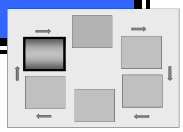
MONITOR STEP – ORGANIZATIONAL PERSPECTIVE



NIST RISK MANAGEMENT FRAMEWORK

Organizations depend on information systems to successfully carry out their missions and business functions. These organizations conduct business in dynamic environments with constantly changing threats, vulnerabilities, and technology. A structured and disciplined process is needed to determine the impacts of the changes on the organization's information systems. A continuous monitoring program provides the up-to-date knowledge that senior leaders need on the organization's security state and risk posture so that they can initiate appropriate responses as changes occur.

A robust continuous monitoring program for an organization requires the active involvement of information owners/information system owners and common control providers, the risk executive (function), chief information officer, senior agency information security officer, and authorizing officials. The continuous monitoring program is described in NIST SP 800-37, Revision 1, *Guide for the Authorization of Federal Information Systems: A Security Life Cycle*, Initial Public Draft, August 2008.

NOTE: The *Organizational Perspective* is provided as one example of how NIST SP 800-37 may be implemented to continuously monitor information systems. Readers should understand that other implementations may be used to support their particular circumstances.

The organizational perspective in this document elaborates on the basic steps and guidance in NIST SP 800-37 as examples for stimulating ideas in implementing an organization-wide continuous monitoring process.

MAINTAIN RELATIONSHIPS WITH ORGANIZATIONAL ENTITIES

An organization's management of security risks is dependent upon the collaboration among the organization's many entities. To maintain those relationships, the information security program office should:

1. Reach out to information owners/information system owners[1] to provide them with the guidance and support they need to effectively and consistently implement the organization's continuous monitoring process.
2. Collaborate with the technical operations personnel to validate that the organization's security policies are implemented effectively within the organizational infrastructure, ensure that responsibilities for common security controls have been assigned, and validate that a configuration management process exists that addresses security in the operational decision making process.

PUBLISH ORGANIZATIONAL GUIDANCE ON CONTINUOUS MONITORING

To ensure the organization's continuous monitoring process is implemented consistently, the information security program office should:

1. Develop continuous monitoring guidance that supplements the guidance in NIST SP 800-37 and provides organization-specific procedures and documentation, approval, and reporting requirements for all monitoring tasks.
2. Prepare templates to support the continuous monitoring process.
3. Distribute the organizational guidance and templates to all individuals involved in the continuous monitoring process.
4. Train individuals involved in the continuous monitoring process.

[1] 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.

Acquire Tools to Support the Continuous Monitoring Process

While automated tools are not required for the continuous monitoring process, risk management can become near real-time through the use of automated tools. If an organization chooses to acquire automated tools to support continuous monitoring, the information security program office should:

1. Determine the specific needs and requirements that the automated tools should meet along with the selection criteria for acquiring the automated tools.
2. Acquire automated tools in accordance with all federal and organizational acquisition regulations.
3. Provide training and support on using the automated tools.

Use the Plan of Action and Milestones in Decision Making

To facilitate a prioritized approach to risk mitigation that is consistent across the organization, the information security program office should:

1. Develop an organizational strategy to manage and collect information from plans of action and milestones.
2. Consolidate information from individual system's plans of action and milestones to determine if there are common weaknesses or deficiencies that are shared among the organization's information systems.
3. Propose solutions to mitigate the common weaknesses and deficiencies for the organization.
4. Use the information to allocate risk mitigation resources for the organization.

Determine Whether Reauthorization Decisions are Needed

The risk executive (function) and senior agency information security officer should periodically review the security status reports and updated critical security documents to assess the organization's security posture and to determine whether reauthorization is required. The risk executive (function) and the senior agency information security officer provide an organizational perspective on risk to the authorizing official.

The risk executive (function) should:

1. Provide input to the senior agency information security officer, authorizing officials, and information owners/information system owners on the organization's tolerance for risk and overall risk mitigation strategy for use in organizational decision making.

The senior agency information security officer should:

2. Analyze the updated critical security documents (i.e., security plans, security assessment reports, and plans of action and milestones) along with the periodic security status reports and determine the current security state of the organization.
3. Determine if proposed changes to an information system or its operating environment meet the organizational criteria for significant changes.

Authorizing officials should:

4. Balance the information in the security authorization package and security status reports with the information obtained from the risk executive (function) on the organization's tolerance for risk along with guidance from the senior agency information security officer to determine whether or not a reauthorization to an information system is required.

5. Coordinate any reauthorization activities with the information owner/ information system owner by meeting with information owners/information system owners to discuss the assessment results obtained during continuous monitoring, the terms and conditions of the authorization, and any other factors affecting the organization at large to determine their impact on the system's authorization.
6. Document the reauthorization decisions in the authorization decision document and transmit it to the information owner/information system owner for implementation.

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*, Working Draft, October 2008
- Monitor Step FAQs, www.csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/monitor/index.html