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

NIST Risk Management Framework (RMF) Select Step

Security and privacy controls are the safeguards and countermeasures employed within an organizational system to protect the confidentiality, integrity, and availability of the system and its information, as well as the privacy of individuals. Selecting and implementing the appropriate controls for a system are important tasks that can have major implications on the operations and assets of an organization, as well as the welfare of individuals and the Nation.

Contents

General Select Step FAQs 3

1. What has been modified from NIST SP 800-37, Rev. 1, to NIST SP 800-37, Rev. 2, for the Select Step? 3
2. What are security and privacy controls? 3
3. Why are organizations required to select security and privacy controls? 3
4. What is the control selection process? 4
5. Who is responsible for selecting and tailoring the security and privacy controls for a system? 5
6. What is the role of the risk executive (function) in the control selection process? 5
7. When NIST revises NIST SP 800-37 or SP 800-53, is the organization required to implement the changes? 5

Select Step Fundamentals FAQs 5

8. Do all federal systems have to meet the minimum requirements specified in FIPS publication 200? 5
9. What other sources should be reviewed to determine if additional security and privacy requirements apply to a system? 6
10. Must all of the controls in a control baseline be used? 6
11. What if selected controls, control enhancements, and compensating controls are insufficient to mitigate or reduce risk(s) caused by a particular threat source or type of PII processing? 6
12. What are the different approaches to control implementation? 7
13. What are system-specific controls? 7
14. What are common controls? 7
15. What are hybrid controls? 7
16. Who is responsible for common controls or the common portion of hybrid controls? 7
17. How are controls allocated to systems? 8

18. What is the structure of a control? 8
19. Why were program management controls added to NIST SP 800-53? 10
20. Do controls need to be periodically reviewed and updated? 10
21. What type of events can trigger a need to modify or update the controls? 10
Organizational Support for the Select Step FAQs 11
22. What is the relationship between the security and privacy controls and an organization's policies and procedures? 11
23. Why should organizations implement a combination of system-specific, common, and hybrid controls? 11
24. How are program management controls selected? 11
25. What is the security and privacy program plan? 11
26. Can the organization provide templates and tools to assist with preparing security and privacy artifacts? 12
System-specific Application of the Select Step FAQs 12
27. What steps should the system owner follow to select controls for a system? 12
28. What is security categorization and how does it influence the selection of the initial control baseline? 13
29. How is the initial control baseline selected? 14
30. What is tailoring? 14
31. How is scoping guidance applied to the system? 14
32. What are some examples or scenarios of applying the scoping guidance to a system? 15
33. What is a compensating control? 16
34. Under what conditions are compensating controls used? 16
35. What are organization-defined parameters and how are they applied within a system? 16
36. Why do organizations supplement their controls? 17
37. How do system owners supplement their controls? 17
38. Why is information on the selected set of controls captured in security and privacy plans? 17
39. What information is captured in security and privacy plans? 18
40. Do security plans have to follow the format provided in NIST SP 800-18? 18
41. Can security and privacy plans be automatically generated? 18
42. Why are controls monitored? 18
43. What is the continuous monitoring strategy? 19
44. How are controls selected for continuous monitoring? 19
45. Why do security and privacy plans need to be approved? 19
References 20

General Select Step FAQs

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

- A new task, Task S-3, *Control Allocation*, has been created.
- Task 2-1, *Common Control Identification*, moved to the Prepare step as Task P-5 (same title).
- Task 2-2, *Security Control Selection*, from NIST SP 800-37, Revision 1 [SP 800-37r1], is now Task S-1, *Control Selection* in NIST SP 800-37, Revision 2.
- A new task, Task S-2, *Control Tailoring*, has been created. Previously, the control tailoring process was discussed in Task 2-2, *Security Control Selection*.
- A new task, Task S-4, *Documentation of Planned Control Implementations*, has been created. Previously, plan development and plan content were discussed in Task 2-2, *Security Control Selection*.
- A previous task, Task 2-3, *Monitoring Strategy*, in NIST SP 800-37, Revision 1, has been re-named Task S-5, *Continuous Monitoring Strategy – System*.
- A previous task, Task 2-4, *Security Plan Approval*, is now covered by Task S-6, *Plan Review and Approval*.
- addition of privacy elements and roles for systems processing personally identifiable information. Elements of privacy were added to this publication as a direct response to OMB Circular A-130 [OMB A130] which requires agencies to implement the Risk Management Framework, and requires agencies to integrate privacy into the RMF process. In establishing requirements for information security programs and privacy programs, the OMB Circular emphasizes the need for both programs to collaborate on shared or conflicting objectives. [Back to Table of Contents]

2. What are security and privacy controls?

Security controls are the safeguards or countermeasures employed within an organizational system to protect the confidentiality, integrity, and availability of the system and its information. *Privacy controls* are administrative, technical, and physical safeguards employed within an organization to protect an individual, ensure compliance with applicable privacy requirements, and manage privacy risks. [Back to Table of Contents]

3. Why are organizations required to select security and privacy controls?

Organizations are required to adequately mitigate risk arising from the use of information and systems in the execution of mission and business functions. A significant challenge for organizations is to determine the appropriate set of security and privacy controls, which – if implemented and determined to be effective – would most cost-effectively mitigate risk while complying with the security and privacy requirements defined by applicable federal laws, Executive Orders, directives, policies, standards, and regulations (e.g., FISMA, OMB Circular A-130 [OMB A130]). Selecting the appropriate set of security and privacy controls helps to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation and to achieve the objectives of conducting the day-to-day operations of the organization and accomplishing the organization's stated mission and business functions. [Back to Table of Contents]

4. What is the control selection process?

Controls are selected according to security and privacy requirements allocated to the system, system elements, and environment of operation. This allocation of requirements is performed in the Prepare step (Task P-17, *Requirements Allocation*). The control selection process includes, as appropriate:

- Choosing an initial set of controls, including common controls and controls selected from a control baseline or organization-generated controls;
- Tailoring the baseline controls by applying scoping, parameterization (i.e., assigning values to *assignment* and *selection* operations where called within the controls), and compensating control guidance;
- As part of the tailoring process, supplementing the baseline controls with additional controls or control enhancements to address unique organizational needs based on a risk assessment and local conditions, including the environment of operation, organization-specific security and privacy requirements, specific threat information, cost-benefit analysis, or special circumstances; and
- Providing additional details to ensure that control implementation fully meets security and privacy requirements.

