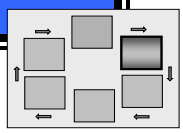
SELECT STEP FAQS



NIST RISK MANAGEMENT FRAMEWORK

Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information. Assurance is the grounds for confidence that the security controls implemented within an information system are effective in their application. Selecting and implementing the appropriate security controls and assurance requirements for an information system or system-of-systems 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.

General Select Step FAQs

1. What are security controls?
2. Why are organizations required to select security controls?
3. What is the select process?
4. When are security requirements considered within the system development life cycle?
5. Who is responsible for selecting the security controls for an information system?
6. What is the role of the risk executive (function) in the security control selection process?
7. Are external service providers required to implement federal security requirements including the security controls?
8. When NIST revises NIST SP 800-53, is the organization required to implement the changes?

Select Step Fundamentals

9. Do all federal information systems have to meet the minimum security requirements specified in FIPS 200?
10. What other sources should be reviewed to determine if additional security requirements apply to an information system?
11. Must all of the security controls in the corresponding security control baseline by used?
12. Under what conditions should the use of an information system be restricted?
13. What are the different types of security controls?
14. What are system-specific controls?
15. What are common controls?
16. What are hybrid controls?
17. Who is responsible of common controls or the common portion of hybrid controls?
18. How are security controls allocated to information systems?
19. What is the structure of a security control?
20. Are organizations expected to apply the supplemental guidance?
21. What is security control assurance?
22. Why were program management controls added to NIST SP 800-53, Rev. 3?
23. Do security controls need to be periodically reviewed and updated?
24. What types of events can trigger a need to modify or update the security controls?

Organizational Support for the Select Step FAQs

25. Are organizations expected to support risk management?
26. What is the relationship between the security controls and an organization's policies and procedures?

27. Why should organizations implement common security controls?
28. Who should define common security controls?
29. How are common controls determined for the organization?
30. Who is responsible for the program management controls?
31. What is the information security program plan?
32. Can the organization provide templates and tools to assist with preparing security documentation?

System-specific Application of the Select Step FAQs

33. What steps should the information system owner follow to select the security controls for an information system?
34. What is the security categorization and how does it influence the selection of the initial security baseline?
35. How is the initial security control baseline selected?
36. What is tailoring?
37. How is scoping guidance applied to the information system?
38. What are some examples or scenarios of applying the scoping guidance to an information system:
39. What is a compensating security control?
40. Under what conditions are compensating controls used?
41. What are organization-defined parameters and how are they applied within an information system?
42. Why do organizations supplement their security controls?
43. How do information system owners supplement their security controls?
44. Which minimum assurance requirements apply to an information system?
45. How are the minimum assurance requirements met by control developers/implementers?
46. Why is the selected set of security controls documented in the security plan?
47. What information is documented in the security plan?
48. Does the security plan have to follow the format provided in NIST SP 800-18?
49. Why are security controls monitored?
50. What is the continuous monitoring strategy?
51. How are security controls selected for continuous monitoring?
52. Why is the security plan approved?

GENERAL SELECT FAQS

1. WHAT ARE SECURITY CONTROLS?

Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information.[1] Selecting the appropriate set of security controls helps to achieve the objective of conducting the day-to-day operations of the organization and accomplishing the organization's stated missions and business functions with what the OMB Circular A-130 defines as adequate security, or security commensurate with risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.[2]

[1] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 1

[2] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 2

2. WHY ARE ORGANIZATIONS REQUIRED TO SELECT SECURITY CONTROLS?

Organizations are required to adequately mitigate risk arising from use of information and information systems in the execution of missions and business functions. A significant challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective, would most cost-effectively mitigate risk while complying with the security requirements defined by applicable federal laws, Executive Orders, directives, policies, standards, or regulations (e.g., FISMA, OMB Circular A-130). Selecting the appropriate set of security controls to adequately mitigate risk by meeting the specific, and sometimes unique, security requirements of an organization is an important task—a task that clearly demonstrates the organization's commitment to security and the due diligence exercised in protecting the confidentiality, integrity, and availability of organizational information and information systems.[3]

3. WHAT IS THE SELECT PROCESS?

Security controls are selected based on the security categorization of the information system and requirements for the organization-specific environment of operations. The security control selection process includes, as appropriate:[4]

- Choosing a set of baseline security controls;
- Tailoring the baseline security controls by applying scoping, parameterization, and compensating control guidance;
- Supplementing the tailored baseline security controls, if necessary, with additional controls or control enhancements to address unique organizational needs based on a risk assessment and local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analysis, or special circumstances; and
- Specifying minimum assurance requirements, as appropriate.

The selection of the initial set of baseline security controls is based on the impact level of the information system as determined by the security categorization process. The organization selects one of three sets of baseline security controls from NIST SP 800-53, Appendix D, corresponding to the low-, moderate-, or high-impact rating of the information system.[5] 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 information system or its environment of operation).[6]

In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system and to satisfy the requirements of applicable federal laws, Executive Orders, directives, policies, standards, or regulations.[7] The supplementation

[3] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 9

[4] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 25

[5] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 19

[6] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 19

[7] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 23

process is used for this purpose. During supplementation, the sufficiency of the tailored baseline to adequately protect the organization's operations is determined. The final determination of the appropriate set of security controls necessary to provide adequate security for an information system is a function of the organization's assessment of risk and what is required to sufficiently mitigate the risks.[8]

4. WHEN ARE SECURITY REQUIREMENTS CONSIDERED WITHIN THE SYSTEM DEVELOPMENT LIFE CYCLE?

All federal information systems, including operational systems, systems under development, and systems undergoing modification or upgrade, are in some phase of a system development life cycle. Requirements definition is a critical part of any system development process and begins very early in the life cycle, typically in the initiation phase. Security requirements are a subset of the overall functional and nonfunctional requirements levied on an information system and are incorporated into the system development life cycle simultaneously with the functional and nonfunctional requirements. Without the early integration of security requirements, significant expenses may be incurred by the organization later in the life cycle to address security considerations that could have been included in the initial design. When security requirements are considered as an integral subset of other information system requirements, the resulting system has fewer weaknesses and deficiencies, and therefore, fewer vulnerabilities that can be exploited in the future.[9]

