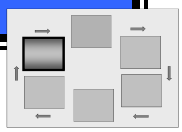
MONITOR STEP FAQS



NIST RISK MANAGEMENT FRAMEWORK

Continuous monitoring programs allow an organization to maintain the security authorization of an information system over time in a highly dynamic operating environment where systems adapt to changing threats, vulnerabilities, technologies, and mission/business processes. While the use of automated support tools is not required, risk management can become near real-time through the use of automated tools.

General Monitor Step FAQs

1. What is continuous monitoring and why is it important?
2. Who is responsible for implementing the continuous monitoring process for individual information systems or common security controls?
3. What is the role of the risk executive (function) in the continuous monitoring process?
4. Are automated tools required for continuous monitoring?
5. Can continuous monitoring results be used for annual FISMA reporting?
6. Are external service providers included in the continuous monitoring process?

Monitor Step Fundamentals

7. What is security configuration management?
8. What planning activities are involved in configuration management?
9. How is an information system configured to a secure state?
10. What is a security configuration checklist?
11. Are SCAP tools required for continuous monitoring?
12. What is a baseline configuration?
13. What is change management?
14. What is the information system component inventory?
15. What is a configuration control board?
16. How is a security impact analysis conducted?
17. Why should configurations be continuously monitored?
18. What measurements are required for configuration management?
19. How are security controls selected for continuous monitoring?
20. What is security control volatility?
21. Should common security controls be continuously monitored?
22. Do the results of continuous monitoring need to be documented and reported?
23. What is the plan of action and milestones?
24. How do the continuous monitoring assessment results influence the authorization decision?

Organizational Support for the Monitor Process FAQs

25. How should the organization support the continuous monitoring process?
26. Who is responsible for implementing an organizational continuous monitoring program?
27. Why should organizations integrate security into the system development life cycle?
28. What continuous monitoring guidance should the information security program office provide to information system owners?
29. How does the organization determine if the information system's security risk remains acceptable?
30. How does the organization use plans of action and milestones in its decision making process?

System-specific Application of the Monitor Process FAQs

31. What steps should the information system owner follow to implement continuous monitoring for an information system?
32. What is a continuous monitoring strategy?
33. What continuous monitoring information should be documented for an information system?
34. What types of changes to the information system or operating environment should be documented?
35. How does the information system owner conduct security impact analysis?
36. How does the information system owner assess a subset of the security controls?
37. How does the information system owner determine which remediation activities must be conducted for their information system?
38. Should the continuous monitoring process be used to update the security control baseline?
39. What critical security documentation is updated during the continuous monitoring process?
40. How does the information system owner report system status during the continuous monitoring process?
41. How does the authorizing official determine if the risk of operating an information system remains acceptable?
42. What are some examples of significant changes to an information system that could trigger a need to reauthorize a system?
43. What activities must the information system owner conduct when a system is decommissioned?

GENERAL MONITOR FAQS

1. WHAT IS CONTINUOUS MONITORING AND WHY IS IT IMPORTANT?

Continuous monitoring addresses the security impacts on information systems resulting from changes to the hardware, software, firmware, or the operational environment. The ultimate objective of continuous monitoring is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as in the environment in which the system operates. Continuous monitoring also provides an effective mechanism to update security plans, security assessment reports, and plans of action and milestones. An effective continuous monitoring process includes:[1]

- Configuration management and control processes for organizational information systems;
- Security impact analyses on actual or proposed changes to information systems and environments of operation;
- Assessment of selected security controls based on a continuous monitoring strategy;
- Security status reporting to appropriate organizational officials; and
- Active involvement by authorizing officials in the ongoing management of information system-related security risks.

[1] NIST SP 800-37, Revision 1, *Guide for Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, pp. 28-29

2. WHO IS RESPONSIBLE FOR IMPLEMENTING THE CONTINUOUS MONITORING PROCESS FOR INDIVIDUAL INFORMATION SYSTEMS OR COMMON SECURITY CONTROLS?

Information owners/information system owners manage the continuous monitoring process for their information systems while common control providers manage the continuous monitoring process for the security controls for which they are responsible. Initially, the information owner/information system owner[2] develops a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes in the information or its operating environment.[3] The information owner/information system owner selects which security controls to monitor and the frequency of the monitoring process, if not defined by organizational policy, with input from the authorizing official and risk executive (function). The selection of the security controls and the frequency with which they are monitored should reflect the organization's priorities and importance of the information system or, in the case of common controls, the information systems inheriting the controls.[4]

The information owner/information system owner also manages changes to the information system by documenting the proposed or actual changes to the information system or its operating environment, analyzing and determining the impact of those changes on the overall security state of the system,[5] determining the appropriate actions to take based on the security impact analysis,[6] and conducting any necessary remediation actions.[7]

3. WHAT IS THE ROLE OF THE RISK EXECUTIVE (FUNCTION) IN THE CONTINUOUS MONITORING 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.[8] During the continuous monitoring process, the risk executive (function) maintains the organization's overall risk posture based on the aggregated risk from each of the information systems and supporting infrastructures for which the organization is responsible[9] and provides that information to information owners/

[2] The common control provider conducts the same role as the information owner/information system owner to continuously monitor the common controls for which they are responsible. In this document the information owner/information system owner will be identified with the expectation that the common control provider conducts equivalent activities related to their common controls.

[3] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 50

[4] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 29

[5] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 29

[6] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 51

[7] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 52

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

[9] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 12

information system owners. This information is used to determine the continuous monitoring strategy, the criteria for selecting security controls and the frequency with which they are monitored,[10] and when information systems should be reauthorized.[11]

4. ARE AUTOMATED TOOLS REQUIRED FOR CONTINUOUS MONITORING?

No, automated tools are not required for continuous monitoring, but near real-time risk management can be achieved with continuous security control monitoring using automated support tools.[12] Organizations are strongly encouraged to use automated support tools in preparing and managing the content of the security authorization package to help provide an effective vehicle for maintaining and updating critical information for authorization officials regarding the ongoing security status of organizational information systems.[13]

Providing orderly and disciplined updates to the system security plan, security assessment report, and plan of action and milestones on an ongoing basis supports the principle of near real-time risk management and facilitates more cost-effective and meaningful reauthorization actions. Ultimately, with the use of automated tools and associated supporting databases, authorizing officials and other senior leaders within the organization should be able to obtain important information to maintain situational awareness with regard to the security state of the information systems supporting the organization's missions and business processes.[14]

