offerings, and it is up to inheriting systems to respond to such changes.

For additional discussion on common controls, see RMF Prepare – Organization Level step, Task P-5, *Common Control Identification*, and NIST SP 800-53 [SP 800-53r5]. [Back to Table of Contents]

18. How are common controls determined for the organization?

The organization-wide process for determining common controls includes considerations of the security categories and impact levels of the systems within the organization; legislative, regulatory, or policy requirements; and the controls necessary to adequately mitigate the security and privacy risks that arise from the use of those systems. When common controls protect multiple organizational systems of differing impact levels, the controls are implemented with regard to the highest impact level among the systems. The allocation of security and privacy requirements to the system and to the environment in which it operates determine which security and privacy controls are designated as common controls. [Back to Table of Contents]

19. Who should define common controls?

The identification of common controls is most effectively accomplished as an organization-wide exercise with the active involvement of the senior agency information security officer, senior agency official for privacy, mission or business owner, senior accountable official for risk management or risk executive (function), chief information officer, authorizing official or authorizing official designated representative, common control provider, and system owner. [Back to Table of Contents]

20. What is an enterprise architecture?

Enterprise architecture[4] is a management practice used by organizations to maximize the effectiveness of mission and business processes and information resources and to achieve mission and business success. An enterprise architecture can help provide a greater understanding of information and operational technologies included in the initial design and development of systems and should be considered a prerequisite for achieving the resiliency and survivability of those systems in the face of increasingly sophisticated threats, as well as for protecting individuals' privacy in light of increasingly complex data processing. Enterprise architecture provides an opportunity for organizations to consolidate, standardize, and optimize information and technology assets. An effectively implemented enterprise architecture produces systems that are more transparent and, therefore, easier to understand and protect. Enterprise architecture also establishes a clear and unambiguous connection from investments to measurable performance improvements. [Back to Table of Contents]

21. What is the difference between security and privacy requirements and security and privacy controls?

The term security and privacy *requirement* is used by different communities and groups in different ways and may require additional explanation to establish the particular contexts for the various use cases. Security and privacy requirements can be stated at a very high level of abstraction, such as in legislation, Executive Orders, directives, policies, standards, and mission and business needs statements. FISMA and FIPS Publication 200 [FIPS 200] articulate requirements at such a level.

Acquisition personnel develop security and privacy requirements for contracting purposes that address the protections necessary to achieve mission and business needs. Systems/security engineers, system developers, and systems integrators develop the security design requirements for the system, develop the system architecture and the architecture-specific derived security and privacy requirements, and subsequently implement specific security functions at the hardware, software, and firmware component level.

Security and privacy requirements are also reflected in various nontechnical security and privacy controls that address such matters as policy and procedures for the management and operational elements within organizations, again at differing levels of detail. It is important to define the context for each use of the term security and privacy requirement so that the respective communities (including individuals responsible for policy, architecture, acquisition, engineering, and mission and business protection) can clearly communicate their intent.

Controls are safeguards – protective mechanisms intended to meet requirements, whether security requirements or privacy requirements. It is important that controls are implemented correctly and working as intended to ensure that the requirements are continuously met. Assessing controls is one method for verifying that requirements are being met. [Back to Table of Contents]

22. What is an authorization boundary?

Authorization boundaries establish the scope of systems to be protected, managed, and authorized for operation or use. Authorization boundaries are determined by authorizing officials with input from the system owner based on mission, management, or budgetary responsibility. Note that the term *system boundary* is no longer used in NIST SP 800-37, Revision 2 [SP 800-37r2]. [Back to Table of Contents]

23. Is the authorization boundary the same as a system boundary?

Historically, NIST has used the terms *authorization boundary* and *system boundary* interchangeably. In the interest of clarity, accuracy, and use of standardized terminology, the term *authorization boundary* is now used exclusively to refer to the set of system

[4] The Federal Enterprise Architecture process is managed by the Office of Management and Budget. [OMB FEA]

elements comprising the system to be authorized for operation or authorized for use by an authorizing official (i.e., the scope of the authorization). Authorization boundary can also refer to a set of common controls to be authorized for inheritance purposes. [Back to Table of Contents]