5. WHO IS RESPONSIBLE FOR SELECTING THE SECURITY CONTROLS FOR AN INFORMATION SYSTEM?

The information system owner and information security architect are responsible for selecting the security controls for the information system and documenting the controls in the security plan.[10] The information system owner is responsible for addressing the operational interests of the user community and for ensuring compliance with information security requirements. In addition, the information system owner, in conjunction with the information system security officer (ISSO), is responsible for the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls.[11]

The information security architect is responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information system supporting those missions and business processes.[12]

[8] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 23

[9] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 9

[10] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 25

[11] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. D-5

[12] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. D-6

6. WHAT IS THE ROLE OF THE RISK EXECUTIVE (FUNCTION) IN THE SECURITY CONTROL SELECTION PROCESS?

The risk executive (function) helps ensure that information security considerations for individual information systems are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its mission/business processes.[13] The risk executive (function) develops a risk management strategy for the organization providing a strategic view of information security-related risks with regard to the organization as a whole and facilitates the sharing or risk-related information among authorizing officials and other senior leaders within the organization.[14] This organizational perspective of risk is considered by the information system owner when selecting the appropriate set of security controls for the information system.

7. ARE EXTERNAL SERVICE PROVIDERS REQUIRED TO IMPLEMENT FEDERAL SECURITY REQUIREMENTS INCLUDING THE SECURITY CONTROLS?

Yes, FISMA and OMB policy require external providers handling federal information or operating information system on behalf of the federal government to meet the same security requirements as federal agencies. Security requirements for external providers including the security controls for information systems processing, storing, or transmitting federal information are expressed in appropriate contracts or other formal agreements.[15] Ultimately, the responsibility for adequately mitigating unacceptable risks arising from the use of external information system services remains with the authorizing official.[16]

The assurance or confidence that the risk from using external services is at an acceptable level depends on the trust that the organization places in the external service provider. The level of trust that an organization places in an external service provider can vary widely, ranging from those who are highly trusted to those who are less trusted and present greater sources of risk.[17] Organizations require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security.[18]

A chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Depending on the nature of the service, it may simply be unwise for the organization to place significant trust in the provider—not due to any inherent untrustworthiness on the provider's part, but due to the intrinsic level of risk in the service.

[13] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 13

[14] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. D-2

[15] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 12

[16] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 13

[17] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 13, Footnote 40

[18] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 13

Where a sufficient level of trust cannot be established in the external services or service providers, the organization employs compensating controls or accepts a greater degree of risk.[19]

8. WHEN NIST REVISES NIST SP 800-53, IS THE ORGANIZATION REQUIRED TO IMPLEMENT THE CHANGES?

The security controls in the security control catalog are expected to change over time, as controls are withdrawn, revised, and added. The security controls defined in the low, moderate, and high baselines are also expected to change over time as the level of security and due diligence for mitigating risks within organizations changes. In addition to the need for change, the need for stability will be addressed by requiring that proposed additions, deletions, and modifications to the catalog of security controls go through a rigorous public review process to obtain government and private sector feedback and to build consensus for the changes. A stable, yet flexible and technically rigorous set of security controls will be maintained in the security control catalog.[20]

Compliance schedules for NIST security standards and guidelines are established by OMB in policies, directives, or memoranda (e.g., annual FISMA Reporting Guidance).[21]

SELECT STEP FUNDAMENTALS

9. DO ALL FEDERAL INFORMATION SYSTEMS HAVE TO MEET THE MINIMUM SECURITY REQUIREMENTS SPECIFIED IN FIPS 200?

Yes, FIPS 200 specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government.[22] Organizations must meet the minimum security requirements in FIPS 200 by selecting the appropriate security controls and assurance requirements as described in NIST SP 800-53.[23]

The guidelines in NIST SP 800-53 are applicable to all federal information 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.[24]

[19] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, pp. 13-14

[20] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 15

[21] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. iv

[22] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006, p. 1

[23] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006, p. 4

[24] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 2

10. WHAT OTHER SOURCES SHOULD BE REVIEWED TO DETERMINE IF ADDITIONAL SECURITY REQUIREMENTS APPLY TO AN INFORMATION SYSTEM?

Additional security requirements may be defined in applicable federal laws, Executive Orders, directives, policies, standards, or regulations.[25] These documents are reviewed and appropriate security controls are identified to satisfy the security requirements. NIST SP 800-53 provides a set of security controls that can satisfy the breadth and depth of security requirements levied on information systems and organizations and that is consistent with and complementary to other established information security standards. The catalog of security controls provided in NIST SP 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements.[26] NIST SP 800-66, Rev. 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, Appendix D provides an example of how the NIST security controls are used to satisfy the security requirements defined in a federal law using the NIST SP 800-53 security control catalog.[27]

11. MUST ALL OF THE SECURITY CONTROLS IN THE CORRESPONDING SECURITY CONTROL BASELINE BE USED?

Organizations must employ all security controls in the respective security control baselines unless specific exceptions are allowed based on the tailoring guidance provided in NIST SP 800-53.[28] Baseline controls are the starting point for the security control selection process and are chosen based on the security category and associated impact level of the information system determined in accordance with FIPS 199 and FIPS 200, respectively. Tailoring the security control baseline allows the organization to adjust the security controls to meet mission/business requirements within the environment of operation. The tailored security control baseline is supplemented based on an organizational assessment of risk and the resulting set of security controls documented in the security plan for the information system.[29]

