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

NIST Risk Management Framework (RMF) Monitor Step

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

Contents

General Monitor Step FAQs

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

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

- Tasks in Revision 2 place greater emphasis and reliance on continuous monitoring in support of ongoing assessments and ongoing authorizations.
- Task 6-6 in Revision 1 has been incorporated into Tasks M-1, M-2, and M-6 in Revision 2.
- Task M-6 in Revision 2 has been introduced for ongoing authorization.
- Continuous monitoring guidance from Appendix G in Revision 1 is now addressed by multiple tasks in Revision 2, including:
    - Task P-7, CONTINUOUS MONITORING STRATEGY – ORGANIZATION
    - Task S-5, CONTINUOUS MONITORING STRATEGY – SYSTEM
    - Task M-4, AUTHORIZATION PACKAGE UPDATES
- Privacy elements and roles for systems processing personally identifiable information have been added as a direct response to OMB Circular A-130 [OMB A130], which requires agencies to implement RMF and integrate privacy into the RMF process. In establishing requirements for information security programs and privacy programs, the OMB Circular emphasizes the need for both programs to collaborate on shared objectives. [Back to Table of Contents]

2. What is continuous monitoring, and why is it important?

The ultimate objective of continuous monitoring is to determine if the security and privacy controls in the system continue to be effective over time in light of the inevitable changes that occur in the system and the environment in which the system operates. Continuous monitoring also provides an effective mechanism to update security and privacy plans, assessment reports, and plans of action and milestones. An effective continuous monitoring process includes:

- Configuration management and control processes for organizational systems,
- A risk assessment for actual or proposed changes to systems and environments of operation,
- An assessment of selected controls based on a continuous monitoring strategy,
- A security and privacy posture that reports to appropriate organizational officials; and
- Active involvement by authorizing officials in the ongoing management of security and privacy risks. [Back to Table of Contents]

3. Who is responsible for implementing the continuous monitoring process for individual systems or common controls?

System owners manage the continuous monitoring process for their systems, while common control providers manage the continuous monitoring process for the controls for which they are responsible. Initially, the system owner develops a strategy for the continuous monitoring of control effectiveness and any proposed or actual changes in the system or its operating environment. The system owner

is responsible for monitoring all implemented controls at the frequency defined by organizational policy with input from the authorizing official and risk executive (function). [Back to Table of Contents]

4. What is the role of the risk executive (function) in the continuous monitoring process?

The risk executive (function) helps ensure that security considerations for individual 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 and business processes. 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 systems and supporting infrastructures for which the organization is responsible and provides that information to information owners/system owners. The aggregated information is used to determine the continuous monitoring strategy and the frequency with which the controls are monitored. [Back to Table of Contents]

5. Are automated tools required for continuous monitoring?

No, automated tools are not required for continuous monitoring, but near real-time risk management cannot be fully achieved without continuous control monitoring using automated support tools. Organizations are strongly encouraged to use automated support tools in preparing and managing the content of the authorization package to help provide an effective vehicle for maintaining and updating critical information for authorization officials regarding the ongoing security status of organizational systems.

Providing orderly and disciplined updates to the system security and privacy plans, assessment reports, and plans 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 systems supporting the organization's mission and business processes. [Back to Table of Contents]

6. Can continuous monitoring results be used for annual FISMA (CIO metrics) reporting?

Agencies may use continuous monitoring assessment results provided by organizations to collect data for metrics reporting to the Office of Management and Budget and the Department of Homeland Security. Reporting guidance is issued each fiscal year by the Office of Management and Budget. [Back to Table of Contents]

7. Are external service providers included in the continuous monitoring process?

Yes, federal systems managed or operated by external service providers also need to be continuously monitored. The authorizing official remains responsible for adequately responding to risks to the organization's operations, assets, or individuals arising from the use of external system services. The information owner/system owner and authorizing official establish a trust relationship with external service providers or business partners. The specifics of establishing and maintaining trust can differ from organization to organization based on mission and 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.