In the baseline control selection approach, control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. In the organization-generated control selection approach, the organization uses its own selection process to select the controls. This may be necessary when the system is highly specialized (e.g., a weapons system or a medical device) or has limited purpose or scope (e.g., a smart meter).

For security control selection, the initial set of baseline controls is based on the impact level of the system as determined by the security categorization process. The organization selects one of three sets of baseline security controls from NIST SP 800-53B [SP 800-53B], corresponding to the low-, moderate-, or high-impact rating of the system. After selecting the initial set of baseline security controls, the organization initiates the tailoring process to appropriately modify and more closely align the controls with the specific conditions within the organization (i.e., conditions specific to the system or its environment of operation).

While security controls aim to protect the confidentiality, integrity, and availability of information and systems, privacy controls are intended to safeguard individuals' privacy when systems process personally identifiable information. Therefore, the organization needs to take into consideration the *privacy requirements* for protecting the *individual* during control selection. Such requirements are allocated to the system and to the environment in which the system operates in Task P-17, *Requirements Allocation*, in the Prepare Step.

For privacy control selection, NIST SP 800-53B provides a privacy control baseline for federal agencies to address privacy requirements and manage privacy risks that arise from the processing of personally identifiable information based on privacy program responsibilities under OMB Circular A-130 [OMB A130]. Not all controls or control enhancements may be removed, added, or specialized with tailoring. Organizations conduct privacy risk assessments that consider the nature of the processing of personally identifiable information and its impact on individuals to guide the tailoring of the privacy control baseline for their program and systems.

Additional controls or control enhancements may be necessary to address specific privacy and security requirements and to satisfy the requirements of applicable federal laws, Executive Orders, directives, policies, standards, or regulations. The final determination of the appropriate set of security and privacy controls necessary to provide adequate security and privacy safeguards for a system is a function of the organization's assessment of risk and what is required to sufficiently mitigate the risks. [Back to Table of Contents]

5. Who is responsible for selecting and tailoring the security and privacy controls for a system?

The system owner is responsible for selecting the controls for the system and capturing information on the selected controls in the security and privacy plans. The system owner is responsible for addressing the operational interests of the user community and for ensuring compliance with security and privacy requirements. In addition, the system owner, in conjunction with the system security officer and system privacy officer, is responsible for the development and maintenance of the security and privacy plans and ensures that the system is deployed and operated in accordance with the agreed-upon controls. If the system owner is a common control provider, the common control provider is responsible for selecting and tailoring the controls for the system offering the common controls. [Back to Table of Contents]

6. What is the role of the risk executive (function) in the control selection process?

The risk executive (function) develops a risk management strategy for the organization by providing a strategic view of risks with regard to the organization as a whole and facilitates the sharing of risk-related information among authorizing officials and other senior leaders within the organization. The organizational perspective of risk is considered by the system owner when selecting the appropriate set of controls for the system. The system owner and authorizing official may also wish to consult with the risk executive (function) to help ensure that selected controls support the organizational risk management strategy. [Back to Table of Contents]

7. When NIST revises NIST SP 800-37 or SP 800-53, is the organization required to implement the changes?

NIST does not determine the timeline for federal agency implementation of NIST publications. Per OMB Circular A-130 [OMB A130], "agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within one year of their respective publication dates unless otherwise directed by OMB. The one-year compliance date for revisions to NIST publications applies only to new or updated material in the publications. For systems under development or for legacy systems undergoing significant changes, agencies are expected to meet requirements of, and be in compliance with, NIST standards and guidelines immediately upon deployment of the systems." [Back to Table of Contents]

Select Step Fundamentals FAQs

8. Do all federal systems have to meet the minimum requirements specified in FIPS publication 200?

Yes, FIPS Publication 200 [FIPS 200] specifies the minimum requirements for all information and systems that support the executive agencies of the Federal Government. Organizations meet the minimum requirements in FIPS Publication 200 by selecting the appropriate controls, as described in NIST SP 800-53B [SP 800-53B].

The guidelines in NIST SP 800-53 are applicable to all federal systems other than those systems designated as national security systems, as defined in 44 U.S.C., Section 3542. The guidelines were broadly developed from a technical perspective to complement similar guidelines for national security systems and may be used for such systems with the approval of appropriate federal officials exercising policy authority over such systems. State, local, and tribal governments, as well as private sector organizations, are encouraged to consider using these guidelines, as appropriate. [Back to Table of Contents]

9. What other sources should be reviewed to determine if additional security and privacy requirements apply to a system?

Additional security and privacy requirements may be defined in applicable federal laws, Executive Orders, directives, policies, standards, or regulations. The review of these and other applicable requirements can support the identification of appropriate security and privacy controls to meet the system and organizational requirements.

NIST SP 800-53 [SP 800-53r5] provides a set of controls that can satisfy the breadth and depth of requirements levied on systems and organizations and is consistent with and complementary to other established standards. The catalog of security and privacy controls provided in NIST SP 800-53 can be used to demonstrate compliance with a variety of governmental, organizational, or institutional security and privacy requirements. [Back to Table of Contents]

10. Must all of the controls in a control baseline be used?

OMB Circular A-130 requires federal agencies to employ all controls in the respective security control baselines unless specific exceptions are allowed based on the tailoring guidance provided in NIST SP 800-53B [SP 800-53B]. The current version of OMB Circular A-130 was released prior to the inclusion of a privacy control baseline in SP 800-53B. However, it is important to note that tailoring of control baselines is expected; baseline controls are merely the starting point for the control selection process. Tailoring the control baseline allows the organization to adjust the controls to meet mission and business requirements within the environment of operation. For tailoring guidance and discussion, see NIST SP 800-53B [SP 800-53B][1] and NIST SP 800-37, Revision 2 [SP 800-37r2], Task S-2. [Back to Table of Contents]

11. What if selected controls, control enhancements, and compensating controls are insufficient to mitigate or reduce risk(s) caused by a particular threat source or type of PII processing?

