CONTINUOUS MONITORING OF INFORMATION SECURITY: AN ESSENTIAL COMPONENT OF RISK MANAGEMENT

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

The effective management of information technology (IT) security, and the assurance of the confidentiality, integrity, and availability of information, are critical to the success of an organization in carrying out its mission and business processes. Today, organizations depend on information technology to perform many mission- and business-related functions. This dependence means that organizations must be able to identify and to respond to new vulnerabilities and threats to their systems, and to adapt their systems to meet changing organizational requirements and environments.

The risks associated with these changing situations can be managed through an integrated organizational approach, bringing together the best collective judgments of individuals and groups within the organization who are responsible for strategic planning, oversight, management, and day-to-day operations.

Federal government organizations are directed by the Federal Information Security Management Act (FISMA) of 2002, and other legislative and executive directives, to develop, document, and implement programs to protect their information and information systems, and to apply a risk-based policy to achieve cost-effective security for their information and information systems. Standards and guidelines developed by the National Institute of Standards and Technology (NIST) help agencies to carry out effective information security programs based on the management of risk.

Information Security Continuous Monitoring and the Risk Management Framework

The Information Technology Laboratory (ITL) at NIST developed the Risk Management Framework (RMF) to help organizations develop a disciplined and structured process that integrates information security and risk management activities into the life cycle of an information system. The RMF describes six basic steps:

- **Categorize** the information system and the information processed, stored, and transmitted by the system based on analysis of the impact to the organization from loss of security;

- **Select** an initial set of baseline security controls for the information system based on the security categorization; tailor and supplement the security controls based on organizational assessment of risk and local conditions;

- **Implement** the security controls and document how the controls are deployed within the information system and environment of operation;

- **Assess** the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and meeting the security requirements for the system;

- **Authorize** information system operation based upon determination of the risk to the organization, its operations and assets, and to others resulting from the operation of the information system and the decision of acceptable risk;

- **Monitor** security controls in the information system on an ongoing[1] basis for effectiveness; document changes to the system or environment of operation; conduct security impact analyses of the changes; and report the security state of the system to appropriate organizational officials.

This last step of ongoing monitoring is an important part of the risk management process. Monitoring and assessing an organization's overall security architecture and security program help to ensure that organization-wide operations remain within an acceptable level of risk when changes are made, and that timely, relevant, and accurate information about systems and security programs is available to the organization.

Information system continuous monitoring (ISCM) is the process of maintaining ongoing awareness of information security, vulnerabilities, and threats in order to support organizational risk management decisions. Organizations adopting an effective ISCM strategy are able to:

- Maintain a clear understanding of organizational risk tolerance, set priorities, and manage risk consistently throughout the organization;
- Review metrics that provide meaningful indications of security status at all levels of the organization;
- Assess continued effectiveness of all security controls;
- Verify compliance with information security requirements derived from organizational functions and from federal directives and policies;
- Maintain information on all organizational IT assets and the security of the assets;
- Control changes to organizational systems and environments of operation; and
- Maintain awareness of threats and vulnerabilities of information systems.

NIST Special Publication (SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

[1] The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.

The Information Technology Laboratory (ITL) at NIST recently issued a new publication to help organizations carry out ongoing monitoring, the last step of the RMF process. NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, assists organizations in developing an ISCM strategy and implementing an ISCM program that provides awareness of threats and vulnerabilities, and that facilitates the assessment of organizational assets and the effectiveness of security controls. Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information.

The authors of the guide are Kelley Dempsey, Arnold Johnson, Matthew Scholl, and Kevin Stine of NIST; Ronald Johnston of the Department of Defense, Chief Information Officer, Defense-wide Information Assurance Program (DOD-CIO, DIAP); Alicia Clay Jones and Angela Orebaugh of Booz Allen Hamilton; and Nirali Shah Chawla of PricewaterhouseCoopers LLP. NIST SP 800-137 builds on concepts of monitoring and on the security control assessment methods that are detailed in other NIST publications. See the **For More Information** section below.

The guide introduces the fundamentals of ongoing monitoring of information security in support of risk management, with discussion of organization-wide views of ISCM, ongoing authorization of systems, the role of automation in ISCM, and organizational roles and responsibilities. One section of the guide is devoted to the ISCM process and includes specific implementation guidelines. The supporting appendices provide general references, definitions, and explanations of terms used, acronyms, and descriptions of technologies for enabling ISCM. NIST SP 800-137 is available on the NIST Web site http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

Integration of the ISCM Process in Risk-related Activities throughout the Organization

Maintaining an up-to-date view of information security risks across an organization is a complex, multifaceted undertaking. It requires the involvement of the entire organization, from senior leaders providing governance and strategic vision to individuals developing, implementing, and operating individual information systems in support of the organization’s core missions and business functions.

The risk management process is integrated throughout the organization by means of a three-tiered approach in order to achieve continuous improvement in risk-related activities and to facilitate effective communication throughout the organization. This three-tiered approach is also discussed in other NIST publications listed in the **For More Information** section.

Tier 1, organizational level, addresses risk by establishing and implementing governance structures that are consistent with the strategic goals and objectives of organizations and the requirements that are defined by federal policies and by mission and business functions. At this tier, the **criteria for ISCM** are defined by the organization’s risk management strategy, including how the organization plans to assess, respond to, and monitor risk, and the oversight required to ensure that the risk management strategy is effective. Security controls, security status, and other metrics defined and monitored at this tier deliver the information necessary to make risk management decisions that support policies.

