PREPARE STEP FAQS

NIST RISK MANAGEMENT FRAMEWORK, REVISION 2.0

The addition of the Prepare step is one of the key updates to the initial public draft of the RMF 2.0 (SP 800-37 Revision 2). The Prepare step was incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes. Although many organizations are already implementing many tasks in the Prepare step as part of organization-wide risk management, including this guidance in a single publication reduces complexity as organizations implement the RMF, promotes IT modernization objectives, conserves security and privacy resources, prioritizes security activities to focus protection strategies on the most critical assets and systems, and promotes privacy protections for individuals. The organization-wide risk management activities conducted in the Prepare step are critical to 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.

General Prepare Step FAQs

1. How does the Prepare step impact my organization's current RMF 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, enterprise-wide governance and the appropriate resources in place to enable the execution of cost-effective and consistent risk management processes across the organization.

2. What is the Prepare step?

   The purpose of the Prepare step is to carry out essential activities at the organization, mission and business process, and system levels of the organization to establish the context and help prepare the organization to manage its security and privacy risks using the *Risk Management Framework*.

3. What are some of the goals/benefits of the Prepare step?

   The goals and benefits of the Prepare step include:
   - facilitating better communication between senior leaders and executives at the organization and mission/business process levels and system owners;
   - facilitating organization-wide identification of common controls and the development of organization-wide 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 (IT) and operations technology (OT) infrastructure using Enterprise Architecture concepts and models to consolidate, optimize, and standardize organizational systems, applications, and services; and
   - identifying, prioritizing, and focusing resources on the organization's high-value assets and high- impact systems that require increased levels of protection—taking steps commensurate with the risk to such assets.

4. What are the outcomes of the Prepare step?

   Each task of the Prepare step has a specific outcome, found in Table 1: Prepare Tasks and Outcomes – Organization Level and Table 2: Prepare Tasks and Outcomes – System Level. These outcomes include: individuals assigned to key RMF roles; a risk management strategy for the organization, including a determination of organizational risk tolerance; an organization-wide and system-level risk assessment; identification of common controls; an organization-wide strategy for monitoring control effectiveness; and determination of the authorization boundary.

5. Who is responsible for the Prepare step?

   Each task in the Prepare step identifies primary and secondary roles to support implementation at the organizational/mission and business levels and the system level. For a list of roles and their associated responsibilities, see the Roles and Responsibilities table. Ultimately, the intention of the Prepare step is to provide the system owner the information and resources necessary to successfully carry out the RMF.

6. Why is the Prepare Step separated into the Organizational Level and the System Level?

   For ease of use and to clarify the appropriate roles and responsibilities, the preparatory activities are grouped into organization-level preparation and system-level preparation.

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

   No, the Prepare step tasks are based on existing best practice guidance from other NIST Special Publications (SPs), including SP 800-30, SP 800-39, SP 800-137, and SP 800-160. Each task in the Prepare steps includes specific references to the task source publication.

8. How does the Prepare step align with the CSF?

   To ensure an effective and efficient transition to Cybersecurity Framework implementation, the RMF has been modified in this update in several key areas. Each task in the RMF includes references to applicable sections of the Cybersecurity Framework. For example, RMF Prepare—Organization Level step, Task 2, *Risk Management Strategy*, aligns with the Cybersecurity Framework Core [Identify Function]; RMF Prepare—Organization Level step, Task 4, *Organization-Wide Tailored Control Baselines and Profiles*, aligns with the construct of Cybersecurity Framework Profiles.

9. What are other resources to help my organization implement the Prepare step?

   Each task in the Prepare step includes references to relevant supporting publications that provide additional guidance.

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

    Prepare Task 4, *Organization-Wide Tailored Control Baselines and Profiles*, and Task 6, *Impact-Level Prioritization*, are optional. Organizational level Task 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 800-53. This would include, for

example, situations when the organization has specific security and privacy risks, has specific mission or business needs, or plans to operate in environments that are not addressed in the initial baselines. Organizational level Task 6 is optional because organizations may desire additional granularity in their impact designations for risk-based decision making. Organizations can use organizational level task 6 to prioritize systems within each impact level. For example, an organization may want to prioritize moderate-impact systems by assigning each moderate system to one of three new subcategories: *low-moderate* systems, *moderate-moderate* systems, and *high-moderate* systems. This more granular prioritization can be used when allocating resources.

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

    While the RMF steps are listed in sequential order in SP 800-37, they can be carried out in any order. Organizations executing the RMF for the first time typically carry out the steps in sequential order, although they may choose to revisit certain steps during initial execution. Once the system is in the operations and maintenance phase of the SDLC as part of the continuous monitoring step, events may dictate nonsequential execution.

Prepare Step Fundamentals

12. 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, privacy, and supply chain risks across the organization with respect to risk tolerance; and approaches for monitoring risk over time.

13. What is a risk assessment?

    Assessing risk is one of the four components of risk management addressed in the organization's risk management strategy (see FAQ 12). 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 information systems. The purpose of 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) 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).