12. UNDER WHAT CONDITIONS SHOULD THE USE OF AN INFORMATION SYSTEM BE RESTRICTED?

There may be situations in which an organization is employing information technology beyond its ability to adequately protect essential missions and business functions (e.g., certain web-based, social networking, and collaborative computing-based technologies). That is, the organization cannot apply sufficient security controls within an information system to adequately reduce or mitigate risk. In those situations, an alternative strategy is needed to prevent the mission and business functions from being adversely affected; a strategy that considers the mission/business risks that result from an aggressive use of information technology. Restrictions on the types of technologies used and how the information system is employed provide an alternative method to reduce or mitigate risk when security controls cannot be implemented within technology/resource constraints, or when controls lack reasonable

[25] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 23

[26] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 3

[27] NIST SP 800-66, Revision 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, pp. D-1-D-2

[28] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006, p. 4

[29] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 9

expectation of effectiveness against identified threat sources. Restrictions on the use of information systems and specific information technologies are in many situations, the only practical or reasonable course of action an organization can take in order to have the ability to carry out its assigned missions and business functions in the face of determined adversaries. Examples of use restrictions include:[30]

- Limiting the information an information 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 information system components from the network (i.e., air gapping); and
- Prohibiting public access to moderate- or high-impact information systems, unless an explicit determination is made authorizing such access.

13. WHAT ARE THE DIFFERENT TYPES OF SECURITY CONTROLS?

There are three types of security controls for information systems that can be employed by an organization:[31]

- System-specific controls—controls that provide a security capability for a particular information system only;
- Common controls—controls that provide a security capability for multiple information systems; or
- Hybrid controls—controls that have both system-specific and common characteristics.

The organization allocates security controls to an information system consistent with the organization's enterprise architecture and information security architecture. The organization has significant flexibility in deciding which families of security controls or specific controls from selected families in NIST SP 800-53 are appropriate for the different type of allocations.[32]

14. WHAT ARE SYSTEM-SPECIFIC CONTROLS?

System-specific controls are security controls that provide a security capability for a particular information system only and are the primary responsibility of information system owners and their respective authorizing officials.[33] An example of a security control that is typically implemented as a system-specific control is IA-6, Authenticator Feedback, where the information system is designed to obscure the feedback of authentication information during the authentication process. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.[34]

[30] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 24

[31] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 16

[32] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 16

[33] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 11

[34] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. F-59

15. WHAT ARE COMMON CONTROLS?

Common controls are security controls that can support multiple information systems efficiently and effectively as a common capability. When these controls are used to support a specific information system, they are referenced by that specific system as inherited controls.[35] Many of the security controls needed to protect organizational information systems (e.g., contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls) are excellent candidates for common control status. Information security program management controls may also be deemed common controls by the organization since the controls are employed at the organizational level and typically serve multiple information systems.[36]

16. WHAT ARE HYBRID CONTROLS?

Hybrid controls are security controls where one part of the control is deemed to be common and another part of the control is deemed to be system-specific.[37] The organization may choose, for example, to implement the Security Awareness security control (AT-2) as a hybrid control with general organization-wide security awareness training provided as a common capability with focused security awareness training provided for the specific information system.

Hybrid controls may also serve as templates for further control refinement. For example, the organization may choose to implement the Contingency Planning security control (CP-2) by providing a template for a generalized contingency plan for all organizational information systems with individual information system owners tailoring the plan, where appropriate, for system-specific uses.[38]

17. 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:[39]

- Documenting the organization-identified common controls in a security plan (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;
- Documenting assessment findings in a security assessment report; and
- Producing a plan of action and milestones for all controls having weaknesses or deficiencies.

[35] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 16

[36] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 10

[37] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 11

[38] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 11

[39] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. D-5

Security plans, security assessment reports, and plans of action and milestones for common controls (or a summary of such information) are made available to information system owners (whose systems are inheriting the controls) after the information is review and approved by the senior official or executive responsible and accountable for the controls. Organizations ensure that common control providers have the capability to rapidly broadcast changes in the status of common controls that adversely affect the protections being provided by and expected of the common controls. Common control providers are able to quickly inform information system owners when problems arise in the inherited common controls (e.g., when an assessment or reassessment of a common control indicates the control is flawed in some manner, when a new threat or attack method arises that renders the common control less than effective in protecting against the new threat or attack method).[40]

18. HOW ARE SECURITY CONTROLS ALLOCATED TO INFORMATION SYSTEMS?

The organization allocates security controls to an information system consistent with the organization's enterprise architecture and information security architecture. This activity is carried out as an organization-wide activity involving authorization officials, information system owners, chief information security officer, senior information security officer, enterprise architect, information security architect, information system security officers, common control providers, and the risk executive (function). By allocating security controls to an information 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.[41]

19. WHAT IS THE STRUCTURE OF A SECURITY CONTROL?

The security control structure consists of the following parts:[42]

- Control section;
- Supplemental guidance section;
- Control enhancements section;
- References section; and
- Priority and baseline allocation section.

The control section provides a concise statement of the specific security capabilities needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system. The supplemental guidance section provides additional information related to a specific security control, but contains no requirements. The security control enhancements section provides statements of security capability to build in additional functionality to a control or increase the strength of a control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to the basic control functionality based on the results of a risk assessment. The references section includes a list of applicable federal laws, Executive Orders, directives, policies, standards, and guidelines that are relevant to a particular security control or control

[40] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 24

[41] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 16

[42] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 7

enhancement. The priority and baseline allocation section provides the recommended priority codes used for sequencing decisions during security control implementation and the initial allocation of security controls and control enhancements for low-, moderate-, and high-impact information systems.[43]

For some security controls in the control catalog, a degree of flexibility is provided by allowing organizations 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 security controls to support specific mission, business, or operational needs. For example, an organization can specify the actions to be taken by the information 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.[44]