5. CAN CONTINUOUS MONITORING RESULTS BE USED FOR ANNUAL FISMA REPORTING?

Yes, organizations can use the current year's continuous monitoring assessment results to meet the annual FISMA security control assessment requirement. To satisfy this requirement, organizations can draw upon the assessment results from various sources, including but not limited to: (i) security control assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring activities; or (iii) testing and evaluation of the information system as part of the system development life cycle process or audit (provided that the testing, evaluation, or audit results are current, relevant to the determination of security control effectiveness, and obtained by assessors with the required degree of independence required by the authorizing official).[15]

[10] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 50

[11] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 51

[12] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 25

[13] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 47

[14] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 47

[15] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 52

6. ARE EXTERNAL SERVICE PROVIDERS INCLUDED IN THE CONTINUOUS MONITORING PROCESS?

Yes, information systems managed or operated by external service providers also need to be continuously monitored. The authorizing official remains responsible for adequately mitigating risks to the organization's operations, assets, or individuals arising from the use of external information system services.[16] The information owner/information system owner and authorizing official establish a trust relationship with external service providers or mission/business partners. The specifics of establishing and maintaining trust can differ from organization to organization based on mission/business requirements, the participants involved in the trust relationship, the impact level of the information being shared or the types of services being rendered, and the risk to the organization participating in the relationship.[17]

The trust relationship depends on the actions taken by the participating/cooperating partners to implement appropriate security controls for the information system that comply with partnership agreements or contracts and the required evidence produced by the partnering organization to demonstrate that the controls have been implemented as intended[18] and remain implemented as intended.

Contracts with external service providers should require the providers to implement and use a configuration management process for the information systems that they operate and manage,[19] to provide regular security status reports that describe the continuous monitoring activities for the information system, and identify the changes made or planned during the reporting period.[20] The external service provider's configuration management process may require inclusion of an information owner/information system owner representative depending on the importance of the system to the organization's mission/business.

MONITOR FUNDAMENTALS

7. WHAT IS SECURITY CONFIGURATION MANAGEMENT?

Security configuration management is the management and control of security configurations for an information system to improve security and the management of risk. In an environment where attacks are growing in number and complexity, security is a preeminent concern among organizations trying to manage the risks to information systems that support their missions and business processes. Having better control of the misconfigurations that lead to vulnerabilities is fundamental to any security program. Through security configuration management, an organization is able to target and remediate vulnerabilities within an information system and also gain clarity into how well organization-wide

[16] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, Initial Public Draft, February 2009, p. 13

[17] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 17

[18] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 18

[19] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, Initial Public Draft, February 2009, p. F-88

[20] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 54

vulnerabilities have been addressed[21] and risks to the organization's operations have been mitigated. Security configuration management activities include:[22]

- Planning how configuration management will be applied to information systems within the framework established by the organization;
- Configuring information systems to a secure state as defined by the organization;
- Managing and controlling changes to information systems;
- Verifying and auditing the information systems to confirm that they have been configured to an expected security state; and
- Reporting on the overall security state of the information system environment.

Configuration management begins by establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently controlling any changes to the system, including additions and deletions,[23] and maintaining an accurate history of those changes.

Prior to any change implementation, the organization analyzes and tests proposed changes to the information system and determines the impacts of those changes on the system's functionality, performance, and security. If the change is approved and the information system is changed, the organization tests the security features of the system to verify that the features are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.[24]

8. WHAT PLANNING ACTIVITIES ARE INVOLVED IN CONFIGURATION MANAGEMENT?

Whether an organization is implementing configuration management for the first time or reengineering existing processes, planning is an important step. Typically, planning takes place at the organizational level, with flexibility in how configuration management is implemented often permitted for individual information systems.[25] As part of planning, organizations should clearly establish the scope of the configuration management effort that includes identifying the system boundary, its constituent parts, and the documentation that will be controlled through the process. Planning also includes developing the policy for the organization that requires the implementation of configuration management and defines the configuration management roles and responsibilities, use of configuration control boards, implementation of change control processes, use of tools and technology, use of standards for configuration settings and configuration baselines, conducting verification of system changes, and reporting on performance metrics related to configuration management.[26] It is also important to provide training for individuals who develop, support, and maintain information systems so that they employ the configuration management practices in a consistent manner. Training is also an opportunity to communicate the reasons why

[21] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[22] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[23] NIST SP 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004, p. 23

[24] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, Initial Public Draft, February 2009, p. F-35

[25] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[26] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

configuration management is a fundamental part of the security program as well as the technical procedures on how to conduct configuration management.[27]

9. HOW IS AN INFORMATION SYSTEM CONFIGURED TO A SECURE STATE?

After the configuration management process has been implemented, organizations should focus on deploying security configurations that put information systems into their most secure state. Configuration settings are parameters that can be changed in a hardware or software component of an information system that affect the component's functionality, performance, and security posture (e.g., minimum password length and maximum password age are two configuration settings related to the passwords that are used in a system component's identification and authentication function). Configuration settings impact a number of different aspects of an information system (including registry keys, files, directories, users, user groups, system or network services, configuration file entries, and graphical user interface controls)[28] that the information system's components employ to enforce a particular security policy.

Managing configuration settings is a difficult task due to the sheer number of software and hardware products found in an information environment, each with possibly hundreds of configuration settings. In light of the many possible configurations for an information system, the challenge for organizations is not only to find an overall configuration that creates a secure state, is cost effective, and supports important missions and business processes and existing technology, but to maintain that security state in the face of the significant changes that occur throughout organizations.[29]

Rather than spend resources determining how to address a bewildering array of possible configurations in hardware, software, and firmware products, organizations should established standards for security configurations. NIST has been instrumental in organizing a number of these standards into the National Checklist Program. These checklists cover a wide range of commercial products. In addition, automated support tools that are security content automation protocol (SCAP)-enabled support an organization's ability to identify and apply security configuration settings to a wide variety of technology products.[30] Most of the checklists available through the National Checklist Program are written in a standard format to facilitate automatic assessment through the SCAP-enabled tools.[31]

10. WHAT IS A SECURITY CONFIGURATION CHECKLIST?

A security configuration checklist (e.g., lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is essentially a document that contains instructions or procedures for securely configuring an information technology product to an operational environment. Some checklists also contain instructions or procedures for verifying that the product has been configured properly. Using well-written, standardized checklists can reduce the vulnerability exposure of information technology products and be particularly helpful to small organizations and individuals in securing their systems.[32]