14. What is a profile?

    A profile is a prioritization of the Cybersecurity Framework Core Categories and/or Subcategory

outcomes based on business/mission functions, security requirements, and risk determinations. Many of the tasks in organizational preparation provide an enterprise-level view of these considerations and can serve as inputs to a profile. The resulting prioritized list of cybersecurity outcomes developed at the organization and mission/business process levels can be helpful in facilitating consistent, risk-based decisions at the system level during the execution of the RMF steps. Profiles, the precursor to control selection in the Cybersecurity Framework, can also be used to guide and inform the development of the tailored control baselines described in SP 800-37 and SP 800-53. For more information about the Cybersecurity Framework, please see: https://www.nist.gov/cyberframework

15. What is a common control?

    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 information systems. Common controls can include, for example, physical and environmental protection controls, system boundary 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 select the set of common controls and allocate those controls to the organizational entities designated as common control providers. Additional information about common controls is provided in SP 800-53.

16. What is an enterprise architecture?

    Enterprise architecture is a management practice used by organizations to maximize the effectiveness of mission/business processes and information resources and to achieve mission and business success. An enterprise architecture can help provide greater understanding of information and operational technologies included in the initial design and development of information systems and should be considered a prerequisite for achieving resilience and survivability of those systems in the face of increasingly sophisticated threats. 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.

17. 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 context for the various use cases. Security requirements can be stated at a very high level of abstraction, for example, in legislation, Executive Orders, directives, policies, standards, and mission/business needs statements. FISMA and FIPS Publication 200 articulate security requirements at such a level.

    Acquisition personnel develop security and privacy requirements for contracting purposes that address the protections necessary to achieve mission/business needs. Systems/security engineers, system developers, and systems integrators develop the security design requirements for the information system, develop the system security architecture and the architecture-specific derived

security 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 at 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 the respective communities (including individuals responsible for policy, architecture, acquisition, engineering, and mission/business protection) can clearly communicate their intent.

18. What is an authorization boundary?

Authorization boundaries establish the scope of protection for information systems (i.e., what the organization agrees to protect under its management control or within the scope of its responsibilities). 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 SP 800-37, Revision 2.*

19. When should the authorization boundary be established?

The authorization boundary is established in Task 4 of the Prepare Step – System Level (very early in the system development life cycle). The authorization boundary is established after determining the missions/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.

20. Who is responsible for establishing the authorization boundary?

The System Owner has the primary responsibility for establishing the authorization boundary with the Chief Information Officer, Authorizing Official or Authorizing Official Designated Representative, Mission or Business Owner, Senior Agency Information Security Officer, Senior Agency Official for Privacy, and Enterprise Architect serving in supporting roles.

Prepare Step – Organizational Level

21. What is an organization-wide tailored control baseline?

An organization-wide control tailored 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 Special Publication 800-53. . Organization-wide 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. Organization-wide baselines can also extend the supplemental guidance where necessary.

22. What is the source of the new tasks in the Prepare Step – Organizational Level?

Each task in the RMF includes a reference to related publications. The Prepare step is not

intended to require new or additional activities for security and privacy programs, but provides a direct linkage to various NIST publications, including the Cybersecurity Framework, FIPS Publication 199, NIST SP 800-30, NIST SP 800-39, NIST SP 800-53, NIST SP 800-53A, NIST SP 800-59, NIST SP 800-60, NIST SP 800-137, NIST SP 800-160, NIST SP 800-161, NIST SP 800-181, NIST IR 8062, and CNSS Instruction 1253.

Prepare Step – System Level

23. Why was the authorization boundary task added?

    The authorization boundary task was added because in the previous version of the RMF, a specific task to determine the authorization boundary did not exist. 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 and for security categorization, especially in situations where lower-impact systems are connected to higher-impact systems.

24. What is the information lifecycle for personally identifiable information (PII)?

    The information life cycle for PII includes the creation, collection, use, processing, storage, dissemination, maintenance, disclosure, or disposal of (i.e., collectively "processing") PII. An information system may need to process PII in whole or in part of its life cycle to achieve the organization's missions 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.

25. 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 SP 800-37, Revision 1, 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 to facilitate incorporation of the system into the enterprise architecture, implementation of protections that are commensurate with risk, and security and privacy posture reporting.

26. What is the source of the new tasks in the Prepare Step – System Level?

    Each task in the RMF includes a reference to related publications. The Prepare step is not intended to require new or additional activities for security and privacy programs, but provides a direct linkage to various NIST publications, include the Cybersecurity Framework, FIPS Publication 199, FIPS Publication 200, NIST SP 800-18, NIST SP 800-30, NIST SP 800-39, NIST SP 800-47, NIST SP 800-53, NIST SP 800-53A, NIST SP 800-59, NIST SP 800-60, NIST SP 800-64, NIST SP 800-122, NIST SP 800-137, NIST SP 800-160, NIST SP 800-161, NIST SP 800-181, NIST IR 8062, NIST IR 8179, CNSS Instruction 1253, NARA CUI Registry, Common Approach to Federal Enterprise Architecture; Federal Enterprise Architecture Framework.