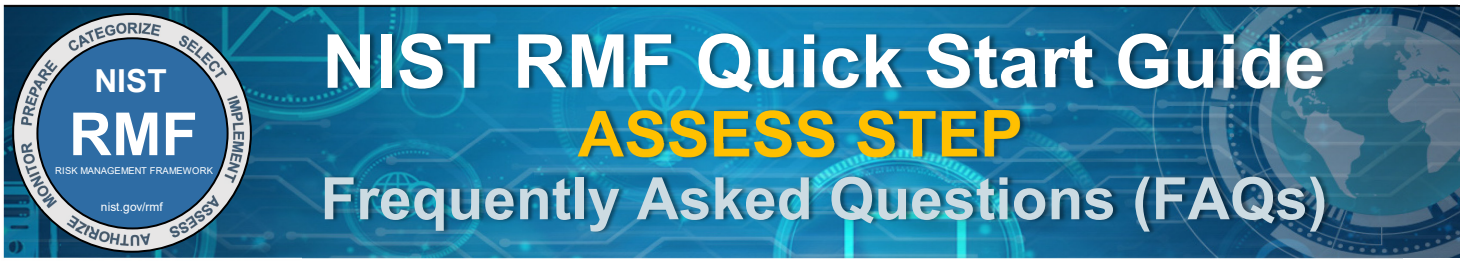
NIST RMF Quick Start Guide
ASSESS STEP
Frequently Asked Questions (FAQs)

NIST Risk Management Framework (RMF) Assess Step

Once security and privacy controls are implemented, they need to be evaluated for correctness and effectiveness. After the initial assessment is completed and the system enters the operations/maintenance phase of the system development life cycle, the controls are assessed on an ongoing basis according to the organization and system's continuous monitoring plans. The ongoing assessment supports the authorizing official's decision to continue or discontinue the system's authorization to operate. Control effectiveness assessments are performed by an independent third-party assessor or assessment team if the system categorization is moderate or high.

Contents



General Assess Step FAQs

1. What has been modified from NIST SP 800-37, Rev. 1, to NIST SP 800-37, Rev. 2, for the Assess 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 Assess step:

- A separate task, Task A-1, *Assessor Selection*, has been created in NIST SP 800-53, Revision 2. Assessor information used to reside in Task 4-1, *Assessment Preparation*, of NIST SP 800-37, Revision 1 [SP 800-37r1].
- Assessor selection and independence have been moved into the Assess Step (Task A-1, *Assessor Selection*) in NIST SP 800-37, Revision 2, from the *Assessment Preparation* task in NIST SP 800-37, Revision 1.
- System Privacy Officer and Senior Agency Official for Privacy responsibilities have been added to Task A-1, *Assessor Selection*, in NIST SP 800-37, Revision 2.
- Security Control Assessment (Task 4-2) in NIST SP 800-37, Revision 1, has been renamed *Control Assessments* (Task A-3) in NIST SP 800-37, Revision 2.
- Task A-3, *Control Assessments*, in NIST SP 800-37, Revision 2, contains information on using the results of control assessments conducted during the system development life cycle phases.
- A separate task, Task A-2, *Assessment Plan*, has been created in NIST SP 800-37, Revision 2. In NIST SP 800-37, Revision 1, this task was the *Assessment Preparation* task (Task 4-1).
- The re-use of information from the assessment controls during the system development life cycle has been moved from Task 4-1, *Assessment Preparation*, in NIST SP 800-37, Revision 1, to Task A-3, *Control Assessments*, in NIST SP 800-37, Revision 2.
- In NIST SP 800-37, Revision 1, Task 4-3, *Security Assessment Report*, has been renamed Task A-4, *Assessment Reports*, in NIST SP 800-37, Revision 2.
- Task 5-1, *Plan of Action and Milestones*, in NIST SP 800-37, Revision 1, has been moved to Task A-6, *Plan of Actions and Milestones*, in NIST SP 800-37, Revision 2.
- Privacy Officer, Privacy Architect, Privacy Engineer, and Senior Agency Official for Privacy roles and responsibilities have been created in NIST SP 800-37, Revision 2.
- Privacy elements and roles for systems that process 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.