[27] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[28] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[29] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[30] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[31] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[32] NIST SP 800-70, Revision 1, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, Draft, September 2008, p. 2-1

Whenever feasible, organizations should apply checklists to operating systems and applications to reduce the number of vulnerabilities that attackers can attempt to exploit and to lessen the impact of successful attacks. Using checklists improves the consistency and predictability of system security; however, there is no checklist that can make a system or product 100% secure. Using checklists does not eliminate the need for ongoing security maintenance, such as patch installation. However, using checklists that emphasize both hardening of systems against software flaws (e.g., by applying patches and eliminating unnecessary functionality) and configuring systems securely will typically reduce the number of ways in which the systems can be attacked, resulting in greater levels of product security and protection from future threats (e.g., zero-day vulnerabilities).[33]

Information technology vendors that configure their products using checklists that adhere to the security control baselines will not only provide more consistency in configuration settings within federal agencies but also provide a much more cost-effective method for establishing and verifying the minimum configuration settings, even if the agencies must modify the original checklists provided by checklist developers to fine-tune the configuration settings for their specific applications and operational environments.[34]

11. ARE SCAP TOOLS REQUIRED FOR CONTINUOUS MONITORING?

Yes, organizations should use SCAP-enabled tools when monitoring the use of security configurations as part of the continuous monitoring process. In fact, organizations are required to use SCAP tools to scan for both federal desktop core configuration (FDCC) security configuration settings and deviations from baseline configuration settings approved by their organization's authorizing official (see the SCAP website for additional information, http://nvd.nist.gov/scap.cfm).[35]

Currently, SCAP content is primarily focused on the Microsoft Windows operating systems. Additional platforms will be available in the future.[36] As additional platforms become available, use of SCAP tools to evaluate configurations settings within those products is highly recommended.

12. WHAT IS A BASELINE CONFIGURATION?

A baseline configuration is a well-defined, documented, and up-to-date specification to which the information system is built. Maintaining a baseline configuration involves creating new baselines as the information system changes over time and keeping old baselines available for possible rollback. A baseline configuration also provides information about the components of an information system and each component's makeup (e.g., the standard software for a notebook computer including updated patch information or security documentation such as user's guides) and the component's logical placement within the information system architecture. A baseline configuration for the information system should be consistent with the organization's enterprise architecture.[37]

[33] NIST SP 800-70, Revision 1, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, Draft, September 2008, p. ES-1

[34] NIST SP 800-70, Revision 1, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, Draft, September 2008, p. 2-3

[35] OMB Memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration*, August 11, 2008, p. 2

[36] NIST, http://nvd.nist.gov/validation.cfm

[37] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, Initial Public Draft, January 2009, p. F-33

13. WHAT IS CHANGE MANAGEMENT?

Change management is the process for managing and controlling a change from its proposal to implementation in an information system. Each step in the process should be clearly defined and articulated so that there is no confusion or misunderstanding about how changes should be handled and who is responsible for each step in the process. Although change management processes may vary, the basic steps include:[38]

- Request the proposed change;
- Document the request for the change and formally enter it into the change management process;
- Analyze the change for its impact on an information system's functionality, performance, and security;
- Approve, plan, schedule, and implement the change; and
- Confirm that the change was implemented properly and effectively.

In many cases, organizations will have some form of change management already in place. If so, implementing security configuration management will involve analyzing the change management process to ensure that it is functioning effectively[39] and, if security has not already been included, integrate security into the existing process. If the change management process is not functioning effectively, the organization should analyze the existing process and implement improvements, including integrating security into the process.

14. WHAT IS THE INFORMATION SYSTEM COMPONENT INVENTORY?

An information system component inventory is a repository that stores an accurate and logical representation of an information environment.[40] The inventory includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., component identifier, manufacturer, model number, serial number, software license information, system/component owner). The component inventory should be consistent with the system boundary. Each organization should determine the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking and reporting).[41]

15. WHAT IS A CONFIGURATION CONTROL BOARD?

A configuration control board is a group of technical and management personnel that analyzes, approves, and schedules changes to an information system. It represents various perspectives from within the organization and evaluates and approves changes for one or more information systems. The configuration control board assures that proposed changes are held to organizationally-defined standards (e.g., within scope, cost-effective, limited impact on security) before being implemented.[42]

Depending on the size and complexity of its information environment, an organization can have many configuration control boards. The information system may require its own dedicated configuration

[38] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[39] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[40] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[41] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, Initial Public Draft, February 2009, p. F-39

[42] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

control board if it has a large number of components, is a moderate- or high-impact system, processes a large number of modifications, or is critical to the mission and business processes of the organization. In other cases, a configuration control board may provide oversight for a number of information systems.[43]

A configuration control board is typically established by a charter that defines the authority of the group and how it operates. The charter should define the membership, the roles and responsibilities of its members, and whether or not it reports to an oversight body. The charter should also describe how the configuration control board handles normal and emergency changes and should address aspects such as the range of dispositions (e.g., approved, not approved, on-hold), evaluation criteria, and criteria for a quorum of members to call a vote. The configuration control board membership should include mission/business users, other end users, information system security engineers, information technology specialists, customers, and vendors. While not all board members are required to have voting rights, their perspectives and inputs provide improved decision making within the configuration control board.[44]

A configuration control board follows a disciplined, systematic approach for introducing change to the information environment. While no two changes are alike, having a clearly defined process or framework for the evaluation and approval of change requests, including predefined evaluation criteria, helps to ensure that each proposed change is evaluated in a consistent and dependable manner according to the appropriate business and technical viewpoints.[45]

In addition to reviewing and adjudicating proposed changes to information systems, the configuration control board provides oversight for security configuration management activities related to the information systems within its jurisdiction. For the information systems represented within the configuration control board, the board is responsible for:

- Validating that a security configuration management plan has been developed and implemented according to organizational policy and is up-to-date;
- Approving initial configuration baselines and evaluating changes for their impacts on those baselines;
- Ensuring that configuration settings are implemented according to defined policy and approving exceptions to that policy;
- Verifying that the component inventory is current and reflects the actual state of the information environment;
- Identifying, remediating, and addressing issues on unauthorized changes and misconfigurations; and
- Consulting applicable technical personnel to determine alternatives for implementing proposed changes to the system's information technology components and to determine the feasibility, effectiveness, urgency, and costs of proposed implementations.

