NIST RMF Quick Start Guide

IMPLEMENT STEP

Frequently Asked Questions (FAQs)

NIST Risk Management Framework (RMF) Implement Step

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. After the controls are selected and tailored (as a product of the Select step of the Risk Management Framework), the next step is to implement the controls in accordance with the system security and privacy plans. It is important that the controls are implemented correctly and operate as expected to protect the system. The Implement step focuses on the implementation of the security and privacy controls. The implementation of controls is evaluated for effectiveness in the Assess step of the Risk Management Framework as well as in the Monitor step through continuous monitoring processes.

Contents

General Implement Step FAQs

1. What has been modified from NIST SP 800-37, Rev. 1, to NIST SP 800-37, Rev. 2, for the Implement Step?

The following modifications have been made from NIST SP 800-37, Revision 1 [SP 800-37r1], to NIST SP 800-37, Revision 2 [SP 800-37r2], in the Implement step:

- NIST SP 800-37, Rev. 2, outlines the purpose of the Implement step up front.
- NIST SP 800-37, Rev. 2, provides further guidance on what is expected in the Implementation step in the form of expected outcomes.
- NIST SP 800-37, Rev. 2, requires the implementation of privacy controls according to privacy plans in addition to security plans
- NIST SP 800-37, Rev. 2, identifies additional roles in support of Implementation step tasks.
- NIST SP 800-37, Rev. 2, further breaks down the system development life cycle phase identification according to "new" systems and "existing" systems.
- The task to capture information on planned control implementation is now in the Select step of NIST SP 800-37, Rev. 2, (previously part of the Implementation step of NIST SP 800-37, Rev. 1). The task to capture information on actual (i.e., "as-implemented") state of controls is in the Implement step of NIST SP 800-37, Rev. 2 (Task I-2, *Update Control Implementation Information*).
- Privacy elements and roles for systems processing personally identifiable information have been added as a direct response to Office of Management and Budget (OMB) Circular A-130 [OMB A130], which requires agencies to implement the Risk Management Framework and integrate privacy into the RMF process. In establishing requirements for security and privacy programs, the OMB Circular emphasizes the need for both programs to collaborate on shared objectives. [Back to Table of Contents]

2. Why is security and privacy program collaboration important for control implementation?

The selection and implementation of security and privacy controls reflect the objectives of information security and privacy programs and how those programs manage their respective risks. Depending on the circumstances, these objectives and risks can be independent or overlapping. Federal information security programs are responsible for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized activity or system behavior) to provide confidentiality, integrity, and availability. Those programs are also responsible for managing security risk and for ensuring compliance with applicable security requirements. Federal privacy programs are responsible for managing risks to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal (collectively referred to as "processing") of PII and for ensuring compliance with applicable privacy requirements. When a system processes PII, the information security program and the privacy program have a shared responsibility to manage the security risks for the PII in the system. Due to this overlap in responsibilities, the controls that organizations select to manage these security risks will generally be the same regardless of their designation as security or privacy controls in control baselines or program or system plans. There may also be circumstances in which the selection and implementation of the control or control enhancement affect the ability of a program to achieve its objectives and manage its respective risks. These permutations in the relationship between information security and privacy program objectives and risk management create a need for close collaboration between programs to select and implement the appropriate controls for information systems processing PII.

Organizations consider how to promote and institutionalize collaboration between the two programs to ensure that the objectives of both disciplines are met and that risks are appropriately managed. For example, NIST has released a Security and Privacy Control Collaboration Index Template (Excel & Word) as a supplemental resource for agency use to support security and privacy program collaboration. It is an optional tool to help programs identify the degree of collaboration needed with respect to the implementation of controls in NIST SP 800-53, Revision 5 [SP 800-53r5].

Implement Step Fundamentals FAQs

3. What does control implementation entail?

The implementation of controls involves the establishment of new or the utilization of existing processes, procedures, products, and services to meet the intent of the controls selected in the RMF Select step. The system security and privacy plans serve as guides for implementing the controls and are updated, if necessary, as controls are implemented. [Back to Table of Contents]

4. Who is responsible for control implementation?

The system owner and the common control provider have primary responsibilities for implementing controls. Refer to NIST SP 800-37 for a listing and brief description of other supporting roles (also summarized in the Roles and Responsibilities Crosswalk RMF Quick Start Guide). [Back to Table of Contents]

5. Are external service providers required to implement federal security and privacy requirements and controls?

Yes, FISMA and OMB policy require external providers handling federal information or operating systems on behalf of the Federal Government to meet the same security and privacy requirements as federal agencies. Security and privacy requirements for external providers and controls for systems processing, storing, or transmitting federal information are expressed in appropriate contracts or other formal agreements.

The implementation of controls by external service providers offering cloud products and services may be assessed, authorized, and continuously monitored through the Federal Risk and Authorization Management Program (FedRAMP) [FedRAMP] program. For more information on the FedRAMP program, visit fedramp.gov.