For systems and organizations that have adopted RMF 1.0 [SP 800-37r1], these "additional" tasks in the Assess Step are not new. That is, these tasks were previously implied (included in the discussion/supplemental guidance portion of the NIST SP 800-37, Revision 2 [SP 800-37r2]), but they are now explicitly identified. [Back to Table of Contents]

2. What is the purpose of the Assess step?

The purpose of the Assess step is to determine that selected security and privacy controls are implemented correctly, operate as intended, produce the desired outcome, and meet organizational or system security and privacy requirements. In the Assess step, the organization identifies control deficiencies and remediation actions. The Assess step tasks also describe assessor selection, assessment

plan development, control assessments, assessment report development, and plan of action and milestones development and approval. [Back to Table of Contents]

3. What is the outcome of a security and privacy control assessment?

Security and privacy control assessments verify that selected controls are implemented correctly, operating as expected, and recorded appropriately (e.g., in security and privacy plans). The deficiencies in the implementation of security and privacy controls should be prioritized by the potential risks they convey to the system, components, and organization. [Back to Table of Contents]

4. Can results from a previous control assessment be leveraged for (re-)authorization purposes?

It may be possible to leverage recent control assessment results provided that the assessment was conducted according to organizationally accepted assessment methodologies and depending on what was assessed and how much time elapsed since the previous assessment. The security and privacy assessment plans play an important role in validating the recent assessment results. Note, however, that a control assessment is a snapshot in time, meaning that the security and privacy posture captured by the assessment reflects the posture at the time the assessment was performed. For additional guidance on the re-use of assessment results, see NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* [SP 800-53A]. [Back to Table of Contents]

5. Does the control implementation by external product and service providers need to be assessed prior to adoption?

The control implementation by external product and service providers may or may not need to be assessed prior to systems utilizing their products and services. It is dependent on whether the products and services require approval/authorization to be consumed by federal systems and organizations. Cloud services utilized by the Federal Government, for instance, require an active FedRAMP [FedRAMP] authorization. [Back to Table of Contents]

6. What is the relationship between the RMF Assess step and the Monitor step?

New systems (i.e., systems in development) go through each step of the RMF sequentially, so the Monitor step is executed after the Assessment and Authorization steps. Existing systems currently in operations/maintenance phase in the system development life cycle consider the tasks from the Assess step while executing the Monitor step. Assess step tasks are important for monitoring because part of monitoring involves control effectiveness assessments, which support ongoing authorization decisions. [Back to Table of Contents]

Assess Step Fundamentals FAQs

7. Why assess controls?

There are two primary motivations for assessing security and privacy controls: 1) to ensure that the security and privacy controls for managing risk are in place and producing the desired outcomes and 2) to provide the authorizing official with the information needed to make an authorization decision. Control assessment verifies that the safeguards are in place and working as planned, providing system management and Authorizing Officials with an overall security and privacy posture of the system. Control assessments may be conducted as controls are implemented in early stages of the system development in order to identify issues with controls early in the development process. [Back to Table of Contents]

8. What controls are assessed?

All implemented controls are assessed with the frequency of assessment determined by the organization. Control assessments are based on control implementation details captured in security and privacy plans, program management control artifacts, common control artifacts, and any other supporting artifacts that provide control implementation details. The organization- and system-level continuous monitoring plans may also define the frequency of control assessment and level of effort for the assessment. [Back to Table of Contents]

9. Who assesses the controls?

The assessment of security and privacy controls is conducted by assessors who are not only familiar with the Risk Management Framework and the controls in the NIST SP 800-53 [SP 800-53r5] control catalog but are also proficient in conducting control effectiveness assessments per NIST SP 800-53A [SP 800-53A] or equivalent. Preferably, the assessor should understand (or be capable of understanding) the system to be assessed, including its business/mission and operating environment, among other items. It may be necessary for assessors to possess specialized skills or knowledge to help ensure that assessment results are reflective of the actual current system security and privacy posture (e.g., if the system includes database services, the assessor should be knowledgeable about the particular database in use). Controls implemented to achieve both security and privacy objectives may require a degree of collaboration between security and privacy control assessors. An independent, third-party assessor is not required to assess systems categorized as low impact but is required to assess moderate and high impact systems to maintain impartiality.

In accordance with OMB Circular A-130 [OMB A130], the senior agency official for privacy serves as the control assessor for the privacy controls and is responsible for conducting an initial assessment of the privacy controls prior to system operation and for assessing the controls periodically thereafter at a frequency sufficient to ensure compliance with privacy requirements and to manage privacy risks. The senior agency official for privacy can delegate the assessment functions, consistent with applicable policies. An independent evaluation of privacy controls is not required. However, an organization may choose to employ independent privacy assessments at the organization's discretion. [Back to Table of Contents]

10. How are assessors selected?

Assessors are selected for their technical expertise related to the type of system or component they are assessing as well as for their experience in all steps of the Risk Management Framework, including the assessment and authorization steps and the tasks that support them. [Back to Table of Contents]