16. HOW IS A SECURITY IMPACT ANALYSIS CONDUCTED?

Security impact analysis is implemented as part of the change management process. While change is a necessary aspect of any information environment, it does not mean that any and all changes should be accepted. Each proposed change should be examined to determine its impacts on the functionality, performance, and security of the information system. If the change impacts security, the configuration

[43] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[44] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[45] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

control board will need to take steps to reduce the vulnerability if the security risk introduced by the change cannot be mitigated.[46]

An initial security impact analysis should be conducted before the change is approved by the configuration control board. If there are security concerns with a proposed change, especially those changes significant enough to influence the decision of the configuration control board, they can be modified before expending time and energy in building, testing, and rolling out the change.[47]

Security impact analysis is not a one-time event that is used to support the decisions of the configuration control board when approving changes. When a change is initially proposed, the manner in which it will be built and implemented may not be known. Therefore, a security impact analysis before deployment should be an ongoing activity that is integrated into the system development life cycle so that at each stage until the change is released to production, the impact on security is being considered.[48]

The process for a security impact analysis consists of the following steps:[49]

- Understand the change in a system change request;
- Identify vulnerabilities that the proposed change may introduce;
- Assess risks to the information system, system users, and the organization's mission/business functions;
- Assess security controls that are impacted by the proposed change;
- Plan safeguards and countermeasures to the identified impacts; and
- Update critical security documentation to reflect the changes made to the information system.

When a change is being proposed, the information owner/information system owner should develop a high-level architecture overview that shows how the change will be implemented. If the change has already been initiated, the functional and technical design documents should be analyzed to gain insight into the change. If the change involves a hardware or software product, identifying vulnerabilities may require a search of vulnerability databases such as those provided for SCAP that enumerate vulnerabilities and misconfigurations. Organizations can leverage this information to address known issues and remove them before they become a concern. If the change includes custom development, a more in-dept analysis is required.[50]

Once a vulnerability has been identified, a risk assessment is needed to identify the likelihood of a threat exercising that vulnerability and the impact of such an event. If a vulnerability is identified, the assessed security risk may be low enough that the risk can be accepted and the change approved without remediation. In other cases, the security risk may be significant and safeguards and countermeasures are required to reduce the risk prior to approving the requested change. Occasionally, the potential security risk to implement a change may be too high and the requested change is not approved.

In addition to assessing the security risk from the change, organizations should also analyze whether a change will impact existing security controls. For example, if a database is used to support auditing

[46] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[47] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[48] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[49] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[50] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

controls and is being upgraded to the latest version, procedures or reports might have to be rewritten to work with the new version. Therefore, when proposing, developing, and implementing changes, organizations should review the list of the information system's security controls and update the system security plan to reflect any changes.[51]

In cases where security risks have been identified, organizations can use the security impact analysis process to identify and plan safeguards and countermeasures to reduce the risk. For instance, if buffer overflow and SQL injection attacks are identified as vulnerabilities for a high-traffic, public-facing web application, the organization can instruct developers to implement field validations to check input length and text.[52]

17. WHY SHOULD CONFIGURATIONS BE CONTINUOUSLY MONITORED?

Continuous monitoring is used as the assessment mechanism that supports configuration management and periodically validates that information systems within the information environment are configured as expected. Planning and implementing security configurations and then managing and controlling change is not a guarantee that information systems will remain configured as expected. Using automated tools, organizations can identify when the information system is not in compliance with security policy and standards and take remediation actions as necessary. Continuous monitoring identifies undiscovered system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which, if not addressed, can expose organizations to increased risk.[53]

18. WHAT MEASUREMENTS ARE REQUIRED FOR CONFIGURATION MANAGEMENT?

Measurements/metrics allow the organization to not only understand the overall security state of an information system, but to measure the performance of the configuration management in controlling the information system. Information owners/information system owners can use measures and reports to identify and address vulnerabilities as well as to improve the processes required to support configuration management.

Configuration management measures and reports should be carried out in a standardized and consistent manner across the organization. Adopting SCAP-enabled tools that confirm whether a system component's configuration complies with applicable standards and policies (e.g., the Federal Desktop Core Configuration) enables standard and consistent measures for scoring and prioritizing vulnerabilities and misconfigurations. The benefit is that all vulnerability and misconfiguration communications precisely identify the relevant issues, enable integration of data feeds using this same standardized language, and enable easy correlation with other data repositories that may have additional information on the relevant vulnerabilities.

The information provided by SCAP-enabled products and other tools can be integrated as part of a comprehensive reporting program that combines information from various operational activities and databases. This can be achieved by integrating vulnerability and configuration databases, the information

[51] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[52] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[53] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

system component inventory, incident databases, and intrusion detection databases, using SCAP data as primary keying material.[54]

Reports on the latest changes to the component inventory within the reporting period can be used as the basis for verifying whether the approved and tested changes to the system that were scheduled for that period were indeed made to those components. Likewise, status reports from the configuration control board that identify the proposed changes (in the form of a system change request) that were received, evaluated, and implemented during a specified period can be used to ensure that all proposed changes have been processed.

19. HOW ARE SECURITY CONTROLS SELECTED FOR CONTINUOUS MONITORING?

If the security controls are not selected at the organizational level, the information owner/information system owner should use recent risk assessment results, results of previous security assessments, and operational requirements of the system in selecting the security controls to be monitored and the frequency of the monitoring process.

Priority for control monitoring should be given to the security controls that have the greatest volatility (i.e., greatest potential for change) after implementation and the controls that have been identified in the plan of action and milestones document for the information system (e.g., controls that have been deemed to be ineffective to some degree).[55]

20. WHAT IS SECURITY CONTROL VOLATILITY?

Security control volatility is a measure of how frequently a control implementation is likely to change over time. For example, a security control for implementing policies and procedures in a particular organization is not likely to change from one year to the next and would, therefore, be considered a security control with low volatility. However, access control mechanisms or other technical controls that are subject to the direct effects or side effects of frequent changes in the hardware, software, or firmware components of an information system (e.g., software patches, new version of a firewall product) would indicate security controls with higher volatility. Organizations should apply greater resources to monitor security controls deemed to be of higher volatility as there is typically a higher return on investment for assessing security controls of this type. [56]

21. SHOULD COMMON SECURITY CONTROLS BE CONTINUOUSLY MONITORED?

Yes, common security controls should be continuously monitored in a process similar to the process followed for system-specific security controls. The common control provider (e.g., facility manager, site manager, network manager/administrator, personnel manager) is responsible for the development, implementation, assessment, and maintenance of common controls.[57]