24. When should the authorization boundary be established?

The authorization boundary is established in Task P-11, *Authorization Boundary*, of the Prepare step – System Level (very early in the system development life cycle). The authorization boundary is established after determining the mission and business processes to be supported by the system and identifying the system stakeholders and the set of assets that require protection but prior to identifying the information types to be processed, stored, or transmitted by the system and conducting a risk assessment. Tasks in the RMF Categorize step and all subsequent RMF steps/tasks cannot be effectively conducted without an established authorization boundary. [Back to Table of Contents]

25. Who is responsible for establishing the authorization boundary?

The authorizing official has the primary responsibility for establishing the authorization boundary with the chief information officer, system owner, mission or business owner, senior agency information security officer, senior agency official for privacy, and enterprise architect serving in supporting roles. The process of establishing boundaries for the organization's systems and determining the associated security authorization implications of those boundaries is an organizational activity that should include careful negotiation among all key participants. After the authorization boundary is established, the information owner/system owner and supporting system security officer are responsible for the overall procurement, development, integration, modification, operation, and maintenance of the system. [Back to Table of Contents]

26. How is the authorization boundary established?

Establishing boundaries for an organization's systems must take into account the organization's mission or business requirements, technical considerations with respect to information security and privacy, programmatic costs to the organization, and the boundaries' effects on authorizing the organization's systems. In order to identify the authorization boundary, the information owner/system owner needs to determine if the information resources:

- Are under the same direct management control;
- Have the same function, mission objective, operating characteristics, and security and privacy needs;
- Process, store, and transmit similar types of information (e.g., categorized at the same impact level); or
- Reside in the same general operating environment (or, in the case of a distributed system, reside in various locations with similar operating environments).

Boundaries that are unnecessarily expansive (i.e., they include too many system components) make the system difficult to manage and the authorization process unwieldy and complex. Boundaries that are unnecessarily limited increase the number of authorizations that must be conducted and inflate the total costs for the organization. For systems processing PII, the privacy and security programs can collaborate to develop a common understanding of authorization boundaries because privacy risks may arise from data processing that occurs beyond what security programs might typically consider the authorization boundary.

Security categories can play an important part in defining appropriate authorization boundaries by partitioning systems according to impact levels and the importance of those systems in carrying out the organization's mission and business processes. The partitioning process facilitates the cost-effective application of controls to achieve adequate security commensurate with the potential adverse impacts that may arise through the respective systems. Data maps created under Task P-13 also help organizations understand where data processing is occurring and how it may affect privacy risks that arise in the systems in order to facilitate the application of appropriate controls. [Back to Table of Contents]

27. What are the various types of information that government systems process?

Systems usually process several types of information. NIST SP 800-60 [SP 800-60v1] divides information into two major categories: information associated with an organization's mission-specific activities and information associated with the administrative, management, and support activities common to most organizations. The business areas that separate government operations into high-level categories can be broken down as follows:

- Mission-based information types:
  - Purpose of government (*services for citizens*)
  - Mechanisms that the government uses to achieve its purpose (*mode of delivery*)
- Management and support information types:
  - Support functions necessary to conduct government operations (*support delivery of services*)
  - Resource management functions that support all areas of the government's business (*management of government resources*)

Mission-based information types are, by definition, specific to individual organizations or groups of organizations, and they are the primary source for determining the privacy risks, security impact values, and privacy engineering and security objectives for mission-based information and systems. The consequences or impacts of unauthorized disclosure of information, breach of integrity, and denial of services are defined by the nature of the two business areas associated with the mission-based information types, which include the following:

- The purpose of government (*services for citizens)* business area describes the mission and purpose of the United States Government in terms of the services it provides both to and on behalf of American citizens. It includes the delivery of citizen-focused, public, and collective goods and benefits as a service, as well as the obligations of the Federal Government to the benefit and protection of the Nation's general population. An example of the *services for citizens* business area is the disaster management line of business that involves the activities required to prepare for, mitigate, respond to, and repair the effects of all disasters, whether natural or human-made. The disaster management line of business includes four information types: 1) disaster monitoring and prediction, 2) disaster preparedness and planning, 3) disaster repair and restore, and 4) emergency response.