20. ARE ORGANIZATIONS EXPECTED TO APPLY THE SUPPLEMENTAL GUIDANCE?

Yes, organizations are expected to apply the supplemental guidance, as appropriate, when defining, developing, and implementing security controls. The supplemental guidance provides important considerations for implementing security controls in the context of an organization's operating environment, mission requirements, or assessment of risk. Security control enhancements may also contain supplemental guidance. Enhancement supplemental guidance is used in situations where the guidance is not generally applicable to the entire control but is instead focused on the particular control enhancement.[45]

21. WHAT IS SECURITY CONTROL ASSURANCE?

Assurance is the grounds for confidence that the security controls implemented within an information system are effective in their application. Assurance can be obtained in a variety of ways including:[46]

- Actions taken by developers, implementers, and operators in the specification, design, development, implementation, operation, and maintenance of security controls; and
- Actions taken by security control assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

NIST SP 800-53, Appendix E describes the minimum assurance requirements in low-, moderate-, and high-impact information systems. For security controls in low-impact systems, the emphasis is on the control being in place with the expectation that no obvious errors exist and that as flaws are discovered, they are addressed in a timely manner. For security controls in moderate-impact systems, in addition to the assurance requirements for low-impact systems, the emphasis is on increasing the grounds for confidence in control correctness. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer or control implementer incorporates, as part of the control, specific

[43] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, pp. 7-8

[44] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 7

[45] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 8

[46] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 14

capabilities to increase grounds for confidence that the control meets its function or purpose. For security controls in high-impact systems, in addition to the assurance requirements for moderate-impact systems, the emphasis is on requiring within the control, the capabilities that are needed to support ongoing, consistent operation of the control and to support continuous improvement in the control's effectiveness.[47]

There are additional assurance requirements available to developers/implementers of security controls supplementing the minimum assurance requirements for the moderate- and high-impact information systems in order to protect against threats from highly skilled, highly motivated, and well-resourced threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with those highly skilled, highly motivated, or well-resourced threat agents.[48]

22. WHY WERE PROGRAM MANAGEMENT CONTROLS ADDED TO NIST SP 800-53, REV. 3?

The program management controls focus on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. The information security program management controls are described in NIST SP 800-53, Rev., Appendix G and they complement the security controls in Appendix F. Organizations are required to implement security program management controls to provide a foundation for the organization's information security program. The successful implementation of security controls for organizational information systems depends on the successful implementation of the organization's program management controls.[49]

23. DO SECURITY 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 information system is authorized for operation in accordance with the organization's risk management strategy. The continuous monitoring strategy includes an ongoing assessment of security control effectiveness to determine if there is a need to modify or update the current deployed set of security controls based on changes in the information system or its environment of operation.[50]

[47] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 14

[48] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 14

[49] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. G-1

[50] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, pp. 27-28

24. WHAT TYPE OF EVENTS CAN TRIGGER A NEED TO MODIFY OR UPDATE THE SECURITY CONTROLS?

There are certain events that can trigger the immediate need to assess the security state of the information system and if required, modify or update the current security controls. These events include, for example:[51]

- An incident results in a breach to the information 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, information 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 information system through the removal or addition of new or upgraded hardware, software, or firmware or changes in the operational environment potentially degrade the security state of the system; or
- Significant changes to the organizational risk management strategy, information security policy, supported missions or business functions, or information being processed, stored, or transmitted by the information system.

When these types of events occur, organizations should, at a minimum, take the following actions:[52]

- Reconfirm the security category and impact level of the information system;
- Assess the current security state of the information 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 information system.

ORGANIZATIONAL SUPPORT FOR THE SELECT STEP FAQS

25. ARE ORGANIZATIONS EXPECTED TO SUPPORT RISK MANAGEMENT?

For risk management to succeed at all levels of the organization, the organization must have a consistent and effective approach to risk management that is applied to all risk management processes and procedures. Organizational officials identify the resources necessary to complete the risk management tasks and ensure that those resources are made available to appropriate personnel. Resource allocation includes both funding to carry out the risk management tasks and assigning qualified personnel needed to accomplish the tasks.[53]

The management of risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect organizational operations and assets, individuals, other

[51] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, pp. 27-28

[52] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, pp. 28-29

[53] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 9

organizations, and the Nation. This risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable federal laws, Executive Orders, directives, policies, regulations standards, or guidelines.[54]

26. WHAT IS THE RELATIONSHIP BETWEEN THE SECURITY CONTROLS AND AN ORGANIZATION'S POLICIES AND PROCEDURES?

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

The use of security controls from NIST SP 800-53 and the incorporation of tailored baseline controls as a starting point in the control selection process, facilitate a more consistent level of security across federal information 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.[55]

27. WHY SHOULD ORGANIZATIONS IMPLEMENT A COMBINATION OF SYSTEM-SPECIFIC, COMMON, AND HYBRID SECURITY CONTROLS?

Partitioning security 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 security controls across the organization. While the concept of security control portioning into common, hybrid, and system-specific controls is straightforward and intuitive, the application within an organization takes significant planning and coordination.[56]

28. WHO SHOULD DEFINE COMMON SECURITY CONTROLS?

The identification of common controls is most effectively accomplished as an organization-wide exercise with the active involvement of the chief information officer, senior information security officer, risk executive (function), authorizing officials, information system owners, information owners/stewards, and information system security officers.[57]

29. HOW ARE COMMON CONTROLS DETERMINED FOR THE ORGANIZATION?

The organization-wide process for determining common controls includes considerations of the security categories and impact levels of the information systems within the organization, as well as the security controls necessary to adequately mitigate the risks arising from the use of those systems. When common controls protect multiple organizational information system of differing impact levels, the controls are

[54] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 16

[55] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 4

[56] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 11

[57] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 10

implemented with regard to the highest impact level among the systems.[58] Common controls promote more cost-effective and consistent information security across the organization and can also simplify risk management activities.[59]

30. WHO IS RESPONSIBLE FOR THE PROGRAM MANAGEMENT CONTROLS?

Organizations specify the individuals within the organization responsible for the development, implementation, assessment, authorization, and monitoring of the information security program management controls. Organizations document the program management controls in the information security program plan. The organization-wide information security program plan supplements the individual security plans developed for each organizational information system. Together, the security plans for the individual information systems and the information security program cover the totality of security controls employed by the organization.[60]

31. WHAT IS THE INFORMATION SECURITY PROGRAM PLAN?

The information security program plan can be represented in a single document or compilation of documents at the discretion of the organization. The plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan indicates which separate security plans, if any, contain descriptions of common controls.

