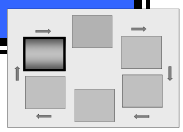
MONITOR STEP – SYSTEM PERSPECTIVE



NIST RISK MANAGEMENT FRAMEWORK

An effective continuous monitoring process integrated with the system development life cycle is needed to determine if the security controls in an information system continue to be effective over time in light of the inevitable changes that occur in the system as well as its operating environment. Continuous monitoring allows an organization to: (i) track the security state of an information system on a continuous basis; and (ii) maintain the security authorization for the system as changes occur in the system. NIST SP 800-37, Revision 1, *Guide for the Authorization of Federal Information Systems: A Security Life Cycle*, Initial Public Draft, defines the requirements for the continuous monitoring process that is used to maintain the system's authorization.[1]

NOTE: The *System Perspective* is provided as one example of how to implement continuous monitoring for information systems in accordance with NIST SP 800-37. Readers should understand that other implementations may be used to support their particular circumstances.

The system perspective in this document elaborates on the basic tasks and guidance in SP 800-37 as examples for stimulating ideas in implementing continuous monitoring guidelines in organization-specific and information system-specific environments.

GATHER INFORMATION SYSTEM DOCUMENTATION

In order to prepare for the continuous monitoring process, the information owner/ information system owner[2] should:

1. Gather all relevant documentation specific to the information system developed and updated throughout the system development life cycle—for example, system changes and their security impact analysis results, changes to system components, system security plan, vulnerability scanning results, or latest security assessment reports.
2. Obtain the organization-wide policies, procedures, and guidance on the continuous monitoring process—including any tools or templates available for use within the organization.
3. Continue organizational relationships with the information security program office, cross-organizational stakeholders, and technical operations staff.

DEVELOP A CONTINUOUS MONITORING STRATEGY

Information owners/information system owners should develop and document a strategy to monitor their information systems. If the organization implements strategy development as a common or hybrid control, the information owner/information system owner is expected to implement the organization's continuous monitoring strategy. To develop a continuous monitoring strategy, the information owner/information system owner should:

1. Establish a strict configuration management process to support their continuous monitoring activities.
2. Define the methodology for conducting security impact analyses to determine the extent to which proposed changes to the system or its operating environment will affect the security state of the system.

[1] The information in the *Monitor Step – System Perspective* should be interpreted as one approach on how to implement the continuous monitoring process. Organizations may develop other methods to implement the NIST standards and guidance.

[2] The common control provider conducts the same role as the information owner/information system owner to provide continuous monitoring for the common controls for which they are responsible.

3. Determine how many subsets of security controls will be assessed during the authorization period, which security controls will be included in each subset, and the schedule according to which the security control subsets will be assessed.
4. Determine the tools that will be used in assessing security controls. For example, Security Content Automation Protocol (SCAP)-validated products should be used to verify whether the security configuration settings of various products comply with government standards, guidance, and policies.
5. Document the continuous monitoring strategy.
6. Obtain approval for the continuous monitoring plan and strategy from the authorizing official and senior agency information security officer.

DOCUMENT CHANGES TO THE INFORMATION SYSTEM OR OPERATING ENVIRONMENT

The information owner/information system owner should document all proposed or actual changes to the information system or its operating environment. The information owner/information system owner should:

1. Document any relevant information about proposed changes to the hardware, software, and firmware components, the system's operating environment, or the organization's policies, procedures, or guidance.
2. Document actual changes to the information system collecting the same information as the proposed changes so that the actual changes can be analyzed and appropriate officials can determine whether or not the actual change can remain in the information system.

DETERMINE SECURITY IMPACT OF CHANGES TO THE INFORMATION SYSTEM

To determine the extent to which changes to the information system or its operating environment will affect the security state of the system, the information owner/ information system owner should:

1. Analyze each proposed/actual change to the information system to determine what impact, if any, the change has on the security posture of the system.
2. Monitor compliance of each information system component's configuration. If the information system contains information technology components for which there exists SCAP-validated tools, those tools should be used to monitor the component's configuration.[3]
3. Document the results of the security impact analysis and share the results with the system management and operations personnel, senior agency information security officer, and the risk executive (function) using an organizationally defined format.
4. Determine if remediation actions or other changes to the system are necessary based on the security impact analysis, determine the impacts of the actions or other changes, and document them in the plan of action and milestones.

ASSESS A SUBSET OF SECURITY CONTROLS

To assess a subset of the selected security controls as defined in the continuous monitoring plan, the information owner/information system owner should:

1. Assign responsibility for assessing a subset of security controls to an assessor who has an appropriate level of independence as defined by the authorizing official and the knowledge, skills, and abilities to complete the assessment.
2. Update the plan of action and milestones after the assessment has been completed based on the updated security assessment report provided by the security control assessor.