[54] NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008

[55] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 29

[56] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 43

[57] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 14

The senior agency information security officer, acting on behalf of the chief information officer, is responsible for coordinating with the common control providers that develop and implement the common controls to ensure that the required controls are put into place, the controls are assessed, and the assessment results are shared with the information owners/information system owners of the information systems that employ those common controls.[58]

22. DO THE RESULTS OF CONTINUOUS MONITORING NEED TO BE DOCUMENTED AND REPORTED?

Yes, the results of each continuous monitoring effort need to be documented in security status reports and reported to the authorizing official and senior agency information security officer periodically[59] as defined in organizational policies or guidelines. The results of the continuous monitoring effort need to be reflected in updates to the system security plan, security assessment report, and plans of action and milestones document.[60]

The frequency of updates to critical authorization-related documents (i.e., system security plan, security assessment report, plan of action and milestones) is at the discretion of information owners/information system owners and authorizing officials in accordance with federal and organizational policies. Updates should be accurate and timely since the information provided influences ongoing security-related actions and decisions by authorization officials and senior leaders within the organization with either direct or indirect responsibility for the ongoing management of information system-related security risks.[61]

23. WHAT IS THE PLAN OF ACTION AND MILESTONES?

The plan of action and milestones, prepared by the information owner/information system owner, describes the specific measures that are planned: (i) to correct weaknesses or deficiencies noted in the security controls during security control assessment; and (ii) to address known vulnerabilities in the information system. The most effective plans of action and milestones contain a robust set of actual and potential weaknesses or deficiencies identified in the security controls deployed in the information system or inherited by the information system. Plans of action and milestones document the following:[62]

- Security category and impact level for the information system;
- Specific weaknesses or deficiencies in the information system security controls;
- Importance of the identified security control weaknesses or deficiencies (i.e., the direct or indirect effects that the weaknesses or deficiencies may have on the overall security state of the information system and on the risk exposure of the organization);
- Organization's proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g., identification of risk mitigation actions, prioritization of

[58] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, Initial Public Draft, February 2009, p. 11

[59] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 30

[60] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 53

[61] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 53

[62] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 22

risk mitigation actions, allocation of risk mitigation resources, schedule of milestones to mitigate or correct identified weaknesses or deficiencies); and
- Organization's rationale for accepting certain weaknesses or deficiencies in the security controls.

Planned changes to the system to correct weaknesses or deficiencies in the security control implementations identified during a security control assessment should also be documented in system change requests for processing by the configuration control board.

24. HOW DO THE CONTINUOUS MONITORING ASSESSMENT RESULTS IMPACT THE AUTHORIZATION DECISION?

The organization determines the impact of the continuous monitoring results on the authorization decision of the system and, if necessary, allocates applicable resources for addressing any weaknesses identified in the continuous monitoring effort. Since organizations operate in dynamic environments with constantly changing threats, vulnerabilities, and technologies, authorization decisions and the acceptance of security risk associated with those decisions need to be revisited on a regular basis[63] and adjusted based on the results of the continuous monitoring process.

A robust and comprehensive continuous monitoring strategy that is integrated in the ongoing system development life cycle process carried out by an organization can significantly reduce the resources required for reauthorizing information systems. Risk management can become near real-time with continuous security control monitoring by using automated support tools. When continuous monitoring is conducted in accordance with the information needs of the authorizing official, the authorizing official can determine the current security state of the information system, the security risks that may result from the system's operation, and whether to authorize continued operation of the system.

The goal is to employ ongoing authorizations for which the authorizing official maintains sufficient knowledge of the current security state of the information system and the risk the information system poses to the organization's operations to determine whether continued system operation is acceptable and, if not, to determine which steps of the Risk Management Framework need to be executed to adequately mitigate the risk.[64]

ORGANIZATIONAL SUPPORT FOR THE MONITOR PROCESS FAQS

25. HOW SHOULD THE ORGANIZATION SUPPORT THE CONTINUOUS MONITORING PROCESS?

To effectively manage the continuous monitoring process, organizations should implement a continuous monitoring program.[65] The organizational continuous monitoring program should require organization-wide participation in the change control process, establish the organization's criteria for selecting an

[63] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 43

[64] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 25

[65] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 28

appropriate subset of security controls for ongoing monitoring, determine the frequency and schedule for the monitoring process, and define the reporting requirements. The continuous monitoring program provides the information on the overall security status of the organization and the ability of the organization's information systems to adequately protect, to the degree necessary, the missions and business functions of the organization. In addition, continuous monitoring should become an integrated and tightly coupled part of the system development life cycle to ensure that security remains an effective part of the organization's information systems, security documents are updated and maintained,[66] and the security impacts of information system changes are evaluated and controlled.[67]

26. WHO IS RESPONSIBLE FOR IMPLEMENTING AN ORGANIZATIONAL CONTINUOUS MONITORING PROGRAM?

The information security program office, under the direction of the senior agency information security officer, is responsible for implementing an organizational continuous monitoring program. The continuous monitoring program allows an organization to: (i) track the security state of its information systems on a continuous basis; and (ii) maintain the security authorization for systems over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and mission/business processes. A robust continuous monitoring program requires the active involvement of information owners/information system owners, common control providers, risk executive (function), chief information officers, senior agency information security officers, authorizing officials,[68] and the organization's technical operations personnel.

The continuous monitoring program includes responsibilities such as ensuring continuous monitoring is integrated into the system development life cycle, providing guidance to the organization on how to develop their continuous monitoring strategies and how to select security controls for continuous monitoring, integrating continuous monitoring with existing organizational change control/configuration management processes, evaluating security status reports and plans of action and milestones provided by information owners/information system owners, and providing organizational decision making guidance when allocating resources to mitigate identified weaknesses and deficiencies.