11. Why is assessor independence important?

Assessors need to be free of any undue influence from officials associated with the systems, components, and organization whose controls are being assessed. Assessors need to make impartial decisions on security and privacy assessment results and provide the authorizing official with unbiased information so that informed risk-based decisions concerning the system and the organization can be made. In accordance with OMB Circular A-130 [OMB A130], an independent evaluation of the privacy program and practices is not required. However, an organization may choose to employ independent privacy assessments at its discretion. 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]

12. Who determines assessor independence?

The authorizing official determines the level of assessor independence required for conducting an unbiased assessment of controls to provide organizational officials with control assessment information that is free of undue influence. Authorizing officials need to trust that assessors produce correct and pertinent assessment information. Assessor independence does not mean that assessors from outside of the organization are needed to conduct the assessment. Internal assessors who are not under the supervision and/or management of the owner of the system being assessed can be employed to conduct the assessment. In accordance with OMB Circular A-130 [OMB

A130], an independent assessment of privacy controls is not required. However, an organization may choose to employ independent privacy control assessments at the organization's discretion. [Back to Table of Contents]

13. What access do assessors need?

For an assessor to conduct an effective and efficient system, component, or organizational security and privacy control assessment, access to information and resources is needed. This includes access to the system, its environment of operation, system documentation, and select personnel (e.g., system owner, security officer, privacy officer, security engineer, privacy engineer, system administrator, network administrator, and application administrator, among other personnel with responsibilities associated with the design, operation, and maintenance of the system or component). Assessors may also need access to system manuals, administrator guides, reports, risk documentation (e.g., plan of action and milestones, risk acceptance artifacts), schematics, system and data flow diagrams, previous control assessment results, and other information and artifacts primarily to support the understanding of the system, mission, and its environment of operation. [Back to Table of Contents]

14. Can organizations conduct self-assessments?

Organizations can conduct self-assessments with two caveats. First, while internal assessors can be employed to conduct self-assessments, assessors should not conduct assessments under the management control of their supervisors. While it may not be considered a conflict of interest, undue influence by supervisors may create scenarios in which deficiency information may be affected. Second, self-assessments can be used to assess low impact systems, while independent assessors should be employed for moderate and high impact systems. Even though self-assessments may be conducted for low impact systems, the assessor's technical expertise and required skills should be at the same level as the assessment for moderate and high impact systems. In accordance with OMB Circular A-130 [OMB A130], an independent assessment of privacy controls is not required. 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]

15. Who develops the security and privacy assessment plans?

Control assessors develop security and privacy assessment plans after reviewing organizational security and privacy plans, organization-approved common controls, and organizational artifacts (e.g., policies, procedures, and other pertinent materials). Organizations may choose to develop a single, integrated security and privacy assessment plan for the system or the organization. [Back to Table of Contents]

16. What information do assessment plans provide?

Assessment plans identify system, component, and organization-related roles and responsibilities, as well as assessment procedures for each security and privacy control. Assessment plans also identify the type of assessment to be conducted, such as development testing, initial authorization, re-authorization, or continuous monitoring. [Back to Table of Contents]

17. Who approves assessment plans?

Assessment plans are reviewed and approved by the authorizing official or the authorizing official designated representative. By approving the plans, the authorizing official or the authorizing official designated representative agree with the level of effort and the resources required to conduct the security and privacy control assessment. [Back to Table of Contents]

18. When/how often should control assessments be conducted?

Controls are assessed as they are implemented and/or modified and at the frequency specified in the system security and privacy plans and/or the organization- and system-level continuous monitoring plans.[1] Security and privacy control assessments can be conducted at any time while a system or component of a system is in production. For example, control assessments can be conducted after a system or component modification (e.g., upgrade) to determine if there is any risk incurred by the new or updated environment. Security and privacy controls may be assessed while the system is being developed (see next question). [Back to Table of Contents]

19. Can controls be applied and assessed during the development process?

Yes, identifying security and privacy requirements, selecting and implementing controls, and assessing implemented controls for effectiveness during the development phase of the system development life cycle (SDLC) is an efficient and effective process for reducing risk to the system, component, and the organization. Controls should be implemented during the development phase of the SDLC to verify that they meet requirements and produce expected outcomes. Conducting control assessments during the development phase of the SDLC provides efficiency as security and privacy requirements are identified and recorded and corresponding controls are identified, implemented, and assessed, thereby reducing risks to the system, component, and organization. Common controls identified prior to system development can also be incorporated into the SDLC. [Back to Table of Contents]