32. CAN THE ORGANIZATION PROVIDE TEMPLATES AND TOOLS TO ASSIST WITH PREPARING SECURITY DOCUMENTATION?

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

Automated tools are important to support consistency in the development of security documentation and the security assessment process. When organizations have the resources necessary to acquire and implement automated tools, the organization further simplifies the development of security documentation and the security control assessment process.

[58] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 10

[59] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 16

[60] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. G-1

SYSTEM-SPECIFIC APPLICATION OF THE SELECT STEP FAQS

33. WHAT STEPS SHOULD THE INFORMATION SYSTEM OWNER FOLLOW TO SELECT THE SECURITY CONTROLS FOR AN INFORMATION SYSTEM?

To determine the appropriate security controls for an information system, the information system owner selects the initial security control baseline based on the categorization, tailors and supplements the security controls based on the risk assessment, and documents the results in the system security plan.

Prepare for Selecting Security Controls

In order to select the appropriate security controls for the information system, the information system owner collects relevant documentation specific to the information systems such as the initial system security plan and the risk assessment results. In addition, the information system owner collects any available guidance documentation issued by the organization.

Select the Initial Security Control Baseline and Minimum Assurance Requirements

Once the system's impact level is determined during the security categorization process, the information system owner identifies the initial set of security controls and minimum assurance requirements. The initial set of security controls is selected from the corresponding low, moderate, or high baselines in NIST SP 800-53, Appendix D. The minimum assurance requirements are defined in NIST SP 800-53, Appendix E. [See questions 34-35 on categorization and determining the initial security control baseline.]

Applying Scoping Guidance

Scoping guidance provides organizations with specific terms and conditions on the applicability and implementation of individual security control baselines. The information system owner follows the scoping guidance considerations and directions on how to apply them to information systems as described in the NIST SP 800-53, Section 3.3. [See questions 35-38 on applying scoping guidance to the initial security control baseline.]

Determine Need for Compensating Controls

Compensating controls are another method for tailoring the system's security controls. A compensating security control is a management, operational, or technical control used by an organization instead of a recommended security control in the low, moderate, or high baseline that provides equivalent or comparable protection for an information system. [See questions 39-40 on identifying and using compensating controls.]

Determine Organization-defined Parameters

Security controls containing 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. [See question 41 on identifying and using organization-defined parameters.]

Supplement the Security Controls

The tailored security control baseline should be viewed as the foundation or starting point for determining the needed set of security controls for an information system. The information system owner uses the risk assessment results to determine the sufficiency of the security controls in the tailored baseline—that is,

determining whether or not the security controls adequately protect the organization's operations and assets, individuals, other organizations, and the Nation. In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations. [See questions 42-43 on supplementing the security controls.]

Determine Assurance Measures for the Minimum Assurance Requirements

Assurance is the grounds for confidence that the security controls implemented within an information system are effective in their application. Assurance can be obtained in a variety of ways, including actions taken by developers, implementers, and operators in the specification, design, development, implementation, operation, and maintenance of security controls. Assurance is also obtained by the actions taken by security control assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The information system owner determines the appropriate minimum assurance requirements and how they will be implemented within the information system. [See questions 44-45 on determining the appropriate minimum assurance requirements for the information system.]

Complete the System Security Plan

The information system owner documents the decisions made during the initial security control selection, tailoring, and supplementation processes, providing a sound rationale for those decisions. This documentation is essential when examining the overall security considerations for information systems with respect to potential mission or business case impact. [See questions 46-48 on documenting the selection decisions in the system security plan.]

Develop a Continuous Monitoring Strategy

The information system owner initiates development of the continuous monitoring strategy to manage the ongoing monitoring of security controls employed within or inherited by an information system. An ongoing monitoring program allows an organization to track the security state of an information system on a continuous basis and, over time, maintain the security authorization for the system. [See questions 49-51 on developing the continuous monitoring strategy.]

Obtain Approval for the System Security Plan

The authorizing official determines if the security plan is complete, consistent, and satisfies the stated security requirements for the information system. Complete coverage of security controls in appropriate security plans facilitates more comprehensive information security, promotes increased accountability, provides an effective vehicle to better manage the risks resulting from the operation and use of information systems, and is required to adequately support the security assessment of systems as part of the authorization process. [See question 52 on obtaining approval for selection of security controls for the information system.]

34. WHAT IS SECURITY CATEGORIZATION AND HOW DOES IT INFLUENCE THE SELECTION OF THE INITIAL SECURITY CONTROL BASELINE?

FIPS 199 requires organizations to categorize their information 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 water mark) for each type of information processed, stored, or transmitted by those information systems.[61]

The high water mark concept is also used to determine the impact level of the information system for the express purpose of selecting an initial set of security controls from one of the three security control baselines. Thus, a low-impact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a high-impact system is an information system in which at least one security objective is high.[62]

35. HOW IS THE INITIAL SECURITY CONTROL BASELINE SELECTED?

The selection of the initial set of baseline security controls is based on the impact level of the information system as determined by the security categorization process. The organization selects one of three sets of baseline security controls from NIST SP 800-53, Appendix D, corresponding to the low-, moderate-, or high-impact rating of the information system. Note that not all security controls are assigned to baselines, as indicated by the phrase *not selected*. Similarly, not all control enhancements are assigned to baselines, as indicated by the security control being *not selected* or the enhancement number, enclosed in parenthesis, not appearing in any baseline.[63]

36. WHAT IS TAILORING?

The information system owner tailors, or modifies and more closely aligns the security controls with the specific conditions within the organization (i.e., conditions specific to the information system or its environment of operation). The tailoring process includes:[64]

- Applying scoping guidance to the initial baseline security controls to obtain a preliminary set of applicable controls for the tailored baseline;
- 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; and
- Specifying organization-defined parameters in the security controls via explicit assignment and selection statements to complete the definition of the tailored baseline.