27. WHY SHOULD ORGANIZATIONS INTEGRATE SECURITY INTO THE SYSTEM DEVELOPMENT LIFE CYCLE?

All federal information systems, including operational systems, systems under development, and systems undergoing some form of modification or upgrade, are in some phase of the system development life cycle. The Risk Management Framework provides a framework for dynamically managing risk throughout the system development life cycle and helps to ensure that appropriate security controls for the information system are developed, implemented, assessed for effectiveness, and maintained. Integrating security requirements into the system development life cycle is the most efficient and cost-effective method for an organization to ensure that its protection strategy is achieved and that authorization activities are not isolated or decoupled from the management process employed by the organization to develop, implement, operate, and maintain information systems supporting ongoing missions or business functions. Security tasks should begin early in the system development life cycle, typically during the

[66] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 30

[67] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 29

[68] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 28

system initiation phase and are important in shaping and influencing the security capabilities of the system.[69]

28. WHAT CONTINUOUS MONITORING GUIDANCE SHOULD THE INFORMATION SECURITY PROGRAM OFFICE PROVIDE TO INFORMATION SYSTEM OWNERS?

The information security program office should provide guidance to information owners/information system owners that establishes the organization's expectations for managing changes to information systems or system component configurations; criteria for selecting the security controls to be monitored during the continuous monitoring process; [70] guidance on preparing security status reports, the frequency with which the reports should be produced, and who should receive the reports; guidance on how the plan of action and milestones will be reviewed and used for allocation of organizational resources; and the security activities that should be completed when information systems are decommissioned.

The organization must make informed decisions regarding the application of assessment resources for conducting continuous monitoring activities to ensure that the expenditures are consistent with the organization's mission requirements, security categorizations, and assessment requirements articulated in federal legislation, policy, directives, and regulations.[71] The information security program office, in collaboration with the chief information officer, senior agency information security officer, and risk executive (function), provides guidance and direction to information owners/information system owners to follow when making resource decisions.

29. HOW DOES THE ORGANIZATION DETERMINE IF THE INFORMATION SYSTEM'S SECURITY RISK REMAINS ACCEPTABLE?

The authorizing official periodically reviews the security status reports for organizational information systems to determine the current security risk of the system to organizational operations and assets, individuals, other organizations, or the Nation. It is the responsibility of the authorizing official to determine, with appropriate inputs from the senior agency information security officer and the risk executive (function), whether the current security risk is acceptable and to forward appropriate direction to information owners/information system owners.

The use of automated support tools to capture, organize, and maintain security status information promotes the concept of near real-time risk management through ongoing situational awareness regarding the overall risk posture of the organization. The security risks being incurred may change over time based on the information provided in the security status reports. Determining how the changing conditions affect the mission/business risks associated with organizational information systems is essential for maintaining adequate security. By carrying out ongoing risk determination and risk acceptance, authorizing officials can manage the security authorization over time.[72]

[69] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 7

[70] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, pp. 29-30

[71] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 30

[72] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 55

30. HOW DOES THE ORGANIZATION USE PLANS OF ACTION AND MILESTONES IN ITS DECISION MAKING PROCESS?

The organization should define a strategy that facilitates a prioritized approach to risk mitigation that is consistent across the organization since most information systems have more vulnerabilities than available resources can address.[73] Organizational strategies for plans of action and milestones should be guided by the impact level of the respective information systems affected by the risk mitigation activities. An organization may decide, for example, to allocate the vast majority of risk mitigation resources initially to the highest impact information systems because a failure to correct the weaknesses or deficiencies in those systems could potentially have the most significant adverse effects on the organization's missions or business operations. An organization should also prioritize weaknesses or deficiencies within its categorized information systems; a high-impact system would have a prioritized list of weaknesses and deficiencies for that system, as would moderate-impact and low-impact systems. In general, the organization-wide plan of action and milestones strategy should always address the highest priority weaknesses or deficiencies within those prioritized systems.[74]

When weaknesses or deficiencies in security controls are corrected, the remediated controls are reassessed to determine the extent to which the remediated controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

SYSTEM-SPECIFIC APPLICATION OF THE MONITOR PROCESS FAQS

31. WHAT STEPS SHOULD THE INFORMATION SYSTEM OWNER FOLLOW TO IMPLEMENT CONTINUOUS MONITORING FOR AN INFORMATION SYSTEM?

To implement a continuous monitoring process for an information system, the information owner/ information system owner should develop a strategy for conducting the required continuous monitoring activities, document changes to the information system or operating environment, determine the security impact of the proposed changes, assess a subset of security controls following a predefined schedule throughout the authorization period, conduct remediation activities as needed, update the selection of security controls for the information system, update critical security documentation, provide security status reports to senior organizational leaders, determine if the risk of the system's operation remains acceptable throughout the system's life cycle, and define and implement a decommissioning strategy when an information system is removed from operation.

Prepare for Continuous Monitoring

Continuous monitoring begins after an information system has been authorized for use; therefore, security documentation, such as the system security plan, risk assessment, plan of action and milestones, and other security related documentation (e.g., vulnerability scanning results, results of last contingency plan test) already exists. The information owner/information system owner should have or obtain this information and provide it to the individuals responsible for the continuous monitoring of the information system.

[73] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 22

[74] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 22

Develop a Continuous Monitoring Strategy

The information owner/information system owner should develop a strategy to monitor the information system during the organization-defined authorization period that is consistent with the organization's continuous monitoring program[75] if it has not already been defined by organizational policy. The continuous monitoring strategy should be documented for the information system or for a group of related information systems. [See questions 32-33 on developing and documenting the continuous monitoring strategy.]

Document Changes to the Information System or Operating Environment

The information owner/information system owner should document any relevant information about proposed or actual changes to the hardware, software, or firmware, descriptions of new or modified features/capabilities, security implementation guidance, or changes to the information system's operating environment. The information owner/information system owner should use this information in assessing the potential security impact of the changes.[76] [See question 34 on documenting changes to the information system or operating environment.]

Determine Impact of the Proposed Changes

The information owner/information system owner should conduct a security impact analysis to determine the extent to which changes to the information system or its operating environment will affect the security state of the system. [See question 35 on conducting the security impact analysis.]

Assess a Subset of Security Controls

After the initial authorization and in accordance with OMB policy and organizational guidance regarding the authorization period, the information owner/information system owner should assess a subset of the security controls. [See question 36 on assessing the selected subset of security controls.]

Conduct Remediation Activities

The information owner/information system owner should initiate remediation actions based on the findings produced during the assessment of the system's security controls, the outstanding items listed in the plan of action and milestones, and the results of performing the activities required by the security controls (e.g., vulnerability scanning, contingency plan testing, incident response handling). [See question 37 on conducting remediation activities.]

