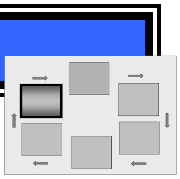
MONITOR STEP – MANAGEMENT PERSPECTIVE



NIST RISK MANAGEMENT FRAMEWORK

Effective risk management requires recognition that organizations operate in a highly complex and interconnected world using state-of-the-art and legacy information systems that organizations depend upon to accomplish critical missions and to conduct important business. **Continuous monitoring is conducted 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. A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that **provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make credible, risk-based decisions regarding the operation of an information system**.

RISK EXECUTIVE (FUNCTION)

Organizations need a **comprehensive approach to manage risk—an approach that recognizes the balance between the organization's mission and business functions and its day-to-day operations—including the use of information systems** to achieve their missions and accomplish their business goals. The management of organizational risks can best be achieved by the implementation of an overall risk executive (function). The **risk executive (function) provides senior leadership input and oversight for all risk management and information security activities across the organization** (e.g., security categorizations, common security control identification, continuous monitoring and reauthorization) to help ensure consistent risk acceptance decisions.

SENIOR LEADERSHIP

Senior leadership oversight in the continuous monitoring process is essential so that the security risks associated with the operation and use of 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 and business functions. An organization-wide continuous monitoring process ensures that managing security risks from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks in planning and achieving mission/business success.

RELATIONSHIP OF CONTINUOUS MONITORING TO FISMA

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 any of the following 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).

ORGANIZATIONAL SUPPORT

To ensure the benefits of an organization-wide continuous monitoring process, **the organization's information security program office should implement a continuous monitoring program that is integrated with the organization's system development life cycle** to maintain ongoing, up-to-date knowledge by senior leaders of the organization's overall security state and risk posture and to initiate appropriate responses as needed when the security state and risk posture change.

Continuous Monitoring Program

A continuous monitoring program allows an organization to **track the security state of an information system on a continuous basis** and to maintain the security authorization to operate the system as new threats, vulnerabilities, technologies, and mission/business processes change the system's operating environment. An effective continuous monitoring program includes:

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

Configuration Management

Configuration management is a discipline that controls changes to the system baseline configuration/architecture (e.g., information technology components that are added, changed, or repositioned), configuration settings for information technology products (e.g., operating systems, firewalls, routers), critical security documentation (e.g., system security plan, security assessment report, plan of action and milestones), operational procedures (e.g., audit review schedule, security training), and the system's operating environment (e.g., improvements at a hosting facility, change in building access procedures).

Prior to any change implementation, **the organization analyzes proposed changes to the information system for their impacts on the system's functionality, performance, and security**. After the information system is changed, the organization tests the security features of the system to verify that the features, both changed and unchanged, are functioning properly.

Security Impact Analysis

Security impact analysis determines the extent to which proposed changes to the information system or its operating environment affect the security state of the system. Proposed changes, for example, 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. If the results of the impact analysis indicate that the proposed changes will affect the security state of the system, corrective actions are initiated and appropriate documents revised or updated or the proposed changes are rejected or rescheduled.

Security Control Monitoring

Security control monitoring is used to check a subset of security controls in an information system on an ongoing basis to determine if the security controls operate correctly and continue to be effective. Organizations should use recent risk assessments, results of previous security assessments, and operational requirements in guiding the selection of security controls to be monitored and the frequency of the monitoring process.

Security Status Reports

Security status reports provide the authorizing official and other senior leaders within the organization **essential information with regard to the security state of the information system**. Security status reports should describe the continuous monitoring activities employed by the information system owner, address vulnerabilities in the information system discovered during the security control assessment, security impact analysis, and security control monitoring, and how the information system owner intends to address those vulnerabilities.

Near Real-Time Monitoring

Organizations are strongly **encouraged to use automated support tools** to help provide an effective vehicle for maintaining and updating critical information for senior leaders regarding the ongoing security status of the organization's information systems. Providing orderly and disciplined updates to the 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**.

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