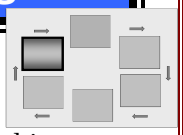
MONITOR STEP – TIPS AND TECHNIQUES FOR ORGANIZATIONS

NIST RISK MANAGEMENT FRAMEWORK



Continuous monitoring is a technique to address the security impacts on information systems resulting from changes to the hardware, software, firmware, or operational environment. 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 status-related information to appropriate organizational officials in order to identify security risks, take risk mitigation actions and make credible, risk-based decisions regarding the operation of an information system. The continuous monitoring program is described in 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.

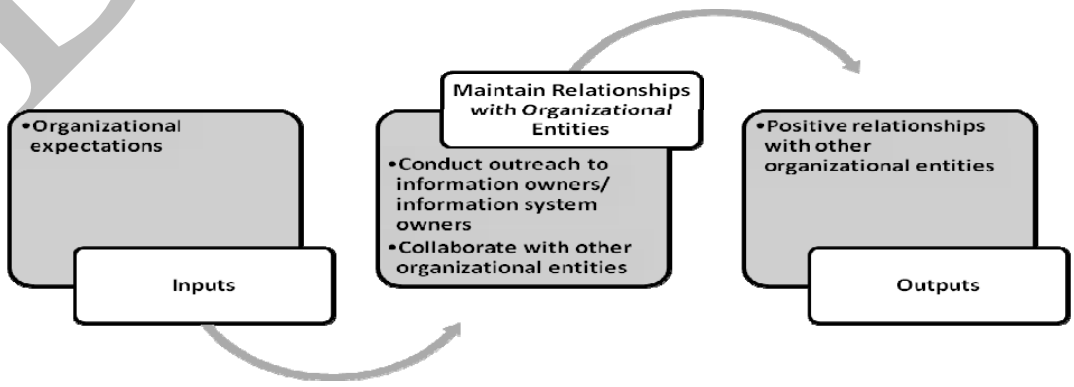
The organization's information security program office (typically managed by the senior agency information security officer) is responsible for implementing an organizational continuous monitoring program that maintains relationships with other organizational entities; provides guidance on continuous monitoring for their organization that addresses developing a continuous monitoring strategy, selecting subsets of security controls for assessment during the system's authorization period, and implementing/integrating security into the existing configuration management processes; acquires tools to support the continuous monitoring process, if needed; evaluates plans of action and milestones for use in organizational decision making; and provides guidance on determining whether system reauthorizations are needed.

NOTE: The *Tips and Techniques for Organizations* are 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 tips and techniques for organizations in this document elaborate on the basic steps and guidance in NIST SP 800-37 as examples for stimulating ideas in an organization-wide continuous monitoring program.

MAINTAIN RELATIONSHIPS WITH ORGANIZATIONAL ENTITIES

An organization's management of security risks is dependent upon the collaboration among the organization's many entities. Working together, senior leaders can make informed decisions, provide adequate security, mitigate risk, and help ensure that the organization's missions and business activities operate successfully. Continuous monitoring provides the information needed to make these ongoing decisions throughout the life of an operational system. The senior agency information security officer and the information security program office serve as the liaison between the mission/business managers, program managers, and the technical operations personnel to ensure the successful implementation of continuous monitoring throughout the organization.



Conduct Outreach to Information and Information System Owners

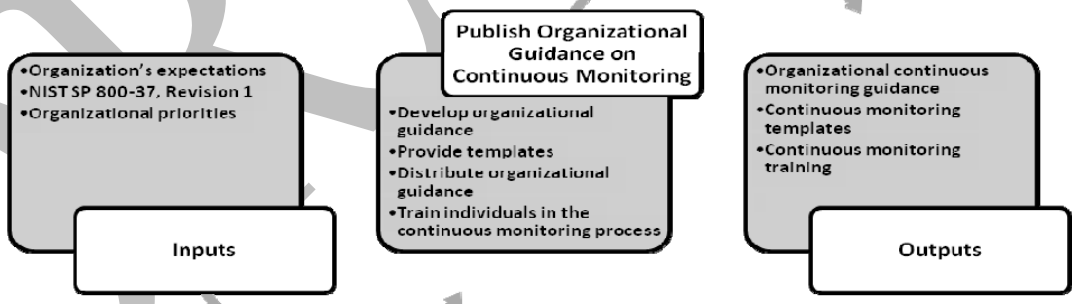
The information security program office should reach out to information owners/ information system owners[1] to provide them with the guidance and support they need to effectively and consistently implement the organization's continuous monitoring process. The outreach activities should include providing guidance on conducting the continuous monitoring process, integrating security into the existing configuration management process, providing training on the continuous monitoring process, developing templates or obtaining tools to support the process, and serving as the organizational point of contact. The information security program office should work with all organizational entities that are responsible for implementing and operating common security controls to ensure the continuous monitoring of those controls.