There may be situations in which an organization is employing information technology beyond its ability to adequately protect essential mission and business functions or individuals' privacy (e.g., certain web-based, social networking, and collaborative computing-based technologies). That is, the organization cannot apply effective protective measures within a system to adequately reduce or mitigate risk, even through control enhancements and compensating controls. In those situations, an alternative strategy is needed to prevent the mission and business functions or individuals' privacy from being adversely affected – a strategy that considers the risks that result from an aggressive use of information technology. Restrictions on the types of technologies used and how the system is employed provide an alternative method to reduce or mitigate risk when controls cannot be implemented within technology/resource constraints or when controls lack a reasonable expectation of effectiveness against identified threat sources or types of PII processing. Restrictions on the use of systems and specific information technologies are, in many situations, the only practical or reasonable course of action that an organization can take in order to have the ability to carry out its assigned mission and business functions in the face of determined adversaries or significant privacy risks. Examples of use restrictions include:

- Limiting the information that a system can process, store, or transmit or the manner in which an organizational mission or business function is automated
- Prohibiting external access to organizational information by removing selected system components from the network (i.e., air gapping)
- Prohibiting public access to moderate- or high-impact systems unless an explicit determination is made authorizing such access [Back to Table of Contents]

[1] Starting with NIST SP 800-53, Revision 5, baselines and tailoring guidance are published as NIST SP 800-53B.

12. What are the different approaches to control implementation?

There are three control implementation approaches for systems to employ within an organization:

1. *Common controls* – controls that provide a capability for multiple systems
2. *System-specific controls* – controls that provide a capability for a particular system only
3. *Hybrid controls* – controls that have both system-specific and common characteristics

The organization allocates controls to a system consistent with the organization's enterprise architecture and information security architecture. The organization has significant flexibility in deciding which families of controls or specific controls from selected families in NIST SP 800-53 [SP 800-53r5] are appropriate for the different types of allocations. [Back to Table of Contents]

13. What are system-specific controls?

System-specific controls provide a capability for a particular system only and are the primary responsibility of system owners and their respective authorizing officials. An example of a control that is typically implemented as a system-specific control is IA-6 AUTHENTICATION FEEDBACK, where the system is designed to obscure the feedback of authentication information during the authentication process. [Back to Table of Contents]

14. What are common controls?

Common controls are controls that support multiple systems efficiently and effectively as a common capability. When common controls are selected to support a specific system, they are referenced by that specific system as inherited controls. Many of the controls needed to protect organizational systems (e.g., physical and environmental protection controls, personnel security controls, and incident response controls) are excellent candidates for common control status, as well as technology-based controls (e.g., identification and authentication controls, boundary protection controls, audit and accountability controls, and access controls). For more information on common controls, refer to the *RMF Quick Start Guide: Prepare Step Frequently Asked Questions (FAQs).* [Back to Table of Contents]

15. What are hybrid controls?

Hybrid controls are controls where one part of the control is deemed to be common and another part of the control is deemed to be system-specific. The organization may choose, for example, to implement the AT-2 LITERACY TRAINING AND AWARENESS control as a hybrid control with general, organization-wide security awareness training provided as a common capability and with focused security awareness training provided for the specific system.

Hybrid controls may also serve as templates for further control refinement. For example, the organization may choose to implement control CP-2 CONTINGENCY PLAN by providing a template for a generalized contingency plan for all organizational systems with individual system owners tailoring the plan, where appropriate, for system-specific uses. [Back to Table of Contents]

16. Who is responsible for common controls or the common portion of hybrid controls?

The common control provider is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls or the common portion of hybrid controls. The common control providers are responsible for:

- Capturing information about organization-identified common controls in security and privacy plans (or equivalent document prescribed by the organization),
- Ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the organization,

- Capturing information from assessment findings in a control assessment report, and
- Producing a plan of action and milestones for all controls with weaknesses.

For more information on common controls, refer to the *RMF Quick Start Guide: Prepare Step Frequently Asked Questions (FAQs).*
[Back to Table of Contents]

17. How are controls allocated to systems?

The organization allocates controls to a system consistent with the organization's enterprise architecture, security or privacy architecture, and allocated security and privacy requirements. Control allocation is carried out as an organization-wide activity involving security architects, privacy architects, system security officers, system privacy officers, chief information officers, authorization officials or the authorizing official designated representative, mission or business owner, senior agency information security officer, senior agency official for privacy, system owners, and common control providers. By allocating controls to a system as system-specific controls, hybrid controls, or common controls, the organization assigns responsibility and accountability to specific organizational entities for the overall development, implementation, assessment, authorization, and monitoring of those controls.
[Back to Table of Contents]

18. What is the structure of a control?

The control structure consists of the following parts:

- Control section (for base controls and control enhancements),
- Discussion section,[2]
- Related controls section,
- Control enhancements section, and
- References section.

[2] The *Supplemental Guidance* section in NIST SP 800-53, Revision 4, is renamed *Discussion* in NIST SP 800-53, Revision 5.