The trust relationship depends on the actions taken by the participating partners to implement appropriate security and privacy controls for the 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 and remain implemented as intended.

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

Similarly, external suppliers (in the supply chain) need to be monitored through assessments and reviews. For additional information, see NIST SP 800-37, Revision 2 [SP 800-37r2], Section 2.8, *Supply Chain Risk Management*, and NIST SP 800-53, Revision 5 [SP 800-53r5], Control SR-6 SUPPLIER ASSESSMENTS AND REVIEWS.

Note that in the case of cloud service offerings by external service providers for the processing, storage, or transmission of organizational information from organizational systems, the authorizing official may leverage the provisional FedRAMP [FedRAMP] authorization (P-ATO) or other Agency ATO as part of the organization's risk management (authorization) process. [Back to Table of Contents]

Monitor Fundamentals

The topics for the following questions and answers were selected because they address important themes related to and in support of the monitor step of the RMF (e.g., change management, configuration management, risk assessments, impact analyses).

8. Why should configurations be continuously monitored?

Continuous monitoring is used as the assessment mechanism that supports configuration management and periodically validates that systems within the information environment are configured as expected. Planning and implementing security configurations and then managing and controlling change do not guarantee that systems remain configured as expected. Using automated tools, organizations can identify when the system is not in a desired state to meet security and privacy requirements and respond appropriately to maintain the security and privacy posture of the system. Continuous monitoring identifies undiscovered system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which can potentially expose organizations to increased risk if not addressed. [Back to Table of Contents]

9. How are security and privacy controls selected for continuous monitoring?

Security and privacy controls are selected for continuous monitoring by the system owner according to the system-level continuous monitoring strategy,[1] which is consistent with the organizational continuous monitoring strategy. Controls that are not selected for continuous monitoring at the organizational level are addressed by the system based on a system-level continuous monitoring strategy. In addition to the control selection, the system defines the criteria for monitoring, such as monitoring frequency, assessment planning, and security and privacy posture reporting, among other definitions. [Back to Table of Contents]

10. What is control volatility?

Control volatility is a measure of how frequently a control implementation is likely to change over time. For example, a 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 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 a system (e.g., software patches, new version of a firewall product) would be considered controls with higher volatility. Organizations should apply greater resources to monitor controls deemed to be of higher volatility due to the increased risks from frequent changes. [Back to Table of Contents]

[1] See Task S-5, *Continuous Monitoring Strategy – System*, for more information.

11. Should common controls be continuously monitored?

Yes, common controls should be continuously monitored in a process similar to the process followed for system-specific 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.

The senior agency information security officer and the senior agency official for privacy are 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/system owners of the systems that employ those common controls. [Back to Table of Contents]

12. Do the results of continuous monitoring need to be documented and reported?

Yes, results from continuous monitoring activities need to be documented in posture reports for the authorizing official, senior agency information security officer, and senior agency official for privacy as defined in organizational policies or guidelines. The results of the continuous monitoring effort need to be reflected in updates to the system security and privacy plans, assessment reports, and plans of action and milestones.

The frequency of updates to critical authorization-related documents (i.e., system security and privacy plans, assessment reports, plans of action and milestones) is defined by information owners/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- and privacy-related actions and decisions by authorization officials and senior leaders within the organization with either direct or indirect responsibility for risk management. [Back to Table of Contents]

13. What are plans of action and milestones?

The plan of action and milestones is prepared by the information owner/system owner and describes the specific measures that are planned to (i) correct weak or deficient security and/or privacy controls identified by a control assessment and (ii) address known vulnerabilities in the system. The plan of action and milestones includes tasks to be accomplished with a recommendation for completion before or after system authorization, resources required to accomplish the tasks, milestones established to meet the tasks, and the scheduled completion dates for the milestones and tasks. The most effective plans of action and milestones contain a robust set of actual and potential weaknesses or deficiencies identified in the controls deployed in the system or inherited by the system. Plans of action and milestones are informed by the following:

- Security category and impact level and privacy risk assessments for the system,
- Specific control weaknesses or deficiencies,
- Importance of the identified 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 system, on the risk exposure of the organization, and/or on the privacy risk exposure of an individual),
- Organization's proposed risk response approach to address the identified weaknesses or deficiencies in the controls (e.g., identification of response actions, prioritization of response actions, allocation of response resources, schedule of milestones to mitigate or correct identified weaknesses or deficiencies), and
- Organization's rationale for accepting certain weaknesses or deficiencies in the controls.