20. Can the results of control assessments conducted during the system development life cycle be used?

Yes, the results of security and privacy control assessments conducted during the system development life cycle (SDLC) can be used for the authorization package. If assessments conducted during the SDLC identify any deficiencies, these can be captured in the security and privacy plans or be mitigated prior to the assessment. If there are no identified deficiencies from assessments conducted during the SDLC, then these security and privacy controls may not need to be re-assessed. [Back to Table of Contents]

21. Can control assessment results be reused?

Control assessment results can be reused if the organization has policies and procedures governing such reuse. Assessment results from the system development life cycle and from assessments conducted by other organizational entities – such as by third parties, vendors, or by other organizations or government agencies – can be reused and incorporated into the assessment results after obtaining approval from appropriate organizational officials. Depending on the system or component operating environment, external assessments, such as those performed for FedRAMP authorizations, can be incorporated into the assessment as well. [Back to Table of Contents]

22. During which phase of the system development life cycle should controls be assessed?

Controls are assessed after they are implemented, before moving to the operational phase, when existing controls are modified, and in the operational phase on an ongoing basis. Controls may be assessed during any phase of the system development life cycle. For example, system owners may opt to perform an initial assessment of controls during early phases of the system development life cycle to obtain a baseline of control effectiveness to avoid the need to re-engineer in later phases. [Back to Table of Contents]

[1] In the past, a three-year control assessment cycle was commonly utilized by systems and organizations. Because of how rapidly a threat to the system (and to an organization) may arise, such a cycle is no longer considered. Instead, a shorter control assessment cycle defined by the organization and coupled with a robust continuous monitoring program needs to be in place to provide more effective risk management.

23. What happens after the controls are assessed?

After control effectiveness is assessed, control assessors produce an assessment report that includes the findings from the assessment. The control assessor presents the assessment results to the authorizing official (and/or authorizing official designated representative) who, in collaboration with the system owner, determines a response to each finding (i.e., mitigate, accept, avoid, or transfer). Findings to be mitigated are captured in plans of action and milestones that are managed by system staff and/or information security program staff. Findings to be accepted, avoided, or transferred remain recorded in the assessment report and are monitored on an ongoing basis for changes in risk factors. [Back to Table of Contents]

24. Why are assessment reports important and who creates the reports?

Security and privacy assessment reports contain important and relevant information for authorizing officials to make risk-based decisions that may or may not lead to the authorization of a system or component to operate. Organizations may develop a single, integrated security and privacy assessment report. These reports include but are not limited to:

- Information about the system or component
- Assessed controls
- Assessment results
- Observed and verified deficiencies
- Mitigation recommendations

Control assessors create control assessment reports that contain information to help determine risks to individuals, the system, components, and/or the organization. [Back to Table of Contents]

25. Can executive summaries be used to provide authorizing officials and other stakeholders control assessment information? What information should be included in the executive summary?

An executive summary can be used to provide authorizing officials and other stakeholders with the results of a control assessment. It should contain information on what was assessed, when it was assessed, any deficiencies identified during the assessment, and any mitigation recommendations for addressing the deficiencies. It is important to include all of the necessary risk information without omission when presenting to authorizing officials. [Back to Table of Contents]

26. What is a plan of action and milestones (POA&M)?

A plan of action and milestones details remediation plans for unacceptable risks identified in security and privacy assessment reports and is one of the artifacts in the authorization package. The plan may include mitigating tasks, resources (e.g., personnel, hardware, software, services, tools, protection mechanisms), milestones, a schedule, and any other information that the system owner may find pertinent to mitigating unacceptable risks. It is reviewed by the authorizing official and used to monitor risk mitigation by tracing back to the actions and milestones as tasks are completed. The development of a plan of action and milestone may also be a result of audits and continuous monitoring and not just a result of a control assessment. [Back to Table of Contents]

27. Who prepares the plan of action and milestones?

Plans of action and milestones (POA&Ms) are prepared and approved by the system owner (and the common control provider) with assistance from personnel with security and privacy responsibilities, such as security officers, privacy officers, system and network administrators, application administrators, and others. System owners may delegate the creation of POA&Ms to other qualified personnel, but the system owners are still the approvers of the POA&Ms. Plan of action and milestones may also be approved by the common control provider, the senior agency information security officer, or the senior agency official for privacy. [Back to Table of Contents]

28. What information is used to develop a plan of action and milestone?

Plans of action and milestones are developed using information collected from risk assessments, audits, inspections, control assessments, testing, continuous monitoring reports, automated scan reports, and other sources. For more information, see Task A-6, *Plan of Action and Milestones*. [Back to Table of Contents]

29. Are plans of action and milestones part of the authorization package?

Plans of action and milestones are part of the authorization package and are presented to the authorizing official. POA&Ms provide information on control deficiencies, possible corrective actions, achievable milestones, and parties responsible for correcting deficiencies. [Back to Table of Contents]