Note that, ultimately, the responsibility for adequately mitigating unacceptable risks that arise from the use of external system services remains with the authorizing official. [Back to Table of Contents]

6. How are controls implemented?

Controls are implemented after they are selected in the Risk Management Framework Select step, which initially occurs during the development or acquisition phase of the system development life cycle. Some of the selected controls may already be in place, such as common controls implemented by the organization. For system-specific control implementation, the system owner determines how the controls are implemented based on security and privacy requirements, organizational risk tolerance, system risk assessment, and system categorization. The following NIST publications provide additional control implementation guidance in support of specific control families and initiatives: NIST SP 800-34 [SP 800-34], NIST SP 800-47 [SP 800-47], NIST SP 800-61 [SP 800-61], and NIST SP 800-128 [SP 800-128]. [Back to Table of Contents]

7. In what order should controls be implemented?

For system-specific control implementation, the system owner determines the control implementation order in collaboration with the security architect, privacy architect, systems security engineer, privacy engineer, information owner, system security officer, and system privacy officer. *Note that Priority Code designations in NIST SP 800-53, Revision 4 [SP 800-53r4], were removed in NIST SP 800-53, Revision 5 [SP 800-53r5], because they ultimately caused confusion for stakeholders.* [Back to Table of Contents]

8. How can implemented controls be validated and verified?

As controls are initially implemented, they can be assessed to ensure that they meet the intent of the control and control specifications in accordance with the system's security and privacy assessment plans. If a control is modified, it is also assessed for effectiveness. The implementation and effectiveness of the controls is then assessed according to the system and/or organization's continuous monitoring plan. Note that, for authorization purposes, systems categorized as moderate or high impact systems are assessed by an independent third-party assessor. For more information, see NIST SP 800-53, Revision 5, CA-2(1) CONTROL ASSESSMENTS | INDEPENDENT ASSESSORS [SP 800-53r5], and NIST SP 800-53B [SP 800-53B]. [Back to Table of Contents]

9. During which phase of the system development life cycle should controls be implemented?

For new systems, controls are implemented during the initial phases of the system development life cycle, including the development/acquisition and implementation/assessment phases. Some systems in development actually perform an initial self-assessment to identify what controls are already in place before implementing any new controls. Existing systems implement new controls and/or update existing (already implemented) controls during the operations/maintenance phase of the system development life cycle. [Back to Table of Contents]

10. Is there any expiration to implemented controls?

Controls are tied to security and privacy requirements captured in the system security and privacy plans as well as to continuous monitoring plans. Controls do not expire, but they can be modified, replaced, or removed, depending on changes to security requirements, privacy requirements, or need. Do not confuse control *expiration* with frequencies recorded as organization-defined control parameters that require certain activities to be performed within a given window of time (e.g., review and update an artifact annually). It is important for implemented controls to be updated as environments change and new threats or privacy risks are identified. [Back to Table of Contents]

11. Can implemented controls be "de-selected"?

Once implemented, controls are expected to be effective in meeting security and privacy requirements. If for any reason they are not, the system owner is expected to respond to the problem, which may or may not result in the "de-selection" (i.e., cancellation or removal) of the control. The "cancellation" may include partial or full removal of the control. Note that changes to the system likely trigger the need for a risk assessment to identify and respond to changes in control implementations that may increase risk. If a control that had already been implemented is removed, then a replacement control is expected to fully or partially meet the control requirement(s) unless in response to a decrease in risk supported by risk assessment results. If the control only partially meets the requirements, then additional compensating controls and/or an acceptance of risk(s) are needed. [Back to Table of Contents]

Organizational Support for the Implement Step FAQs

12. How can organizations support a system's implementation of controls?

Organizations can support a system's implementation of controls by identifying risk management roles and responsibilities, defining organization-level risk management and continuous monitoring strategies, and completing other organization-level tasks (see PREPARE TASKS – ORGANIZATION LEVEL in NIST SP 800-37, Revision 2).

Organizations are also responsible for implementing and supporting the implementation of common controls, as well as organizational policies, processes, and procedures. In addition, organizations may offer enterprise solutions, guidance, and additional resources to all systems under their purview to facilitate meeting organizational requirements and to cut any unnecessary operational costs. [Back to Table of Contents]

System-specific Application of the Implement Step FAQs

13. Can control implementation increase risk to the system?

The implementation of controls may necessitate changes to the system, and changes have the potential to increase risk to the system. For example, consider CM-6 CONFIGURATION SETTINGS, specifically item "b" (i.e., "*The organization implements the configuration settings*"). When applied, certain settings from security configuration checklists may impact the functionality of an information technology product. If this happens, implementing a portion of this control could pose a risk to the system unless the implementation is properly scoped and the risk of not applying the risky setting is identified and acted upon. It is important to ensure that effective configuration management processes are in place to ensure that changes (directly or indirectly caused by control implementation) do not pose unacceptable risks. [Back to Table of Contents]

14. Can controls be partially implemented by the system and partially implemented by another entity?

Yes. This is an example of a hybrid control. Controls may not need to be fully implemented by the system if the system can inherit all or part of a control that is available for inheritance. The selection of an inheritable common control is captured in the system security and privacy plans. [Back to Table of Contents]

15. What happens if common controls cannot meet system requirements for security and/or privacy?

If a common control does not meet system requirements for security and privacy, the system owner may identify and implement compensating controls or choose not to inherit the common control and implement the control as a system-specific control. [Back to Table of Contents]

References

[FedRAMP] General Services Administration, *Federal Risk and Authorization Management Program* (FedRAMP)
https://www.fedramp.gov

[SP 800-34] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010.
https://doi.org/10.6028/NIST.SP.800-34r1

[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 800-47] Grance T, Hash J, Peck S, Smith J, Korow-Diks K (2002) Security Guide for Interconnecting Information Technology Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47.
https://doi.org/10.6028/NIST.SP.800-47

[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 800-61] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

[SP 800-128] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128

[Back to Table of Contents]