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

14. 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 risk associated with those decisions need to be revisited on a regular basis and adjusted based on the results of the continuous monitoring process.

A robust and comprehensive continuous monitoring strategy that is integrated into the ongoing system development life cycle process carried out by an organization can significantly reduce the resources required for reauthorizing systems. Risk management can become near real-time with continuous control monitoring by using automated support tools. Automated support tools can support both ongoing assessments and ongoing authorizations. When continuous monitoring is conducted in accordance with the information needs of the authorizing official, the authorizing official can determine the current security and privacy state of the system, the 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 and privacy state of the system and the risk that the system poses to organizational operations and assets, individuals, other organizations, and the Nation 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 respond to risk adequately. [Back to Table of Contents]

Organizational Support for the Monitor Step FAQs

15. How can the organization support the continuous monitoring process?

To effectively manage the continuous monitoring process, organizations implement a continuous monitoring program, which establishes the organization's criteria for selecting an appropriate subset of controls for ongoing monitoring, determines the frequency and schedule for the monitoring process, defines the reporting requirements, and requires organization-wide participation in the change control process. The continuous monitoring program provides information on the overall security and privacy status of the organization and the ability of the organization's systems to adequately protect the mission and business functions of the organization and individuals' privacy to the degree necessary. In addition, continuous monitoring becomes an integrated and tightly coupled part of the system development life cycle to ensure that the security and privacy controls remain effective across the organization's systems, security and privacy artifacts are updated and maintained, and the security and privacy impacts of system changes are evaluated and controlled. For guidance on establishing a continuous monitoring program, see NIST SP 800-137 [SP 800-137]. For guidance on assessing continuous monitoring programs, see NIST SP 800-137A [SP 800-137A]. [Back to Table of Contents]

16. Who is responsible for implementing an organizational continuous monitoring program?

The senior agency information security officer and the senior agency official for privacy are responsible for implementing an organizational continuous monitoring program for security and privacy controls. The continuous monitoring program allows an organization to (i) track the security and privacy state of its systems on a continuous basis and (ii) maintain the authorization for systems over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and mission and business processes. A robust continuous monitoring program requires the active involvement of information owners/system owners, common control providers, risk executive (function), chief information officers, senior agency information security officers, senior agency officials for privacy, authorizing officials, and the organization's technical operations personnel. Privacy and security continuous monitoring programs can be the same or different programs.

The continuous monitoring program includes responsibilities such as ensuring that 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 and privacy controls for continuous monitoring, integrating continuous monitoring with existing organizational change control/configuration management processes, evaluating security and privacy posture reports and plans of action and milestones provided by information owners/system owners, and providing organizational decision making guidance when allocating resources to mitigate identified weaknesses and deficiencies. For guidance on establishing a continuous monitoring program, see NIST SP 800-137 [SP 800-137]. For guidance on assessing continuous monitoring programs, see NIST SP 800-137A [SP 800-137A]. [Back to Table of Contents]

17. Why should organizations integrate security and privacy into the system development life cycle?

All federal 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 controls for the system are developed, implemented, assessed for effectiveness, and maintained. Integrating security and privacy 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 systems supporting ongoing missions or business functions. Risk management tasks should begin early in the system development life cycle, typically during the system initiation phase and are important in shaping and influencing the security and privacy capabilities of the system. [Back to Table of Contents]

18. What continuous monitoring guidance should the information security and privacy program office(s) provide to system owners?