[3] OMB Memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration (FDCC),* August 11, 2008

The security control assessor should:

3. Develop the security assessment plan that defines the appropriate procedures from NIST SP 800-53A to assess the security controls.
4. Obtain approval for the security assessment plan from the authorizing official.
5. Conduct the security assessment in accordance with the agreed-upon procedures, personnel, milestones, and schedule.
6. Update the security assessment report with the information gained during the assessment of the subset of security controls and submit it to the information owner/information system owner.

CONDUCT REMEDIATION ACTIVITIES

The information owner/information system owner should initiate remediation actions based on the findings produced during the continuous monitoring assessments of the security controls, the outstanding items listed in the plan of action and milestones, and the results of performing the activities required by the system's security control (e.g., vulnerability scanning, contingency plan testing, incident response handling). The information owner/information system owner should:

1. Consult with the authorizing official, senior agency information security official, and the risk executive (function) and review each assessor finding and determine the severity or seriousness of the finding and whether the finding is significant enough to be worthy of further investigation or remedial action.
2. Determine the appropriate steps required to correct any identified weaknesses or deficiencies that require remediation efforts, establish an implementation plan and schedule for the defined actions, and update the plan of action and milestones with the planned remediation actions.
3. Assess the system after the remediation actions have been completed to determine if the security controls remain effective after changes have been implemented.
4. Update the plan of action and milestones with the current status when a remediation action has been successfully completed.

UPDATE THE SELECTED SECURITY CONTROLS

The information owner/information system owner needs to revisit, on a regular basis, the risk management activities described in the Risk Management Framework to ensure the selection of security controls remains appropriate for the information system. The information owner/information system owner should:

1. Monitor events that occur throughout the organization and determine if those events introduce or uncover new vulnerabilities or threats to the information system.
2. Determine whether the selected security controls remain sufficient to protect the information and information system assets against the newly identified vulnerabilities and threats.
3. Reconfirm the system's impact level and security category of the information system and the information processed, stored, or transmitted by the system and determine if they should be changed.
4. Reassess the risks to organizational operations and assets, individuals, other organizations, or the Nation arising from use of the information system.
5. Consult with the authorizing official, senior agency information system officer, and risk executive (function) to determine if the authorization should be updated.

Update Critical Security Documentation

Continuous monitoring provides information owners/information system owners with an effective tool for producing ongoing updates to security plans, security assessment reports, and plans of action and milestones. These documents are critical to understanding and explicitly accepting risk on a day-to-day basis. The information owner/information system owner should:

1. Ensure that the security control assessor updates the security assessment report with the results of the security control assessments conducted during the continuous monitoring phase.
2. Update the security plan and plan of action and milestones to identify changes to the information system, the operating environment, the security controls, and the implementation of the system's security controls.
3. Preserve the original version of the documents so that they are available for oversight, management, security control assessments, and auditing purposes.
4. Share the updated documentation with others. In the case of common controls, the common control provider should inform information owners/information system owners about any changes that impact the level of security they are inheriting from the use of common controls within their individual information systems.

Report Status in Security Status Reports

The information owner/information system owner should document the results of the continuous monitoring activities in security status reports and provide them to the authorizing official and other designated senior leaders in the organization. The information owner/information system owner should:

1. Describe the continuous monitoring activities and how the vulnerabilities discovered during the security control assessments and security impact analyses are being addressed.
2. Provide the security status reports to the authorizing official, senior agency information security officer, and risk executive (function) at appropriate organization-defined frequencies.

Determine if Risk Remains Acceptable

The information owner/information system owner should provide sufficient information to the authorizing official, senior agency information security officer, and risk executive (function) for them to be able to make appropriate reauthorization decisions. The authorizing official should:

1. Review the updated security assessment report, system security plan, plan of action and milestones, and security status reports to determine whether the risk to the information and information system remains acceptable.
2. Determine whether the information system requires reauthorization.
3. Document the decision and forward it to the information owner/information system owner for appropriate action.

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 decommissioning are implemented. The information owner/information system owner should:

1. Determine a decommissioning strategy for the information system when the system is no longer needed by the organization.
2. Keep users and application owners served by the decommissioned information system or system components informed about the decommissioning activities and any issues associated with their information or applications.

3. Sanitize or destroy information system components in accordance with applicable regulations and guidance to remove system information from information system media so that there is reasonable assurance that the information cannot be retrieved or reconstructed.
4. Update the organization's tracking and management systems to identify the specific information system components that are being removed from the inventory.
5. Record the decommissioned status of the information systems in the system security plan and distribute the document to appropriate individuals or organizations.

REFERENCES

- NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008
- 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
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, Initial Public Draft, February 2009
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008
- NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008
- NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008
- Monitor Step FAQs, www.csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/monitor/index.html