Organizations have the flexibility to perform the tailoring process at the organization level for all information systems (either as the required tailored baseline or as the starting point for system-specific tailoring), at the individual information system level, or using a combination of organization-level and system-specific approaches. Tailoring decisions for all affected security controls in the selected baseline, including the specific rationale for those decisions, are documented in the security plan for the

[61] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 18

[62] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 18

[63] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 19

[64] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 19

information system and approved by appropriate organizational officials as part of the security plan approval process.[65]

37. HOW IS SCOPING GUIDANCE APPLIED TO THE INFORMATION SYSTEM?

Scoping guidance in NIST SP 800-53 provides organizations with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines. 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 information system based on specific mission/business requirements and particular environments of operation. There are several scoping considerations that can potentially affect how the baseline security controls are applied and implemented by organizations:[66]

- Common control-related considerations;
- Security objective-related considerations;
- System component-related considerations;
- Technology-related considerations;
- Physical infrastructure-related considerations;
- Policy/regulatory-related considerations;
- Operational/environmental-related considerations;
- Scalability-related considerations; and
- Public access-related considerations.

38. WHAT ARE SOME EXAMPLES OR SCENARIOS OF APPLYING THE SCOPING GUIDANCE TO AN INFORMATION SYSTEM?

Several examples and scenarios for applying the scoping guidance to an information system are described below.[67]

Common Security Control-Related Considerations

Security controls designated by the organization as common controls are, in most cases, managed by an organizational entity other than the information system owner. Organizational decisions on which security controls are viewed as common controls may greatly affect the responsibilities of individual information system owners with regard to the implementation of controls in a particular baseline.[68]

Examples include:

- The organization's Plant Division provides emergency lighting for the entire facility;

[65] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 19

[66] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, pp. 20-22

[67] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, pp. 20-22

[68] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 20

- The organization publishes an enterprise Incident Response Plan and Procedures that ensures that all computer incidents in the organization are handled in the same manner to ensure consistency and completeness in the response;
- The Information Security Program Office publishes a contingency plan template for use on all organizational information systems; and
- The Physical Security Office monitors all physical access to the facility and provides guards to restrict access at approved entrances.

Security Objective-Related 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 199 security category for the supported security objectives before moving to the 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 information system. Downgrading actions apply only to the moderate and high baselines.[69]

The following security controls are recommended candidates for downgrading:

- Confidentiality: MA-3(3), MP-2(1), MP-3, MP-4, MP-5(1) (2) (3), MP-6, PE-5, SC-4, SC-9;
- Integrity: SC-8; and
- Availability: CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE-11, PE-13, PE-15, SC-6.

A scenario includes:

- System ABC has the following security category:

  SC_{ABC} = {(confidentiality, moderate), (integrity, high), (availability, low)}.
- Therefore, the impact level for the information system is high, based on the high-water mark 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 is moderate and the availability security objective is low; and
- Based on the scoping guidance in NIST SP 800-53, the security 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 800-53 (and above).

System Component-Related Considerations

Security controls in the baseline represent an information system-wide set of controls that may not be necessary for or applicable to every component in the system. Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control. Organizations assess the inventory of information system components to determine which security controls are applicable to the

[69] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 20

various components and subsequently make explicit decisions regarding where to allocate the controls in order to satisfy organizational security requirements.[70]

- Auditing controls are typically allocated to components of an information system that provide auditing capability (e.g., servers, etc.) and are not necessarily applied to every user-level workstation within the organization;
- A database management system may employ role-based access control while the operating system on which it resides may use identity-based (user name and password) access control; and
- When information system components are single-user, not networked, or part of a physically isolated network, one or more of these characteristics may provide appropriate rationale for not allocating selected controls to that component.

Technology-Related Considerations

Security 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 information system. Security 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 security controls, implemented through non-automated mechanisms or procedures, are used to satisfy specified security control requirements.[71]

- Systems that do not implement wireless technology do not need security 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; and
- Automated mechanisms may be required to maintain up-to-date, complete, accurate, and easily available baseline configurations of organizational information systems, but if automated mechanisms are not available, compensating controls may be implemented to satisfy the security control.

Physical Infrastructure-Related Considerations

Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system (including its information technology assets such as electronic mail or web servers, server farms, data centers, networking nodes, workstations, boundary protection devices, and communications equipment).[72] Many physical infrastructure-related security controls are implemented as common or hybrid controls.

Examples include:

[70] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 21

[71] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 21

[72] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 21

- The requirement for emergency power applies to the physical infrastructure housing the information system rather than other system components; and
- A central organization manages physical access to the building providing approved authorization credentials to all individuals approved for access to the facility.

Policy/Regulatory-Related Considerations

Security controls that address matters governed by applicable federal laws, Executive Orders, directives, policies, standards, or regulations (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable laws, Executive Orders, directives, policies, standards, or regulations.[73]

Examples include:

- Organizations are required to conduct a privacy impact assessment on an information system in accordance with OMB policy. The current OMB policy, defined in OMB Memorandum 03-22, requires a privacy impact assessment before developing or procuring information technology systems or projects that collect, maintain, or disseminate information in 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.[74] Systems that do not meet the criteria established in OMB policy are not required to implement PL-5, Privacy Impact Assessment.
- AC-3, Access Enforcement, includes the requirement for use of FIPS 140-2 if the access enforcement mechanism is encrypted. This requirement does not apply if the information system does not employ encryption as an access enforcement mechanism or the information to be encrypted is classified (see AC-3 text for specifics related to classified information).