- The mechanisms the Government uses to achieve its purpose (*mode of delivery)* business area describes the mechanisms that the Government uses to deliver its services to citizens. An example of the *mode of delivery* business area is the federal financial assistance line of business that provides earned and unearned financial or monetary-like benefits to individuals, groups, or corporations. There are four information types associated with the federal financial assistance line of business: 1) federal grants, 2) direct transfers to individuals, 3) subsidies, and 4) tax credits.

Much of an organization's information and supporting systems are not used to provide direct mission-based services but primarily to support the delivery of services and to manage resources. The two business areas associated with the management and support information types include the following:

- The support functions necessary to conduct government operations (*support delivery of services*) business area provides the critical policy, programmatic, and managerial foundation to support Federal Government operations. An example of the *support delivery of services* business area is the regulatory development line of business that involves activities associated with developing regulations, policies, and guidance to implement laws. The regulatory development line of business includes four information types: 1) policy and guidance development, 2) public comment tracking, 3) regulatory creation, and 4) rule publication.

- The resource management functions that support all areas of the Government's business (*management of government resources*) business area refers to the support activities that enable the Government to operate efficiently. An example of the *management of government resources* business area is the human resource management line of business that involves all activities associated with the recruitment and management of personnel. The human resources management line of business includes ten information types: 1) human resources strategy, 2) staff acquisition, 3) organization and position management, 4) compensation management, 5) benefits management, 6) employee performance management, 7) employee relations, 8) labor relations, 9) separation management, and 10) human resources development.

Each system may process information that does not fall neatly into one of the information types included in NIST SP 800-60, Volume II [SP 800-60v2]. Once a set of information types has been identified for a system, it is prudent to review the actual information processed, stored, or transmitted to determine if additional types of information need to be identified for security and privacy impact assessment purposes. [Back to Table of Contents]

Organizational Support for the Prepare Step FAQs

28. How do organizations establish mission-based information types?

The approach to establishing mission-based information types begins by documenting the organization's mission and business areas. In the case of mission-based information, the information security program office – in coordination with management, technical operations personnel, enterprise architecture, and other stakeholders – compiles a comprehensive set of the organization's mission areas, lines of business, and applicable sub-functions related to the lines of mission and business areas. For example, one organization's mission might be related to economic development. Sub-functions that are part of the organization's economic development mission might include business and industry development, intellectual property protection, or financial sector oversight. Each of these sub-functions represents an information type.

When an organizational information type is not categorized in NIST SP 800-60 [SP 800-60v2], the responsible individuals within the organization must make an initial impact determination based on the FIPS Publication 199 [FIPS 199] categorization criteria defined in Table 1, *Potential Impact Definitions for Security Objectives*. For each information type, each security objective (confidentiality, integrity, and availability) is assigned an impact value (low, moderate, or high) by selecting and adjusting appropriate FIPS Publication 199 Table 1 values.

After the organization's information types have been identified, validated as consistent with the organization's enterprise architecture, and documented, the information security program office prepares a supplement to NIST SP 800-60 [SP 800-60v2] of additional, organization-specific information types, the recommended impact values for each security objective (confidentiality, integrity, and availability), the rationale for each impact value chosen, and the special factors that affect the impact determination for each organization-specific information type. The organization's supplement to NIST SP 800-60 is distributed to information owner/system owners for their use when categorizing their individual systems. [Back to Table of Contents]

29. What are key organizational roles and responsibilities in the Prepare step?

Refer to the *RMF Roles and Responsibilities Crosswalk* chart for key organizational roles and responsibilities. [Back to Table of Contents]

30. What is an organizationally tailored control baseline?

An organizationally tailored control baseline is applied to two or more organizational systems and provides a fully specified set of controls, control enhancements, and supplemental guidance derived from established control baselines described in NIST SP 800-53B [SP 800-53B]. Organizationally tailored baselines complement the initial control baselines by adding or eliminating controls, specifying compensating controls, specifying implementation requirements, and establishing parameter values for assignment or selection statements in controls and control enhancements that are agreeable to organizational communities of interest. Organizationally tailored baselines can also extend the supplemental guidance where necessary. [Back to Table of Contents]