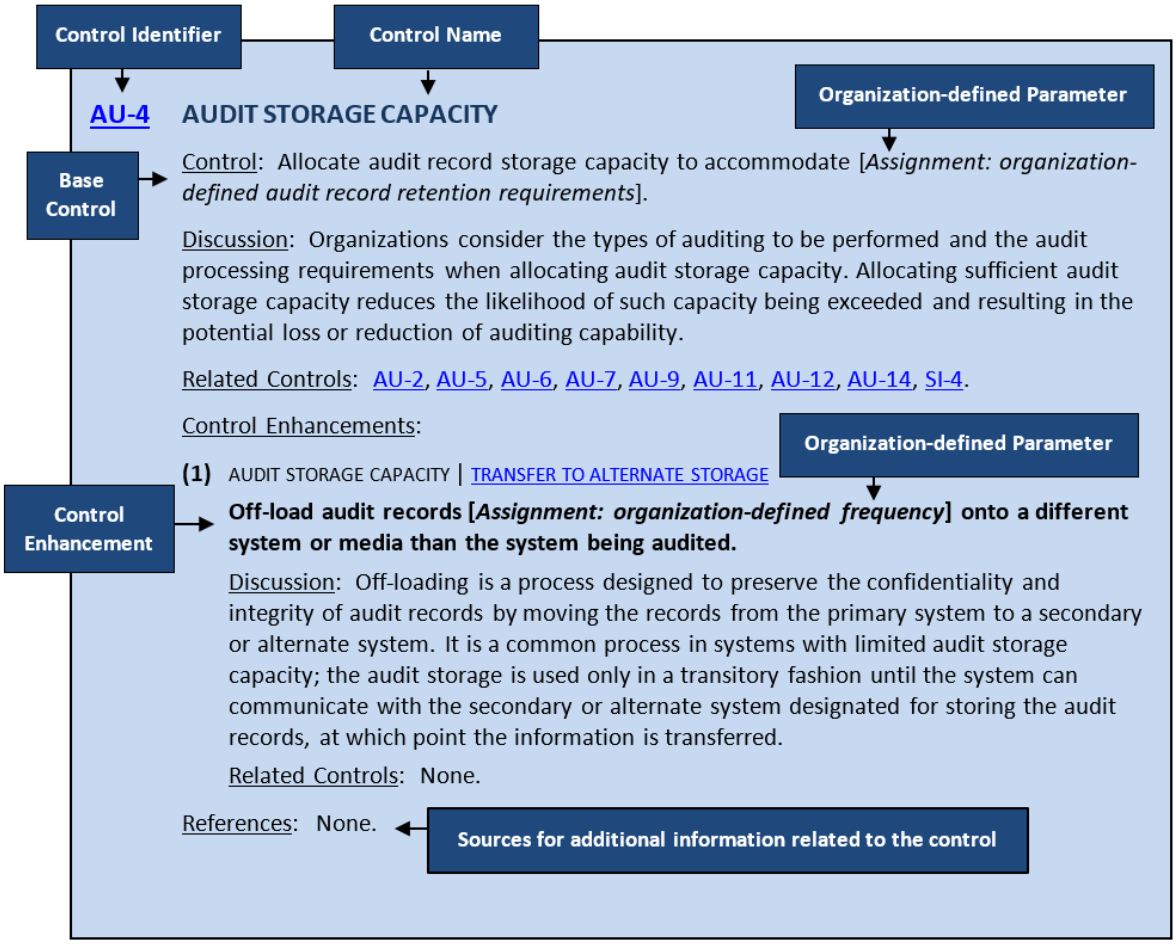

Figure 1 Control Structure (from NIST SP 800-53, Revision 5)

The control section (for base controls and control enhancements) provides a concise statement of the specific security or privacy capabilities that need to be implemented. The control statement describes specific activities or actions to be carried out by the organization or the system. The discussion section provides additional information related to a specific control but contains no requirements. The control enhancements section provides statements about security and privacy capability to build in additional functionality to a base control or increase the strength of a base control. In both cases, the control enhancements are used when organizations seek additions to the basic control functionality based on the results of a risk assessment or in a system that requires greater protection due to the potential impact of loss. The references section includes a list of applicable federal laws, Executive Orders, directives, policies, standards, and guidelines that are relevant to a particular control or control enhancement.

For some controls in the control catalog, organizations are allowed a degree of flexibility to selectively define input values for certain parameters associated with the controls. This flexibility is achieved through the use of assignment and selection operations within the control. Assignment and selection operations provide an opportunity for an organization to tailor the controls to support specific mission, business, or operational needs. For example, an organization can specify the actions to be taken by the system in the event of an audit processing failure, the specific events to be audited within the system, the frequency of conducting system backups, restrictions on password use, or the distribution list for organizational policies and procedures. [Back to Table of Contents]

19. Why were program management controls added to NIST SP 800-53?

Federal agencies are required to develop, implement, and provide oversight for organization-wide security and privacy programs to help ensure the confidentiality, integrity, and availability of federal information processed, stored, and transmitted by federal systems and to protect individual privacy. The information security program management controls, originally listed in Appendix G and a number of privacy controls originally listed in Appendix J of NIST SP 800-53, Revision 4 [SP 800-53r4], are incorporated into the main security and privacy control catalog starting with NIST SP 800-53, Revision 5 [SP 800-53r5]. The program management controls focus on the organization-wide information security and privacy requirements that are independent of any particular system but are essential for managing security and privacy programs. Organizations are required to implement program management controls to provide a foundation for the organization's security and privacy programs. The successful implementation of security and privacy controls for organizational systems depends on the successful implementation of the organization's program management controls. [Back to Table of Contents]

20. Do controls need to be periodically reviewed and updated?

Yes, the organization initiates specific follow-on actions as part of a comprehensive continuous monitoring program after the system is authorized for operation in accordance with the organization's risk management strategy. The continuous monitoring strategy includes an ongoing assessment of control effectiveness to determine if there is a need to modify or update the current deployed set of controls based on changes in the system or its environment of operation. If this is the case, a re-selection of controls may be needed, which would include performing one or more steps in the control selection process. [Back to Table of Contents]

21. What type of events can trigger a need to modify or update the controls?

Events may occur that can trigger the immediate need to assess the state of the system and, if required, modify or update the current controls. These events include but are not limited to:

- An incident results in a breach to the system, producing a loss of confidence by the organization in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system.
- A newly identified, credible, system-related threat to organizational operations and assets, individuals, other organizations, or the Nation is identified based on intelligence information, law enforcement information, or other credible sources of information.
- Significant changes to the configuration of the system through the removal or addition of new or upgraded hardware, software, or firmware or changes in the operational environment potentially degrade the security or privacy state of the system.
- Significant changes are made to the organizational risk management strategy, security and privacy policy, supported mission or business functions, or information being processed, stored, or transmitted by the system.

When events trigger the need to reassess, modify, or update controls, organizations should – at a minimum – take the following actions:

- Reconfirm the security category and impact level of the system;
- Assess the current state of the system and the risk to organizational operations and assets, individuals, other organizations, and the Nation;
- Plan for and initiate any necessary correction actions; and
- Consider reauthorizing the system. [Back to Table of Contents]

Organizational Support for the Select Step FAQs

22. What is the relationship between the security and privacy controls and an organization's policies and procedures?

An organization's security and privacy policies and procedures should extend the FIPS Publication 200 [FIPS 200] requirements and NIST SP 800-53 [SP 800-53r5] security and privacy controls to their specific organizations by providing implementation guidance and organization-specific restrictions.