Operational/Environmental-Related Considerations

Security controls that are based on specific assumptions about the operational environment are applicable only if the information system is employed in the assumed environment.[75]

An example is:

- A system residing on an earth-orbiting satellite will not need physical controls like physical access logs, visitor controls, temperature and humidity controls, and water damage protection. Therefore, these controls (and possibly others) do not apply to the information system.

Scalability-Related Considerations

Security controls are scalable with regard to the extent and rigor of the implementation. Scalability is guided by the security category and impact level of the information system being protected. Organizations use discretion in applying the security controls to information systems, giving

[73] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 21

[74] OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003

[75] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 22

consideration to the scalability factors in particular environments. This approach is a cost-effective, risk-based approach to security control implementation that expends no more resources that necessary, yet achieves sufficient risk mitigation and adequate security.[76]

An example includes:

- A contingency plan for a high-impact information system is expected to be quite lengthy and to contain a significant amount of detail, while a contingency plan for a low impact system can be shorter and have less detail.

Public Access-Related Considerations

When public access to organizational information systems is allowed, security controls are applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable to public access.[77]

Examples include:

- If a system is a public web server, then some security controls will not apply, including AC-17, Remote Access, and PE-2, Physical Access Authorizations; and
- Identification and authentication requirements apply to organizational personnel that maintain and support an information system that provides public access to publicly-accessible information but the identification and authentication requirements do not apply to users accessing the publicly available information though the organization's website.

39. WHAT IS A COMPENSATING SECURITY CONTROL?

A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST SP 800-53, Appendix D. The compensating control provides an equivalent or comparable level of protection for an information system and the information processed, stored, or transmitted by that system. More than one compensating control may be required to provide the equivalent or comparable protection for a particular security control. Compensating controls are typically selected after applying the scoping considerations in the tailoring guidance to the initial set of baseline security controls.[78]

The organization may, on occasion, employ compensating controls when the organization is unable to implement a security control in the baseline, or when, due to the specific nature of an information system or its environment of operation, the control in the baseline is not a cost-effective means of obtaining the needed risk mitigation. For example, compensating controls may be needed by the organization when

[76] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 22

[77] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 22

[78] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 22

applying technology-based considerations addressing the lack of capability to support automated mechanisms as part of a security control or control enhancement requirement.[79]

40. UNDER WHAT CONDITIONS ARE COMPENSATING CONTROLS USED?

A compensating control for an information system may be employed only under the following conditions:[80]

- The organization selects the compensating control from NIST SP 800-53, 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 information system and why the related baseline security control could not be employed; and
- The organization assesses and formally accepts the risks associated with employing the compensating control in the information system.

41. WHAT ARE ORGANIZATION-DEFINED PARAMETERS AND HOW ARE THEY APPLIED WITHIN AN INFORMATION SYSTEM?

Organization-defined parameters are the assignment and selection statements included in many security controls. Security controls containing 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 security controls, organizations review the list of security 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.[81]

Organizations may choose to specify values for security controls parameters before selecting compensating controls since the specification of those parameters completes the definition of the security control and may affect the compensating control requirements.[82]

42. WHY DO ORGANIZATIONS SUPPLEMENT THEIR SECURITY CONTROLS?

The final determination of the appropriate set of security controls necessary to provide adequate security for an information system 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 security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system and to satisfy the requirements of federal laws, Executive Orders, directives, policies, standards, or regulations. The risks assessment at this stage

[79] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, pp. 22-23

[80] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 23

[81] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 23

[82] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 23

in the security control selection process provides important inputs to determine the sufficiency of the security controls in the tailored baseline.[83]

43. HOW DO INFORMATION SYSTEM OWNERS SUPPLEMENT THEIR SECURITY CONTROLS?

Organizations are encouraged to make maximum use of the security control catalog in NIST SP 800-53, Appendix F, to facilitate the process of enhancing security controls or adding controls to the tailored baseline. In selecting the security control and control enhancements to supplement the tailored baseline, the organization can employ a requirements definition approach or a gap analysis approach.[84]

In the requirements definition 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 security controls and control enhancements from NIST SP 800-53, Appendix F, to obtain such security capability or level of preparedness.[85]

The gap analysis approach begins with an organizational assessment of its current security capability or level of cyber preparedness. From that initial security capability assessment, the organization determines the types of threats it can reasonably expect to address. If the organization's current security capability or level of cyber preparedness is insufficient, the gap analysis determines the required capability and level of preparedness. The organization subsequently defines the security controls and control enhancements from NIST SP 800-53, Appendix F, needed to achieve the desired capability or cyber preparedness level.[86]

44. WHICH MINIMUM ASSURANCE REQUIREMENTS APPLY TO AN INFORMATION SYSTEM?

The assurance requirements are grouped by information system impact level (low, moderate, or high) since the requirements apply to each control within the respective impact level. The minimum assurance requirements are defined in NIST SP 800-53, Appendix E. The minimum assurance requirements are applied to an information system on a control-by-control basis. [87]

[83] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 23

[84] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, pp. 23-24

[85] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 24

[86] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. 24

[87] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. E-1

45. HOW ARE THE MINIMUM ASSURANCE REQUIREMENTS MET BY CONTROL DEVELOPERS AND IMPLEMENTERS?

Assurance is obtained by the actions taken by developers, implementers, and operators in the specification, design, development, implementation, operation, and maintenance of security controls or through the actions taken by security control assessors to determine the extent to which the controls are implemented correctly, operating as intended, and providing the desired outcome with respect to meeting the security requirements for the system. The actions taken by the security control assessors will be addressed in the Assess FAQ.