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

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, privacy impact assessments, and assessment requirements articulated in federal legislation, policy, directives, and regulations. The information security program and privacy program office(s) provides guidance and direction to information owners/system owners to follow when making resource decisions in collaboration with the chief information officer, senior agency information security officer, senior agency official for privacy, and risk executive (function). [Back to Table of Contents]

19. How does the organization determine if the system's security and privacy risk remains acceptable?

The authorizing official periodically reviews the security and privacy posture reports for organizational systems to determine the current security and privacy 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 input from the senior agency information security officer, senior agency official for privacy, and the risk executive (function) – whether the current security and privacy risk is acceptable and to forward appropriate direction to information owners/system owners.

The use of automated support tools to capture, organize, and maintain security and privacy 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 and privacy risks being incurred may change over time based on the information provided in the security and privacy posture reports. Determining how the changing conditions affect the mission and business risks and/or risks to an individual's privacy associated with organizational systems is essential for appropriately managing risk. By carrying out ongoing risk determination and risk acceptance, authorizing officials can manage the authorization over time. [Back to Table of Contents]

20. How does the organization use plans of action and milestones in its decision-making process?

The organization defines a strategy that facilitates a prioritized approach to risk response that is consistent across the organization since most systems often have more risks than available resources can address. Organizational strategies for plans of action and milestones should be guided by the impact on the respective systems affected by the risk response activities. For example, an organization may decide to initially allocate the vast majority of risk response resources to the highest impact 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 mission and business operations and on an individual's privacy. An organization should also prioritize weaknesses or deficiencies within its systems with the greatest privacy risks and/or categorized systems (e.g., 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 addresses the highest priority weaknesses or deficiencies within those prioritized systems.

When weaknesses or deficiencies in 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 and privacy requirements for the system. [Back to Table of Contents]

System-specific Application of the Monitor Step FAQs

21. What steps should the system owner follow to implement continuous monitoring for a system?

To implement a continuous monitoring process for a system, the information owner/system owner develops a strategy for conducting the required continuous monitoring activities, documents changes to the system or operating environment, determines the security and privacy impact of the proposed changes, assesses a subset of controls following a predefined schedule throughout the authorization period, conducts response activities as needed, updates the selection of security and privacy controls for the system, updates critical security and privacy documentation, provides security and privacy posture reports to senior organizational leaders, determines if the risk of the system's operation remains acceptable throughout the system's life cycle, and defines and implements a system disposal strategy when a system is removed from operation.

Prepare for Continuous Monitoring

Continuous monitoring begins after a system has been authorized for use. Therefore, security and privacy documentation – such as the system security and privacy plans, risk assessment, plan of action and milestones, and other security- and privacy-related documentation (e.g., vulnerability scanning results, results of last contingency plan test) – has already been developed and can be provided to the individuals responsible for the continuous monitoring of the system.

Develop a Continuous Monitoring Strategy

During the organization-defined authorization period, the information owner/system owner develops a strategy to monitor the system that is consistent with the organization's continuous monitoring program if it has not already been defined by organizational policy. The continuous monitoring strategy is documented for the system or for a group of related systems.

Document Changes to the System or Operating Environment

The information owner/system owner documents relevant information about proposed or actual changes to the hardware, software, or firmware; descriptions of new or modified features/capabilities; security and privacy implementation guidance; or changes to the system's operating environment. The information owner/system owner uses this information to assess the potential security and privacy impact of the changes.

Determine Impact of the Proposed Changes

The information owner/system owner conducts security and privacy risk assessments to determine the extent to which changes to the system or its operating environment affect the system and impact to an individuals' privacy.

Assess a Subset of Controls

After the initial authorization and in accordance with OMB policy and organizational guidance regarding the authorization period, the information owner/system owner assesses a subset of the controls.

Conduct Remediation Activities

The information owner/system owner initiates a response based on the findings produced during the assessment of the system's controls, the outstanding items listed in the plan of action and milestones, and the results of performing the activities required by the controls (e.g., vulnerability scanning, contingency plan testing, incident response handling).