The use of security and privacy controls from NIST SP 800-53 [SP 800-53r5] and the incorporation of tailored baseline controls from NIST SP 800-53B [SP 800-53B] as a starting point in the control selection process facilitate a more consistent level of protection across federal systems and organizations. It also offers the needed flexibility to appropriately modify the controls based on specific organizational policies and requirements, particular conditions and circumstances, known threat and vulnerability information, and tolerance for risk. [Back to Table of Contents]

23. Why should organizations implement a combination of system-specific, common, and hybrid controls?

Allocating implementation approaches for controls into common, hybrid, and system-specific controls can result in significant savings to the organization in implementation and assessment costs, as well as a more consistent application of the controls across the organization. While the concept of control allocation into common, hybrid, and system-specific controls is straightforward and intuitive, the application within an organization takes significant planning and coordination. [Back to Table of Contents]

24. How are program management controls selected?

Organizations specify the individuals within the organization who are responsible for the development, implementation, assessment, authorization, and monitoring of the Program Management (PM) controls. The PM controls are implemented at the organization level, are not directed at individual systems, are independent of the FIPS 200 [FIPS 200] impact levels, and are not associated with the control baselines described in NIST SP 800-53B [SP 800-53B]. Organizations capture information about the program management controls in the security and privacy program plan. The organization-wide security and privacy program plan supplements the individual security and privacy plans developed for each organizational system. Together, the security and privacy plans for the individual systems and the security and privacy program cover the totality of controls employed by the organization. [Back to Table of Contents]

25. What is the security and privacy program plan?

The information security program plan captures information about the organization-wide program management controls and organization-defined common controls. The information security program plan can be represented in a single artifact or compilation of artifacts at the discretion of the organization. The privacy program provides an overview of the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. Together, the security and privacy plans, which can be consolidated into one plan or maintained as separate plans, for individual systems and the organization-wide security and privacy program plans provide complete coverage for all controls employed within the organization. Common control information is captured in an appendix to the organization's program plan unless the controls are included in a separate security and privacy plan for a system (e.g., controls employed as part of an intrusion detection system that provides organization-wide boundary protection inherited by one or more organizational systems). The organization-wide program plan indicates which separate security and privacy plans, if any, contain descriptions of common controls. [Back to Table of Contents]

26. Can the organization provide templates and tools to assist with preparing security and privacy artifacts?

Yes, the organization can provide templates and tools to assist in the preparation of security and privacy artifacts. An organizational approach to developing and implementing artifact templates (e.g., security and privacy plans, contingency plan, incident response plan) or to selecting automated tools that support the control assessment process and the development of artifacts establishes expectations for artifacts that lead to greater consistency in the organization's approach to control assessments. Providing artifact templates or automated tools for the organization establishes clear expectations about what is required for each artifact, including the level of detail that should be included.

Automated tools are important to support consistency in the development of artifacts and the control assessment process. When organizations have the resources necessary to acquire and implement automated tools, the organization further simplifies the development of artifacts and the control assessment process. NIST is currently developing machine-readable representations of control catalogs, control baselines, security and privacy plans, and assessment plans with its Open Security Controls Assessment Language (OSCAL) [OSCAL]. Among other applications, OSCAL can be used to automate the generation of an artifact. [Back to Table of Contents]

System-specific Application of the Select Step FAQs

27. What steps should the system owner follow to select controls for a system?

To determine the appropriate controls for the system and the environment of operation, the system owner selects the initial control baseline (based on the categorization process for security control baselines or organization-generated control selection), tailors and supplements the controls based on the risk assessment, allocates controls, and captures the results in the security and privacy plans.

Select the Initial Control Set

If the controls are selected from an initial baseline, the system owner identifies the initial set of controls once the system's impact level is determined during the security categorization process. The initial set of controls is selected from the corresponding *low*, *moderate*, or *high* baselines and initial privacy control baseline in NIST SP 800-53B [SP 800-53B]. *Note that if the organization uses an organizational-generated control selection method, the following steps still apply.*

Tailor the Controls

Identify and select common controls in the initial baselines and apply scoping considerations to remaining controls. Scoping guidance provides organizations with specific terms and conditions on the applicability and implementation of individual control baselines. The system owner follows the scoping guidance considerations and directions on how to apply them to systems, as described in NIST SP 800-53B, Section 2.4.

Compensating controls are another method for tailoring the system's controls. A compensating control is a management, operational, or technical control used by an organization instead of a recommended control from a control baseline (or organization-generated control set) that provides equivalent or comparable protection for a system.

Controls that contain organization-defined parameters (i.e., Assignment or Selection operations) give organizations the flexibility to define selected portions of the controls to support specific organizational requirements or objectives. Where specified, minimum and maximum values are prescribed by applicable laws, Executive Orders, directives, policies, standards, or regulations or are indicated by the risk assessment in order to adequately mitigate risk.

The tailored control baseline should be viewed as the foundation or starting point for determining the needed set of controls for a system. The system owner uses the risk assessment results to determine the sufficiency of the controls in the tailored baseline (i.e., whether or not the controls adequately protect the organization's operations and assets, individuals, other organizations, and the Nation). In many cases, additional controls or control enhancements may be needed to address security and privacy requirements or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations.

Allocate Controls

Once controls are selected and tailored, system-specific controls are allocated to the individual system elements so that they can meet their security and privacy requirements, although not all controls are necessarily allocated to every system element. Control allocation is based on the need to provide a specific security or privacy capability to a given system element. Therefore, controls are allocated to system elements based on the security and privacy requirements allocated to the system, system elements, and the environment of operation.

Capture Information on Planned Control Implementation in Security and Privacy Plans

The system owner captures the decisions made during the initial control selection, tailoring, and supplementation processes, providing a sound rationale for those decisions in individual or consolidated plans for security and privacy. This information is essential when examining the overall security and privacy considerations for systems with respect to potential mission or business case impact. Special care should be taken when reviewing inheritable controls (from other systems or organizations) that are hybrid controls: ensure that the system portion of the control implementation statements are complete and address the selected controls/control enhancements.