Update the Selected Security Controls

The organization should periodically determine if there is a need to update the current, agreed upon security controls of its information systems that are documented in the security plan and implemented within the information system by revisiting on a regular basis the risk management activities described in the Risk Management Framework. Additionally, events such as security incidents, new OMB policies, new threat/vulnerabilities, and new technologies may trigger the immediate need to assess the security

[75] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 50

[76] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 51

state of the information system and require, if needed, an update of the current security controls.[77] [See question 38 for guidance on updating the selected security controls.]

Update Critical Security Documentation

The information owner/information system owner should update the system security plan and the plan of actions and milestones while security assessors should update the security assessment report. [See question 39 on updating critical security documentation.]

Report Status in Security Status Reports

Information owners/information system owners should document the results of continuous monitoring activities in security status reports and provide the reports to the authorizing official. At a minimum, security status reports should summarize key changes to security plans (including risk assessments), security assessment reports, and plans of action and milestones. [See question 40 on monitoring security status reports.]

Determine if Risk Remains Acceptable

The authorizing official should review the security status reports to determine if the current risk of the information system to organizational operations and assets, individuals, other organizations, or the Nation remains acceptable and forward appropriate direction to the information owner/information system owner. [78] The information owner/information system owner should address the direction provided by the authorizing official to maintain the security status of the information system. [See questions 41-42 on system reauthorization.]

Implement a Decommissioning Strategy

When an information system is removed from operation, the information owner/information system owner should ensure that all security controls addressing information system decommission (e.g., media sanitization and disposal, configuration management and control) are implemented. [See question 43 on decommissioning an information system.]

32. WHAT IS A CONTINUOUS MONITORING STRATEGY?

A continuous monitoring strategy is a plan that describes how the information owner/information system owner will monitor the security controls applied to the information systems under his or her management and manage proposed and actual changes to the information system or it operating environment. If the organization implements continuous monitoring as a common or hybrid security control, the information owner/information system owner is expected to implement the organization-wide continuous monitoring strategy that may also include the organizationally-defined security controls for ongoing monitoring.

The strategy (if not defined by organizational policy) should establish configuration management and control processes to support the continuous monitoring activities. The continuous monitoring strategy should also address the requirement to conduct security impact analyses to determine the extent to which proposed or actual changes to the system or its operating environment will affect the security state of the

[77] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, Initial Public Draft, February 2009, p. 23

[78] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 55

system.[79] The strategy should also define the process for selecting the security controls to be monitored and the frequency of the monitoring process.[80] Security controls that are volatile or critical to protecting the information system should be assessed at least annually. All other controls should be assessed at least once during the information system's authorization cycle.[81]

After the information owner/information system owner and authorizing official agree on the subset of security controls and the frequency of the monitoring activity, the strategy is approved by the authorizing official and senior agency information security officer.[82]

33. WHAT CONTINUOUS MONITORING INFORMATION SHOULD BE DOCUMENTED FOR AN INFORMATION SYSTEM?

Information owners/information system owners should document their strategies for managing changes to their information systems, their roles and responsibilities in the configuration management process, and the methodologies that they will follow to monitor the security controls of their information systems. The strategy can be documented in a continuous monitoring plan, in the organization's policies and procedures, or in other organizationally defined documents.

The documentation should identify the security controls that will be monitored, the frequency with which those controls will be monitored, the security controls deemed volatile, the continuous monitoring schedule, and the conditions that could alter the control selection and assessment schedule.

34. WHAT TYPES OF CHANGES TO THE INFORMATION SYSTEM OR OPERATING ENVIRONMENT SHOULD BE DOCUMENTED?

The information owner/information system owner documents any relevant information about specific changes to the hardware, software, or firmware (e.g., version or release numbers), descriptions of new or modified features/capabilities (e.g., new search function or additional reporting capability), and security implementation guidance (e.g., Oracle security implementation guidance or firewall configuration guidance). It is also important to document any changes to the information system's operating environment such as modifications to hosting facilities or organizational processes and procedures. The information owner/information system owner should use this information in assessing the potential security impact of the changes.[83]

Documenting proposed and actual changes to the information system or its operating environment and subsequently assessing the potential impact that those changes may have on the overall security state of the system or the organization is an important aspect of security control monitoring, achieving situational

[79] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 51

[80] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 43

[81] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, pp. 29-30

[82] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 50

[83] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 51

awareness, and maintaining the security authorization. Information system changes should not be made prior to assessing the security impact of those changes.[84]

35. HOW DOES THE INFORMATION SYSTEM OWNER CONDUCT A SECURITY IMPACT ANALYSIS?

The information owner/information system owner conducts a security impact analysis to determine the extent to which proposed or actual changes to the information system or its operating environment affect the security state of the system. Changes to the information system or its operating environment may affect the security controls currently in place, produce new vulnerabilities in the system, or generate requirements for new security controls that were not previously needed. In assessing a change's impact, the information owner/information system owner should consider the new or modified features and capabilities that the change will provide, any changes that are made to the operating environment (e.g., updates to the rules of behavior, providing physical security of a new system component), and the criticality of the change regarding system operation.

If the information system contains information technology components for which there exist SCAP-enabled tools, the information owner/information system owner should monitor compliance of the component's configuration using the SCAP-validated tools.[85]

If the results of the security impact analysis indicate that the proposed or actual changes to the information system will affect or have affected the security state of the system, corrective actions should be initiated and the appropriate documents revised/updated. The authorizing official or designated representative should use the revised/updated security assessment report, security status reports, and plans of action and milestones along with input from the senior agency information security officer and risk executive (function) to determine if a reauthorization action is necessary.[86]

36. HOW DOES THE INFORMATION SYSTEM OWNER ASSESS A SUBSET OF THE SECURITY CONTROLS?

After the initial authorization, the information owner/information system owner assesses a subset of the security controls in accordance with OMB policy and organizational guidance. The selection of an appropriate subset of security controls to monitor and the frequency of monitoring is based on the system's continuous monitoring strategy.[87] Security controls are assessed following the guidance and assessment procedures in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, and previously developed security assessment plans and procedures.[88]

[84] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 51

[85] OMB Memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration*, August 11, 2008, p. 2

[86] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 51

[87] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 52

[88] NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008, p. 6

37. HOW DOES THE INFORMATION SYSTEM OWNER DETERMINE WHICH REMEDIATION ACTIONS SHOULD BE CONDUCTED FOR THEIR INFORMATION SYSTEM?