Update the Selected Controls

The organization determines if there is a need to update the current, agreed-upon controls of its systems, which are documented in the security and privacy plans and implemented within the system, by revisiting the risk management activities described in the Risk Management Framework on a regular basis. Additionally, events such as security incidents, breaches, new OMB policies, new threats or vulnerabilities, and new technologies may trigger the immediate need to assess the security and privacy state of the system and require an update of the current controls.

Update Critical Security Documentation

The information owner/system owner updates the system security and privacy plans and the plan of actions and milestones while control assessors update the assessment report.

Report Status in Security Status Reports

The information owner/system owner documents the results of continuous monitoring activities in security and privacy posture reports and provides the reports to the authorizing official. At a minimum, security and privacy posture reports summarize key changes to security and privacy plans (including risk assessments), assessment reports, and plans of action and milestones.

Determine if Risk Remains Acceptable

The authorizing official reviews the security and privacy posture reports to determine if the current risk of the system to organizational operations and assets, individuals, other organizations, or the Nation remains acceptable and forwards appropriate direction to the information owner/system owner. The information owner/system owner addresses the direction provided by the authorizing official to maintain the security and privacy status of the system.

Implement a System Disposal Strategy

When a system is removed from operation, the information owner/system owner ensures that all controls addressing system disposal (e.g., media sanitization and disposal, configuration management and control) are implemented. [Back to Table of Contents]

22. What is a continuous monitoring strategy?

The continuous monitoring strategy for a system[2] determines what controls are to be monitored, when the controls are monitored (e.g., ongoing or according to a predefined frequency), how changes to the system are monitored, how risk assessments are to be conducted, and the security and privacy posture reporting requirements. It is approved by the authorizing official or authorizing official designated representative and can be included in the security and privacy plan. In accordance with OMB Circular A-130 [A-130], the Privacy Continuous Monitoring (PCM) strategy includes all of the available privacy controls implemented and ensures that they are monitored on an ongoing basis. For greater efficiency, the information security continuous monitoring (ISCM) and PCM strategies and programs may be consolidated into a single unified strategy and program.

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

23. What continuous monitoring information is documented for a system?

Information owners/system owners document strategies for managing changes to systems, their roles and responsibilities in the configuration management process, and the methodologies to monitor the controls of the systems. The strategy is documented in a continuous monitoring plan, the organization's policies and procedures, or other organization-defined documents.

The documentation identifies the security and privacy controls that are monitored, the frequency with which those controls are monitored, the controls deemed volatile, the continuous monitoring schedule, and the conditions that could alter the control selection and assessment schedule. [Back to Table of Contents]

24. What types of changes to the system or operating environment are documented?

The information owner/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 or capabilities (e.g., new search function or additional reporting capability); and security configuration settings (e.g., common secure configuration). It is also important to document any changes to the system's operating environment, such as modifications to hosting facilities or organizational processes and procedures. The information owner/system owner uses this information to assess the potential security and privacy impact of the changes.

Documenting proposed and actual changes to the system and its operating environment and subsequently assessing the potential impacts that those changes may have on the overall security state of the system, organization, and individual privacy are important aspects of control monitoring, achieving situational awareness, and maintaining authorization. It is not advisable that system changes be made prior to assessing the security and privacy impact of those changes. [Back to Table of Contents]

25. How does the system owner conduct security and privacy risk assessments?

The information owner/system owner conducts a security and privacy risk assessment to determine the extent to which proposed or actual changes to the system or its operating environment affect the security state of the system or an individual's privacy. Changes to the system or its operating environment may affect the controls currently in place, produce new vulnerabilities or risks in the system,

[2] See NIST SP 800-37, Revision 2 [SP 800-37r2], for additional guidance on the continuous monitoring strategy for systems (Task S-5) and organizations (Task P-7).

or generate requirements for new controls that were not previously needed. In assessing a change's impact, the information owner/system owner considers the new or modified features and capabilities that the change provides, 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 system contains information technology components for which there exist SCAP-enabled [SCAP] tools, the information owner/system owner should monitor compliance of the component's configuration using the SCAP-validated tools.