Tier 2, mission/business process level, encompasses designing, developing, and implementing mission and business processes that support the functions defined at Tier 1. The **Tier 2 criteria for continuous monitoring** of information security are defined by how core mission and business processes are prioritized with respect to the overall goals and objectives of the organization, the types of information needed to successfully execute the stated mission and business processes, and the organization-wide information security program strategy. Tier 2 controls are deployed organization-wide and support all information systems.

Tier 3, information system level, integrates risk management activities into the system development life cycle of organizational information systems, from the initiation of a system, through development, implementation, operation, maintenance, and disposal. **ISCM activities at Tier 3** include ensuring that all system-level security controls are implemented correctly, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system, and continue to be effective over time. ISCM activities at Tier 3 also include assessing and monitoring controls implemented at the system level. Security status reporting at this tier can include security alerts, security incidents, and identified threat activities. The ISCM strategy for Tier 3 also ensures that security-related information supports the monitoring requirements of other organizational tiers.

The monitoring step (Step 6) of the RMF involves interactions between the three tiers and includes data from system owners, common control providers, and authorizing officials on security control assessments and system authorizations. By implementing a robust ISCM strategy, organization officials are provided with a clear view of the organization’s overall security status and the contribution of each system to the overall security.

The ISCM Process

Organizations should take the following steps to establish, implement, and maintain an ISCM strategy and program:

- **Define** an ISCM strategy that is based on the organization’s risk tolerance and that maintains clear views related to assets, awareness of vulnerabilities, up-to-date threat information, and impact on the organization’s mission and business processes.

- **Establish** an ISCM program determining metrics, frequency of status monitoring, frequency of control assessments, and development of a technical architecture that supports ISCM.

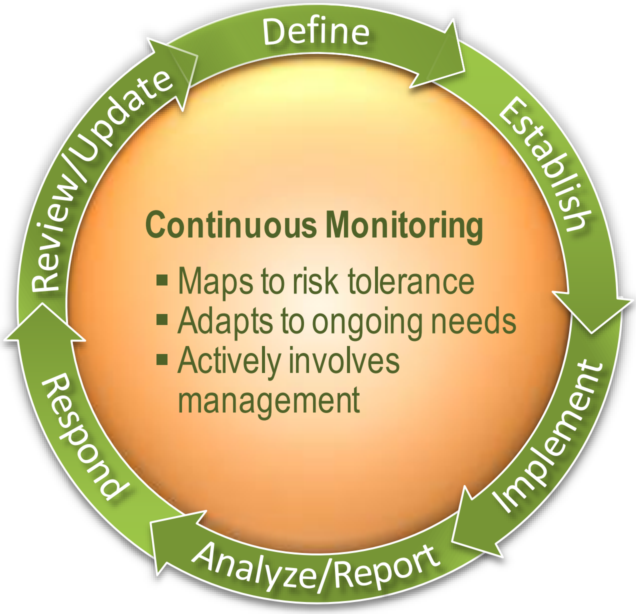
- **Implement** an ISCM program and collect the security-related information using metrics to evaluate and control ongoing risk to the organization, and to facilitate the assessment of security controls and reporting on the security status of systems. Automate the collection, analysis, and reporting of data where possible. Automated processes and tools, such as vulnerability scanning tools and network scanning devices, can make the process of continuous monitoring more cost-effective, consistent, and efficient.

- **Analyze** the data collected and **Report** findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.

- **Respond** to findings at all tiers of the organization through activities such as risk mitigation, risk acceptance, risk avoidance or rejection, or risk sharing or transfer, in accordance with organizational risk tolerance.

- **Review and Update** the monitoring program, adjusting the ISCM strategy and the monitoring and assessment activities to increase information about assets and awareness of vulnerabilities. Review the continuous monitoring strategy to assure that it supports the organization's risk tolerance policies, that the metrics remain relevant, and that data is current and complete. This review identifies ways to improve organizational insight into security posture, effectively supports informed risk management decision making and ongoing authorizations, and improves the organization's ability to respond to known and emerging threats.

The ISCM process is illustrated in the figure below:



For More Information

The publications listed below include information related to risk management and the system development life cycle. For information about these and other security-related publications, see http://csrc.nist.gov/publications/index.html.

NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, provides instructions, recommendations, and considerations for planning the interim measures that an organization can adopt to recover information systems after disruptions to services.

NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, describes monitoring security controls at the system level and also includes an organization-wide perspective, integration with the system development life cycle, and support for authorization of security controls.

NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, describes three key organization-wide ISCM activities: monitoring for effectiveness, monitoring for changes to systems and environments of operation, and monitoring for compliance.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, as amended, guides organizations in the selection and specification of controls for information systems that process, store, or transmit federal information in accordance with organizational risk tolerance.

NIST SP 800-53A Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, provides guidelines for building security assessment plans and procedures for assessing the effectiveness of the security controls defined in NIST SP 800-53.

NIST SP 800-55 Rev. 1, *Performance Measurement Guide for Information Security*, assists in the development, selection, and implementation of measures to be used at the information system and program levels to indicate the effectiveness of security controls applied to information systems and security programs.

NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, includes guidelines for integrating security considerations into the process of managing the configuration of information system architecture and components for the secure processing, storing and transmitting of information, and for implementing the Configuration Management family of security controls defined in NIST SP 800-53.

General information about the Risk Management Framework (RMF), and access to standards and guidelines that pertain to the RMF, are available from the NIST Web page http://csrc.nist.gov/groups/SMA/fisma/framework.html.

Information about NIST's information security programs is available from the Computer Security Resource Center at http://csrc.nist.gov/.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.