Develop a Continuous Monitoring Strategy

The system owner initiates development of the continuous monitoring strategy to manage the ongoing monitoring of management, operational, and technical controls employed within or inherited by a system. An ongoing monitoring program allows an organization to track the state of a system on a continuous basis and, over time, maintain the authorization for the system. Note that the continuous monitoring strategy of systems is consistent with and supplements the continuous monitoring strategy for the organization.

Obtain Approval for Security and Privacy Plans

The authorizing official determines if the plan is complete, consistent, and satisfies the stated security and privacy requirements for the system. Complete coverage of controls in appropriate plans facilitates more comprehensive information security, promotes increased accountability, provides an effective vehicle to better manage the risks that result from the operation and use of systems, and is required to adequately support the assessment of systems as part of the authorization process. [Back to Table of Contents]

28. What is security categorization and how does it influence the selection of the initial control baseline?

FIPS Publication 199 [FIPS 199] requires organizations to categorize their systems as low-, moderate-, or high-impact for the security objectives of confidentiality, integrity, or availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high watermark) for each type of information processed, stored, or transmitted by those systems.

The high watermark concept is also used to determine the impact level of the system for the express purpose of selecting an initial set of controls from one of the three security control baselines in NIST SP 800-53B [SP 800-53B]. Thus, a low-impact system is defined as a system in which all three of the security objectives are low. A moderate-impact system is a system in which at least one of the security objectives is moderate and no security objective is greater than moderate. Finally, a high-impact system is a system in which at least one security objective is high. [Back to Table of Contents]

29. How is the initial control baseline selected?

The selection of the initial set of baseline security controls is based on the impact level of the system as determined by the categorization process. The organization selects one of three sets of baseline security controls and initial privacy baselines for federal agencies from NIST SP 800-53B [SP 800-53B] that correspond to the low-, moderate-, or high-impact rating of the system. Note that not all controls from NIST SP 800-53 [SP 800-53r5] are assigned to baselines (as indicated by the phrase *not selected*), and not all control enhancements are assigned to baselines (as indicated by the control being *not selected* or the enhancement number, enclosed in parenthesis, not appearing in any baseline). [Back to Table of Contents]

30. What is tailoring?

The system owner tailors and more closely aligns the controls with the specific conditions within the organization (i.e., conditions specific to the system or its environment of operation). The tailoring process includes:

- Identifying and designating common controls in the control baselines;
- Applying scoping considerations to the remaining baseline controls;
- Selecting (or specifying) compensating controls, if needed, to adjust the preliminary set of controls to obtain an equivalent set deemed to be more feasible to implement;
- Assigning specific values to organization-defined control parameters using either assignment of selection statements; and
- Providing specification information for control implementation.

Organizations have the flexibility to perform the tailoring process at the organization level for all systems (either as the required tailored baseline or as the starting point for system-specific tailoring), at the individual system level, or using a combination of organization-level and system-specific approaches. Tailoring decisions for all affected controls in the selected baseline, including the specific rationale for those decisions, are captured in the security and privacy plans for the system and approved by appropriate organizational officials as part of the security and privacy plan approval process. [Back to Table of Contents]

31. How is scoping guidance applied to the system?

Scoping guidance in NIST SP 800-53B [SP 800-53B] provides organizations with specific terms and conditions on the applicability and implementation of individual controls in the control baselines. The application of scoping guidance helps to ensure that organizations implement only those controls that are essential to providing the appropriate level of protection for the system based on specific mission or business requirements and particular environments of operation. There are several scoping considerations that can potentially affect how the baseline controls are applied and implemented by organizations, such as:

- Control implementation, applicability, and placement considerations
- Operational and environmental considerations
- Technology considerations
- Mission and business considerations
- Security objective considerations
- Legal and policy considerations [Back to Table of Contents]

32. What are some examples or scenarios of applying the scoping guidance to a system?

Several examples and scenarios for applying the scoping guidance to a system are described below (from [SP 800-53B]).

Security Objective Considerations

Security controls that support only one or two of the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS Publication 199 [FIPS 199] security category for the supported security objectives before moving to the FIPS Publication 200 [FIPS 200] impact level, (ii) is supported by an organizational assessment of risk, and (iii) does not adversely affect the level of protection for the security-relevant information within the system. Downgrading actions apply only to the moderate and high baselines.

The following controls are recommended candidates for downgrading:

- Confidentiality: AC-21, MA-3(3), MP-3(3), MP-4, MP-5, MP-6(1), MP-6(2), PE-4, PE-5, SC-4
- Integrity: CM-5, CM-5(1), CM-5(3), SI-7, SI-7(1), SI-7(5), SI-10
- Availability: CP-2(1), CP-2(2), CP-2(3), CP-2(5), CP-2(8), CP-3(1), CP-4(1), CP-4(2), CP-6, CP-6(1), CP-6(2), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-7(6), CP-8, CP-8(1), CP-8(2), CP-8(3), CP-8(4), CP-8(5), CP-9(2), CP-9(3), CP-9(5), CP-9(6), CP-10(2), CP-10(4), CP-11, MA-6, PE-9, PE-10, PE-11, PE-11(1), PE-13(1), PE-13(2), PE-15(1)

A scenario includes:

- System ABC has the following security category:

  SC_{ABC} = {(confidentiality, moderate), (integrity, high), (availability, low)}.
- Therefore, the impact level for the system is high based on the high watermark concept since the value for the integrity security objective is high.
- While the impact level for the system is high because the value for the integrity security objective is high, the values for the confidentiality security objective are moderate, and the availability security objective is low.
- Based on the scoping guidance in NIST SP 800-53B, the controls that uniquely support the confidentiality and availability objectives may be selected for downgrading if the downgrading action is consistent with the conditions defined in NIST SP 800-53B (and above).

Technology Considerations

Controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the system. Controls that can be supported by automated mechanisms do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. If automated mechanisms are not readily available, cost-effective, or technically feasible, compensating controls implemented through non-automated mechanisms or procedures are used to satisfy specified security and privacy control requirements. Examples include:

- Systems that do not implement wireless technology do not need controls for wireless access restrictions.
- If a system does not employ public key infrastructure technologies, public key certificates do not need to be issued or managed.
- Automated mechanisms may be required to maintain up-to-date, complete, accurate, and easily available baseline configurations of organizational systems. If automated mechanisms are not available, compensating controls may be implemented to satisfy the control.