31. What is the source of the new tasks in the Prepare step – Organizational Level?

Prepare step tasks are derived from OMB policy (e.g., OMB Circular A-130 [OMB A130]) and from various NIST risk management-related publications (e.g., FIPS Publication 199 [FIPS 199], NIST SP 800-30 [SP 800-30], NIST SP 800-39 [SP 800-39], NIST SP 800-53 [SP 800-53], NIST SP 800-60 [SP 800-60v1 and SP 800-60v2], NIST SP 800-137 [SP 800-137], NIST SP 800-160 [SP 800-160], NIST SP 800-161 [SP 800-161], and NIST IR 8062 [IR 8062]). [Back to Table of Contents]

System-specific Application of the Prepare Step FAQs

32. Why was the authorization boundary task added?

The authorization boundary task was added because a specific task to determine the authorization boundary did not exist in the previous version of the Risk Management Framework. Determination of the authorization boundary establishes the scope of protection for a system; a system owner is unable to determine the information resources needed without a clear delineation of the authorization boundary. Clear delineation of authorization boundaries is important for accountability, privacy impact assessments, and security categorization, especially in situations where lower-impact systems are connected to higher-impact systems. Furthermore, tasks in the Categorize step and all subsequent RMF steps/tasks cannot be effectively conducted without an established authorization boundary. [Back to Table of Contents]

33. What is the information life cycle?

The information life cycle for personally identifiable information (PII) includes the creation, collection, use, processing, storage, dissemination, maintenance, disclosure, or disposal (i.e., collectively "processing") of PII. A system may need to process PII in whole or in part of its life cycle to achieve the organization's mission or business functions. Identifying and understanding all parts of the information life cycle helps inform the organization's privacy risk assessment and subsequent selection and implementation of controls. [Back to Table of Contents]

34. What is system registration?

System registration, in accordance with organizational policy, serves to inform the governing organization of plans to develop the system or the existence of the system, the key characteristics of the system, and the expected security and privacy implications for the organization due to the ongoing use and operation of the system. In NIST SP 800-37, Revision 1 [SP 800-37r1], system registration was a task in the Categorize step. It was moved into the Prepare step because it provides organizations with an effective management/tracking tool early in the system development life cycle to facilitate the incorporation of the system into the architecture, implementation of protections that are commensurate with risk, and security and privacy posture reporting. [Back to Table of Contents]

35. What is the source of the new tasks in the Prepare step – System Level?

Prepare step tasks are derived from OMB policy (e.g., OMB Circular A-130 [OMB A130]) and various NIST risk management-related publications (e.g., FIPS Publication 199 [FIPS 199], NIST SP 800-30 [SP 800-30], NIST SP 800-39 [SP 800-39], NIST SP 800-53 [SP 800-53], NIST SP 800-60 [SP 800-60v1 and SP 800-60v2], NIST SP 800-137 [SP 800-137], NIST SP 800-160 [SP 800-160], NIST SP 800-161 [SP 800-161], and NIST IR 8062 [IR 8062]). [Back to Table of Contents]

References

[FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

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

[IR 8062] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

[NIST CSF] National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), Version 1.1, April 2018. https://www.nist.gov/cyberframework

[NIST PF] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0 (National Institute of Standards and Technology, Gaithersburg, MD). Available at: https://doi.org/10.6028/NIST.CSWP.01162020

[OMB A130] Office of Management and Budget (2016) *Managing Information as a Strategic Resource*. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[PRAM] NIST Privacy Risk Assessment Methodology (PRAM) https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

[SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-37r1] Joint Task Force (2010) Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 1 [withdrawn]. https://doi.org/10.6028/NIST.SP.800-37r1

[SP 800-37r2] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-53r5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5

[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) 800-53B. https://doi.org/10.6028/NIST.SP.800-53B

[SP 800-60v1] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[SP 800-60v2] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1

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

[SP 800-160v1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[SP 800-161] Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. https://doi.org/10.6028/NIST.SP.800-161

[Back to Table of Contents]