If the results of the security and privacy risk assessments indicate that the proposed or actual changes to the system could affect or have affected the security state of the system or the privacy of an individual, corrective actions are initiated and the appropriate documents revised or updated. The authorizing official or designated representative uses the revised/updated assessment report, security and privacy posture reports, plans of action and milestones, and input from the senior agency information security officer, senior agency official for privacy, and risk executive (function) to determine if a reauthorization action is necessary. [Back to Table of Contents]

26. How does the system owner assess a subset of the controls?

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

27. How does the system owner respond to findings from control assessments?

The information owner/system owner reviews the recommended remediation actions included in the findings produced during the assessment of the system's security and privacy controls, the outstanding items listed in the plan of action and milestones, and the results of performing the activities required by the security and privacy controls (e.g., vulnerability scanning, contingency plan testing, incident response handling). By using the assessment results of *satisfied* and *other than satisfied*, information owners/system owners gain a better understanding of the specific weaknesses and deficiencies in the systems and decide how (or if) to mitigate risks in accordance with organizational priorities. The information owner/system owner applies their 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.

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

28. Should the continuous monitoring process be used to update the control baseline?

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

- An incident results in a breach to the 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 threat to the organization's operations or assets, individuals, other organizations, or the Nation is identified based on intelligence information, law enforcement information, or other credible sources of information.

Significant changes to the configuration of the system through the removal or addition of new or upgraded hardware, software, or firmware; changes in PII processing; or changes in the operational environment potentially degrade the security or privacy state of the system.

- Regulatory changes require changes in policies and procedures. [Back to Table of Contents]

29. What critical security and privacy documentation is updated during the continuous monitoring process?

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

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

30. How does the system owner report system status during the continuous monitoring process?

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

31. How does the authorizing official determine if the risk of operating a system remains acceptable?

The authorizing official or designated representative may need to reauthorize a system depending on the severity of an event; the impact of an event or change in organizational operations, organizational assets, or individuals; and the extent of the corrective actions required to fix the identified deficiencies in a system. The authorizing official reviews the security and privacy posture 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 the system (for which an assessment of all of a system's security and privacy controls is conducted) in consultation with the information owner/system owner, the senior agency information security officer, the senior agency official for privacy, 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/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. The information owner/system owner addresses the direction provided by the authorizing official to maintain the security and privacy status of the system. [Back to Table of Contents]

32. What are some examples of significant changes to a system that could trigger a need to reauthorize a system?

The information owner/system owner reconsiders the reauthorization decision when reauthorization is due (i.e., time-driven) or when significant changes occur to a system or its operating environment. Examples of potential significant changes to a 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
- Modifications to how information, including PII, is processed
- Modifications to cryptographic modules or services
- Changes in information types processed, stored, or transmitted by the system
- Modifications to security and privacy controls

While not always directly related to the system, changes in laws, directives, policies, or regulations can also potentially affect the security and privacy of the system and trigger a reauthorization action. Risk assessment results may be used to determine if changes to systems or common controls are significant and trigger an authorization 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 risks that may arise from system changes. [Back to Table of Contents]

33. What activities should the system owner conduct when a system is disposed of?

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

References

[FedRAMP] General Services Administration (2020) *Federal Risk and Authorization Management Program* (FedRAMP) https://www.fedramp.gov

[OMB A130] Office of Management and Budget (2016) *Managing Information as a Strategic Resource*. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[SCAP] Security Content Automation Protocol https://csrc.nist.gov/projects/security-content-automation-protocol

[SP 800-37r1] Joint Task Force (2010) Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 1 [withdrawn]. https://doi.org/10.6028/NIST.SP.800-37r1

[SP 800-37r2] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP 800-53r5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5

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

[SP 800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137

[SP 800-137A] Dempsey KL, Pillitteri VY, Baer C, Niemeyer R, Rudman R, Urban S (2020) Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137A. https://doi.org/10.6028/NIST.SP.800-137A

[Back to Table of Contents]