Legal and Policy Considerations

Controls that address matters governed by applicable federal laws, Executive Orders, directives, policies, standards, or regulations (e.g., privacy impact assessments) cannot be tailored out unless the employment of those controls is consistent with the types of information and systems covered by the applicable laws, Executive Orders, directives, policies, standards, or regulations.

For example, as defined in OMB Memorandum 03-22 [OMB M-03-22], federal agencies are required to conduct a privacy impact assessment on a system before developing or procuring information technology systems or projects that collect, maintain, or disseminate information in an identifiable form from or about members of the public or before initiating – consistent with the Paperwork Reduction Act – a new electronic collection of information in identifiable form for ten or more persons (excluding agencies, instrumentalities, or employees of the Federal Government) or as the director of the organization deems appropriate. Systems that do not meet the criteria established in OMB policy are not required to implement RA-8 PRIVACY IMPACT ASSESSMENTS, although they have the discretion to implement it if doing so supports the management of privacy risks.

Operational and Environmental Considerations

Controls that are based on specific assumptions about the operational environment are applicable only if the system is employed in the assumed environment. For example, a system that resides on an earth-orbiting satellite does not need physical controls like physical access logs, visitor controls, temperature and humidity controls, or water damage protection. Therefore, these controls (and possibly others) do not apply to the system. [Back to Table of Contents]

33. What is a compensating control?

A compensating control is a security or privacy control that provides an equivalent or comparable level of protection for a system or organization. More than one compensating control may be required to provide the equivalent or comparable protection for a particular security or privacy control. Compensating controls are typically selected after applying the scoping considerations in the tailoring guidance to the initial set of baseline security and privacy controls.

The organization may, on occasion, employ compensating controls when the organization is unable to implement a control in the baseline or when the control in the baseline is not a cost-effective means of obtaining the needed risk mitigation due to the specific nature of a system or its environment of operation. For example, compensating controls may be needed by the organization when applying technology-based considerations that address the lack of capability to support automated mechanisms as part of a control or control enhancement requirement. [Back to Table of Contents]

34. Under what conditions are compensating controls used?

A compensating control for a system may be employed in lieu of another control only under the following conditions:

- The organization selects a control and/or control enhancement from the NIST SP 800-53 [SP 800-53r5] security and privacy control catalog that is not in any baseline, or if an appropriate compensating control is not available, the organization adopts a suitable compensating control from another source;
- The organization provides supporting rationale for how the compensating control delivers an equivalent security capability for the system and why the related baseline control could not be employed; and
- The organization assesses and formally accepts the risks associated with employing the compensating control in the system. [Back to Table of Contents]

35. What are organization-defined parameters and how are they applied within a system?

Organization-defined parameters are the assignment and selection statements included in many controls. Controls with organization-defined parameters give organizations the flexibility to define certain portions of the controls to support specific organizational

requirements or objectives. After the application of scoping guidance and selection of compensating controls, organizations review the list of controls for assignment and selection operations and determine the appropriate organization-defined values for the identified parameters. Values for organization-defined parameters are adhered to unless more restrictive values are prescribed by applicable federal laws, Executive Orders, directives, policies, standards, guidelines, or regulations.

Organizations may choose to specify values for control parameters before selecting compensating controls since the specification of those parameters completes the definition of the control and may affect the compensating control requirements. [Back to Table of Contents]

36. Why do organizations supplement their controls?

The final determination of the appropriate set of security and privacy controls necessary to provide adequate protection is a function of the organization's assessment of risk and what is required to sufficiently mitigate the risks to organizational operations and assets, individuals, other organizations, and the Nation. In many cases, additional controls or control enhancements may be needed to address security and privacy requirements and to satisfy the requirements of federal laws, Executive Orders, directives, policies, standards, or regulations. The risk assessment at this stage in the control selection process provides important input to determine the sufficiency of the controls in the tailored baseline. [Back to Table of Contents]

37. How do system owners supplement their controls?

Organizations are encouraged to make maximum use of the security and privacy control catalog in NIST SP 800-53 [SP 800-53r5] in order to facilitate the process of enhancing controls or adding controls to the tailored baseline. In selecting the control and control enhancements to supplement the tailored baseline, the organization can employ a requirements definition approach or a gap analysis approach.

In the organization-generated control selection approach, the organization acquires specific and credible threat information (or makes a reasonable assumption) about the activities of adversaries with certain capabilities or attack potential (e.g., skill levels, expertise, available resources). To effectively withstand cyber attacks from adversaries with the stated capabilities or attack potential, the organization strives to achieve a certain level of preparedness. Organizations can choose additional controls and control enhancements from NIST SP 800-53 to obtain such capabilities or level of preparedness.

The gap analysis approach begins with an organizational assessment of its current capabilities or level of cyber preparedness. From that initial capability assessment, the organization determines the types of threats it can reasonably expect to address. If the organization's current capabilities or level of cyber preparedness are insufficient, the gap analysis determines the required capabilities and level of preparedness. The organization subsequently defines the controls and control enhancements from NIST SP 800-53 needed to achieve the desired capabilities or cyber preparedness level. [Back to Table of Contents]

38. Why is information on the selected set of controls captured in security and privacy plans?

The selected set of security and privacy controls and the supporting rationale for selection decisions and system use restrictions are captured in security and privacy plans for the system. The information in security and privacy plans is essential when examining the security and privacy considerations for systems with respect to potential mission and business impact. This is particularly important during control assessments since assessors need to know what to assess against in order to verify control effectiveness.

Capturing any significant risk management decisions in the security and privacy control selection process in the security and privacy plans is imperative in order for authorizing officials to have the necessary information to make credible, risk-based decisions regarding the authorization of organizational systems. In addition, without such information, the understanding, assumptions, and rationale supporting those important risk decisions may not be available when the state of the systems or environments of operation change and the original risk decisions are revisited. [Back to Table of Contents]

39. What information is captured in security and privacy plans?

Organizations may develop a consolidated plan that incorporates security and privacy plans or maintain separate plans. The security and privacy plans prepared by the system owner provide an overview of the security and privacy requirements for the system and describe the controls in place or planned for meeting the security and privacy requirements. The security and privacy requirements overview is described in sufficient detail to determine that the security and privacy controls selected would meet those requirements. In addition to the list of security and privacy controls selected for implementation, the security and privacy plans capture information about the intended application of each control in the context of the system with sufficient detail to enable a compliant implementation of the control.