30. Can the authorizing official designated representative accept the plan of action and milestones?

No, the plan of action and milestones can only be accepted by the authorizing official because POA&Ms record deficiencies and are considered risks to individuals, the system, component, and/or organization. Only the authorizing official can accept security and privacy risks and assumes responsibility for the system, component, and common controls. [Back to Table of Contents]

31. What if security and privacy controls are provided by external entities?

If security and privacy controls are provided by external entities, such as through interagency agreements or contracts, it is the organization's responsibility to request and review assessment results as well as any recorded deficiencies and mitigating actions. Copies of plans of action and milestones can be requested and reviewed to enable the authorizing official to make informed, risk-based decisions on whether to accept the assessment results or request another assessment of the controls. [Back to Table of Contents]

32. Can automation be used to conduct control assessments?

Automation can be used to conduct control assessments (that can be automated). Configuration settings, asset inventory management, and patch level (vulnerability) scanning conducted according to organizational policy and schedules efficiently and effectively support continuous monitoring of the security and privacy posture of the systems, components, and organization. Additional NIST initiatives in support of the automation of control assessments include the Automation Support for Control Assessments (see NIST Interagency Report [NISTIR] 8011 [NISTIR 8011] for description), and the Open Security Control Assessments Language (OSCAL) project [OSCAL]. [Back to Table of Contents]

33. Whose responsibility is it to respond to risks from assessment findings?

The system owner is responsible for managing and responding to risks from assessment findings. The system owner is also responsible for implementing mitigation actions in response to assessment findings. [Back to Table of Contents]

34. Who determines remediation actions?

System owners and common control providers determine remediation actions since they are responsible for addressing deficiencies and mitigating risks. They provide the resources required to mitigate the deficiencies and consult with system and component administrators, security and privacy engineers and officers, senior organizational officials, and any other subject matter expert while remediation actions are being considered. Any residual risk is to be reported to the authorizing official. [Back to Table of Contents]

35. Who updates the security and privacy plans after a control assessment?

As controls are assessed (and reassessed), the security and privacy plans are updated by the system owner with new or modified control implementation information post-assessment and post-mitigation to reflect the current security and privacy posture. The updated security and privacy plans identify the most current state of the controls, contain any updates to the implementation details, and capture information on any residual risk identified during the assessments. [Back to Table of Contents]

36. Why are control reassessments conducted?

Controls may be reassessed to verify that deficiencies have been corrected and that controls are implemented correctly and produce the desired outcome. Reassessments can help identify the level of residual risk associated with the system, component, or organization. [Back to Table of Contents]

Organizational Support for the Assess Step FAQs

37. How can organizations support system control assessments?

Organizations can support system control assessments through the provision of enterprise solutions that can automate some of the tasks associated with not only security and privacy control assessments but with risk assessment (e.g., vulnerability assessments). Organization-wide security and privacy solutions may also include governance, risk management, and compliance applications that support assessment and authorization activities (e.g., plan of action and milestone tracking, configuration management tools). In addition to enterprise solutions and enterprise security services, organizations may provide the workforce for supporting control assessments, including independent control assessment teams. [Back to Table of Contents]

System-specific Application of the Assess Step FAQs

38. Is the system owner required to mitigate all risks identified by a control assessment?

All risks must be responded to (i.e., reviewed and analyzed) regardless of whether or not risks will be mitigated. Risk responses include risk acceptance, risk mitigation, risk avoidance, and risk transfer. If the system owner decides not to mitigate a risk for any reason, a decision needs to be made about the risk (e.g., accept, avoid, or transfer the risk). The system owner and the authorizing official work together to determine the appropriate response for each assessment finding of “other than satisfied.” Note that only the authorizing official can accept risks that cannot be mitigated. [Back to Table of Contents]

39. Can control assessments increase risks to the system?

Control assessments are not intended to increase any risk to the system. However, control assessments utilize various methods for evaluating control implementation effectiveness, including automated tools and technical tests that could negatively impact a system depending on how tools are configured or how tests are conducted. Minimizing the risks to individuals and to system confidentiality, integrity, and availability is one of the main motivations for establishing ground rules for control assessments captured in the assessment plans. [Back to Table of Contents]

References

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

[IR 8011] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 1: Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Vol. 1. https://doi.org/10.6028/NIST.IR.8011-1

[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

[OSCAL] Open Security Controls Language (OSCAL) https://nist.gov/oscal

[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 800-53r5] 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 800-53A] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4

[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

[Back to Table of Contents]