The minimum assurance requirements levy requirements on the control developers/implementers of moderate- or high-impact systems to produce specific documentation supporting an increased confidence that the control meets its required function or purpose. In addition, for high-impact systems, the developer/implementer is expected to produce design and implementation documentation that supports component/integration testing. Developers/implementers of high-impact systems may also be required to develop records with structure and content suitable to support improvement in the effectiveness of the control.[88] These requirements must be identified and defined prior to the implementation of security controls.

Specific security controls within the NIST SP 800-53 security control catalog also levy requirements on the control developers/implementers. For example, SA-8, Security Engineering Principles, defines specific principles that are applied during the specification, design, development, implementation, and modification of moderate- and high-impact information system. Examples of security engineering principles include:[89]

- Developing layered protections;
- Establishing sound security policy, architecture, and controls as the foundation for design;
- Incorporating security into the system development life cycle;
- Delineating physical and logical security boundaries;
- Ensuring system developers and integrators are trained on how to develop secure software;
- Tailoring security controls to meet organizational and operational needs; and
- Reducing risk to acceptable levels, thus enabling informed risk management decisions.

46. WHY IS THE SELECTED SET OF SECURITY CONTROLS DOCUMENTED IN THE SECURITY PLAN?

The selected set of security controls along with the supporting rationale for selection decisions and any information system use restrictions are documented in the security plan for the information system. This documentation is essential when examining the security considerations for information systems with respect to potential mission/business impact. Documenting in the security plan any significant risk management decisions in the security control selection process is imperative in order for authorizing officials to have the necessary information to make credible, risk-based decisions regarding the authorization of organizational information systems. In addition, without such information, the understanding, assumptions, and rationale supporting those important risk decisions will, in all likelihood,

[88] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, pp. E-1-E-2

[89] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. F-100

not be available when the state of the information systems or environments of operation change, and the original risk decisions are revisited.[90]

47. WHAT INFORMATION IS DOCUMENTED IN THE SECURITY PLAN?

The security plan, prepared by the information system owner, provides an overview of the security requirements for the information system and describes the controls in place or planned for meeting those requirements.[91] The security requirements overview is described in sufficient detail to determine that the security controls selected would meet those requirements. In addition to the list of security controls to be implemented, the security plan documents the intended application of each control and assurance requirement in the context of the information system with sufficient detail to enable a compliant implementation of the control.[92]

Descriptive information about the information system is documented in the system identification section of the security plan, included in attachments to the plan, or referenced in other standard sources for information generated as part of the system development life cycle. Duplication of information is avoided, whenever possible. Information is added to the system description as it becomes available during the system development life cycle and execution of the Risk Management Framework tasks.[93]

The level of detail provided in the security plan is determined by the organization and is typically commensurate with the security categorization of the information system.[94] NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides detailed information on preparing the security plan.

48. DOES THE SECURITY PLAN HAVE TO FOLLOW THE FORMAT PROVIDED IN NIST SP 800-18?

No, organizations are not required to follow the security plan structure or template included in NIST 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.[95]

49. WHY ARE SECURITY CONTROLS MONITORED?

Organizations develop a strategy and implement a program for the continuous monitoring of security control effectiveness including the potential need to change or supplement the control set, taking into account any proposed/actual changes to the information system or its environment of operation.

---

[90] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, pp. 24-25

[91] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. F-1

[92] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 25

[93] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 21

[94] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 21

[95] NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006, p. vii

Conducting a thorough point-in-time assessment of the deployed security 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 security 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 security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system.[96]

50. WHAT IS THE CONTINUOUS MONITORING STRATEGY?

The continuous monitoring strategy for an information system identifies the security controls to be monitored, the frequency of monitoring, and the control assessment approach. The strategy also defines how changes to the information system will be monitored, how security impact analyses will be conducted, and the security status reporting requirements. The monitoring strategy can be included in the security plan.[97]

The authorizing official approves the monitoring strategy including the set of security controls that are to be monitored on an ongoing basis as well as the frequency of the monitoring activities. The approval of the monitoring strategy can be obtained in conjunction with the security plan approval.[98]

51. HOW ARE SECURITY CONTROLS SELECTED FOR CONTINUOUS MONITORING?

All security controls deployed within or inherited by organizational information systems are subject to continuous monitoring.[99] The criteria for determining the frequency of the monitoring is established by the information system owner in collaboration with other organizational officials. Security 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 consistent with the criticality of the function and capability of the monitoring tools.[100]

52. WHY IS THE SECURITY PLAN APPROVED?

An independent review of the security plan by the authorizing official with support from the senior information security officer, chief information officer, and risk executive (function), helps determine if the plan is complete, consistent, and satisfies the stated security requirements for the information system. The security plan review also helps to determine, to the greatest extent possible with available planning or operational documents, if the security plan correctly and effectively identifies the potential risk to

[96] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. G-1

[97] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 26

[98] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 26

[99] NIST Continuous Monitoring FAQs, www.csrc.nist.gov/SMA/fisma/faqs.html

[100] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 26

organizational operations and assets, individuals, other organizations, and the Nation, that would be incurred if the controls identified in the plan were implemented as intended.[101]

Based on the results of this independent review and analysis, the authorizing official may recommend changes to the security plan. If the security plan is deemed unacceptable, the authorizing official sends the plan back to the information system owner (or common control provider) for appropriate action. If the security plan is deemed acceptable, the authorizing official approves the plan.[102]

The acceptance of the security plan represents an important milestone in both the risk management process and the system development life cycle. The authorizing official, by approving the security plan, agrees to the set of security controls (system-specific, hybrid, or common) proposed to meet the security requirements for the information system. This approval allows the risk management process to advance to the Implement Step in the Risk Management Framework. The approval of the security plan also establishes the level of effort required to successfully complete the remainder of the steps in the Risk Management Framework and provides the basis of the security specification for the acquisition of the information system, subsystems, or components.[103]

[101] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 27

[102] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 27

[103] NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, p. 27