Descriptive information about the system is captured in the system identification section of the security and privacy plans, included in attachments to the plans, or referenced in other standard sources for information generated as part of the system development life cycle. Duplication of information is avoided whenever possible by providing references or pointers to supporting information rather than repeating the same information in the security and privacy plans. New information is added and existing information is modified in the system description section as it becomes available during the system development life cycle and execution of the Risk Management Framework tasks.

The level of detail provided in the security and privacy plans is determined by the organization and is typically commensurate with the security categorization of the system. NIST SP 800-18, *Guide for Developing Security Plans for Federal Systems* [SP 800-18], provides detailed information on preparing security plans. [Back to Table of Contents]

40. Do security plans have to follow the format provided in NIST SP 800-18?

No, organizations are not required to follow the plan structure or template included in NIST SP 800-18 [SP 800-18]. Additional information may be included in the basic plan and the structure and format organized according to the organization's needs as long as the major sections described in NIST SP 800-18 are adequately covered and readily identifiable. [Back to Table of Contents]

41. Can security and privacy plans be automatically generated?

Yes, security and privacy plans can be automatically generated. This is accomplished with commercial governance, risk, and compliance (GRC) solutions or similar tools. The plan can also be generated via custom templates, scripts and the use of the NIST Open Security Controls Assessment Language (OSCAL) [OSCAL]. [Back to Table of Contents]

42. Why are controls monitored?

Organizations develop a strategy and implement a program for the continuous monitoring of control effectiveness for all implemented controls, including the potential need to change or supplement the control set, while taking into account any proposed or actual changes to the system or its environment of operation. Conducting a thorough point-in-time assessment of the deployed controls is a necessary but not sufficient condition to demonstrate security due diligence. The objective of continuous monitoring is to determine if the set of deployed controls continue to be effective over time in light of the inevitable changes that occur. A well-designed, well-managed continuous monitoring process can effectively transform an otherwise static control assessment and risk determination process into a dynamic process that provides essential, near real-time status-related information to organizational officials so that they can take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the system. For more information, see NIST SP 800-37, Revision 2 (Monitor Step) [SP 800-37], and RMF Monitor Step Frequently Asked Questions (FAQs) Quick Start Guide. [Back to Table of Contents]

43. What is the continuous monitoring strategy?

The continuous monitoring strategy for a system determines what controls are to be monitored, when the controls are monitored (e.g., ongoing or according to a predefined frequency), how changes to the system are monitored, how risk assessments are to be conducted, and the security and privacy posture reporting requirements, including recipients of the reports. It is approved by the authorizing official or authorizing official designated representative and can be included in the security and privacy plans.

The continuous monitoring strategy for systems is part of an overall organization continuous monitoring program that addresses monitoring requirements at the organization and mission and business process levels in addition to system level requirements. To assist organizations in the development of an information security continuous monitoring strategy and the implementation of an information security continuous monitoring program, NIST has developed SP 800-137, *Information Security Continuous Monitoring (ICSM) for Federal Information Systems and Organizations.* [SP 800-137]. For more information and discussion on organizational continuous monitoring strategy, see Task P-7, *Continuous Monitoring Strategy – Organization*. [Back to Table of Contents]

44. How are controls selected for continuous monitoring?

All implemented controls are monitored at an organization-defined frequency. The criteria for determining the frequency with which controls are to be monitored post implementation/authorization is established by the system owner in collaboration with other organizational officials and in accordance with the organizational level continuous monitoring strategy. The criteria reflect the priorities and importance of the system to organizational operations and assets, individuals, other organizations, and the Nation. Controls that are volatile (i.e., most likely to change over time), critical to certain aspects of the organization's protection strategy, or identified in current plans of action and milestones are assessed as frequently as necessary and consistent with the criticality of the function and capability of the monitoring tools.

An organizational assessment of risk (either formal or informal) can also be used to guide the frequency of control monitoring. The approach to control assessments during continuous monitoring may include detection of the status of system components, analysis of historical and operational data, and the reuse of assessment procedures and results that supported the initial authorization decision. For more information, see NIST SP 800-137 [SP 800-137] and RMF Monitor Step Frequently Asked Questions (FAQs) Quick Start Guide. [Back to Table of Contents]

45. Why do security and privacy plans need to be approved?

An independent review of the security and privacy plans by the authorizing official with support from the senior accountable official for risk management or risk executive (function), chief information officer, senior agency information security officer, and senior agency official for privacy helps determine if plans are complete, consistent, and satisfy the stated security and privacy requirements for the system. The security and privacy plan review also helps to determine – to the greatest extent possible with available planning or operational artifacts – if the security and privacy plans correctly and effectively identify the potential risk to organizational operations and assets, individuals, other organizations, and the Nation that would be incurred if the controls identified in the plans were implemented as intended.

Based on the results of this independent review and analysis, the authorizing official may recommend changes to the security and privacy plans. If the security and privacy plans are deemed unacceptable, the authorizing official sends the plans back to the system owner (or common control provider) for appropriate action. If the security and privacy plans are deemed acceptable, the authorizing official approves the plan. By approving the security and privacy plans, the authorizing official agrees to the set of security and privacy controls (system-specific, hybrid, or common) proposed to meet the security and privacy requirements for the system. This approval allows the risk management process to advance to the Implement step in the Risk Management Framework. The approval of the security and privacy plans also establishes the level of effort required to successfully complete the remainder of the RMF steps and provides the basis of the security and privacy specification for the acquisition of the system, subsystems, or components. [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

[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

[OMB M-03-22] Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. September 2003. https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/

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

[SP 800-18] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1

[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 800-53r4] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[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 800-66] Scholl MA, Stine KM, Hash J, Bowen P, Johnson LA, Steinberg DI, Smith CD (2008) An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-66, Rev. 1. https://doi.org/10.6028/NIST.SP.800-66r1

[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

[Back to Table of Contents]