The information owner/information system owner reviews the recommended remediation actions included in the findings produced during the assessment of the system's security controls, the outstanding items listed in the plan of action and milestones,[89] and the results of performing the activities required by the security controls (e.g., vulnerability scanning, contingency plan testing, incident response handling). By using the assessment results of *satisfied* and *other than satisfied*, information owners/information system owners gain a better understanding of the specific weaknesses and deficiencies in the information systems and decide how (or if) to mitigate risks in accordance with organizational priorities. The information owner/information system owner applies his or her judgment with regard to the severity or seriousness of each finding to determine whether the finding is significant enough to warrant further investigation or remedial action.[90]

The information owner/information system owner, with the concurrence of designated organizational officials (e.g., authorizing official, chief information officer, senior agency information security officer, mission owners), determines how and when to conduct the selected remediation activities to correct the identified weaknesses and deficiencies.[91] Security controls modified, enhanced, or added during this process should be reassessed by the assessor to ensure that appropriate actions have been taken to eliminate weaknesses or deficiencies or mitigate the identified risk.[92]

38. SHOULD THE CONTINUOUS MONITORING PROCESS BE USED TO UPDATE THE SECURITY CONTROL BASELINE?

Yes, organizations should initiate specific actions to determine if there is a need to update the selection of security controls documented in the security plan and implemented within the information system. Specifically, the organization should review, on a regular basis, its risk management activities as defined in the NIST Risk Management Framework. Additionally, events can trigger the immediate need to assess the security state of the information system and, if required, to update the security controls. Examples of these events include: [93]

- An incident results in a breach to the information system, producing a loss of confidence in the confidentiality, integrity, or availability of the information processed, stored, or transmitted by the system;
- A newly identified, credible information system-related threat to the organization's operations or assets, individuals, other organizations, or the Nation is identified based intelligence information, law enforcement information, or other credible sources of information;

[89] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 52

[90] NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008, p. 25

[91] NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008, p. 25

[92] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 52

[93] NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, Initial Public Draft, February 2009, p. 23

- 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
- Regulatory changes require changes in policies and procedures.

39. WHAT CRITICAL SECURITY DOCUMENTATION IS UPDATED DURING THE CONTINUOUS MONITORING PROCESS?

The information owner/information system owner updates the system security plan and the plan of actions and milestones. Updated security plans should reflect any modifications to security controls based on risk mitigation activities (e.g., modifying, enhancing, or adding security controls). Updated plans of action and milestones should report progress made on the current outstanding items listed in the plan, address vulnerabilities in the information system discovered during the security impact analysis or security control monitoring, and describe how the information owner/information system owner intends to address those vulnerabilities. Security assessors update the security assessment report. Updated security assessment reports should reflect the results of additional assessment activities carried out to determine security control effectiveness.[94]

The frequency of updates to critical authorization-related documents (e.g., system security plan, security assessment report, plan of action and milestones) is at the discretion of the information owner/information system owner and the authorizing official in accordance with federal and organization policies. When updating critical information in documents, the information owner/information system owner should ensure that the original version of the document is preserved and available for oversight, management, and auditing purposes.[95]

40. HOW DOES THE INFORMATION SYSTEM OWNER REPORT SYSTEM STATUS DURING THE CONTINUOUS MONITORING PROCESS?

Information owners/information system owners should document the results of continuous monitoring activities in security status reports and provide them to the authorizing official. The security status reports should describe the continuous monitoring activity, address the vulnerabilities discovered during the security control assessment, security impact analysis, or security control monitoring, and the information owner/information system owner's plans to address those vulnerabilities. At a minimum, security status reports should summarize key changes to security plans (including risk assessments), security assessment reports, and plans of action and milestones. Security status reports should be provided at appropriate intervals to transmit significant security-related information about the information system in accordance with federal and organizational policies, but not so frequently as to generate unnecessary work. Security status reports should be appropriately marked, protected, and handled.[96]

[94] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 53

[95] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 53

[96] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 54

41. HOW DOES THE AUTHORIZING OFFICIAL DETERMINE IF THE RISK OF OPERATING AN INFORMATION SYSTEM REMAINS ACCEPTABLE?

The authorizing official or designated representative may need to reauthorize an information system depending on the severity of an event, the impact of an event or change in organizational operations, organizational assets, or on individuals, and the extent of the corrective actions required to fix the identified deficiencies in an information system. The authorizing official reviews the security status reports and updated plans of action and milestones to determine if reauthorization is required based on the current determination of risk.

The authorizing official makes the final determination for the need to reauthorize (for which an assessment of all of an information system's security controls is conducted) the information system in consultation with the information owner/information system owner, the senior agency information security officer, risk executive (function), and chief information officer.

If the authorizing official determines that reauthorization is necessary, the authorizing official documents the required actions in an authorization decision document that transmits an updated authorization decision to the information owner/information system owner and other key organizational officials. The authorization decision document identifies why reauthorization is needed, the terms and conditions for the authorization including what steps within the Risk Management Framework should be completed, and the expected completion date for the reauthorization efforts.[97] The information owner/information system owner addresses the direction provided by the authorizing official to maintain the security status of the information system.

42. WHAT ARE SOME EXAMPLES OF SIGNIFICANT CHANGES TO AN INFORMATION SYSTEM THAT COULD TRIGGER A NEED TO REAUTHORIZE A SYSTEM?

The information owner/information system owner should reconsider the reauthorization decision when significant changes occur to an information system or its operating environment. Examples of potential significant changes to an information system that should be reviewed for possible reauthorization decisions include, but are not limited to:

- Installation of a new or upgraded operating system, middleware component, or application;
- Modifications to system ports, protocols, or services;
- Installation of a new or upgraded hardware platform or firmware component; or
- Modifications to cryptographic modules or services.

Changes in laws, directive, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reauthorization action. Reauthorization should be avoided in situations where the continuous monitoring process provides the necessary and sufficient information to authorizing officials to manage the potential risk arising from the information system changes.[98]

[97] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 25

[98] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 26

43. WHAT ACTIVITIES SHOULD THE INFORMATION SYSTEM OWNER CONDUCT WHEN A SYSTEM IS DECOMMISSIONED?

When an information system is removed from operation, the information owner/information system owner should ensure that all security controls addressing information system decommission (e.g., media sanitization, configuration management) are implemented and that the organization's tracking and management systems are updated to indicate the specific information system components that are being removed from the system's inventory. The information owner/information system owner should also reflect the new status of the information system in the security status reports, notify users and owners of applications running on the decommissioned information system, and review and assess any security control inheritance relationships for their security impacts.[99]

[99] NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008, p. 55