Collaborate with Other Organizational Entities

The information security program office should collaborate with the technical operations staff to validate that the organization's security policies are implemented effectively within the organization's information technology infrastructure, ensure that responsibilities for common security controls have been assigned, and validate that a configuration management process exists that includes security in the organizational decision making process.

PUBLISH ORGANIZATIONAL GUIDANCE ON CONTINUOUS MONITORING

In order to ensure the continuous monitoring process is implemented consistently throughout the organization, the information security program office should prepare organization-specific guidance that defines the organization's continuous monitoring process, distribute the guidance to all individuals involved in the process, and provide appropriate training. The guidance should cover topics such as developing a continuous monitoring strategy for information systems, implementing configuration management and control processes, selecting subsets of security controls for assessment during the authorization period, integrating security into existing configuration management processes, preparing security status reports, and decommissioning information systems.



Develop Organizational Guidance

The organization's information security program office should develop continuous monitoring guidance that supplements the guidance in NIST SP 800-37 and provides organization-wide procedures and documentation, approval, and reporting requirements. The guidance should address how information owners/information system owners should:

- Develop a continuous monitoring strategy for their information systems;
- Handle specific types of changes to their information systems;

[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.

- Select subsets of security controls for assessments during the system's authorization period;
- Integrate security into existing configuration management processes;
- Document proposed changes to their information systems as system change requests;
- Obtain decisions on their system change requests;
- Prepare security status reports;
- Use updated security documentation in organizational decision making processes;
- Determine if the system's security posture remains adequate;
- Maintain the system's authorization decision; and
- Decommission the information system when it has been removed from operation.

Some organizations implement the security control assessment portion of continuous monitoring as a common security control. In those situations, the organization will: (i) define an organization-wide policy, procedure, and strategy; (ii) train information owners/information system owners on how to implement the strategy; (iii) select security controls to be assessed during the authorization period and the frequency of the assessments; and (iv) define reporting requirements to ensure that the continuous monitoring strategy is implemented as intended. In those situations, the information owner/information system owner implements the organizationally-defined strategy.

In other situations, organizations may implement continuous monitoring as a hybrid control in which case the information owners/information system owners manage their system-specific continuous monitoring tasks in accordance with an organization-wide policy and guidance that addresses, for example, the contents of a continuous monitoring strategy, the organization-required activities that the system-specific continuous monitoring procedures should address, the organization-allowed methods for selecting security control subsets for assessment and for determining the frequency of the subset assessments, the organization-allowed methods for monitoring and controlling changes to the information system, and the contents of organization-required reports and documents.

Provide Templates to Support Continuous Monitoring

The organizational guidance should include templates for the documents and reports that the organization will employ in the continuous monitoring of its information systems to promote a common understanding of the expectations for its continuous monitoring process. The templates that the information security program office may develop include templates for continuous monitoring strategies and plans, security assessment plans, security assessment reports, security status reports, system change status reports, and the authorization decision document.

Distribute Organizational Guidance

After the organization-specific continuous monitoring guidance has been prepared and approved, the guidance should be distributed to all individuals within the organization that are involved in the continuous monitoring process (e.g., authorization officials, information owners/information system owners, common control providers, and individuals that review security status reports, plans of action and milestones, or security assessment reports for the organization). The distribution method should be consistent with the size and complexity of the organization, with options ranging from email and paper distribution to making the guidance available on a website or security portal.

Train Individuals in the Continuous Monitoring Process

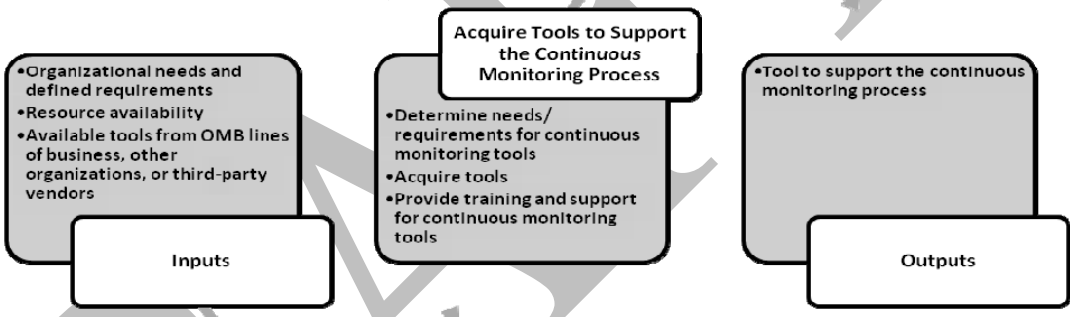
In addition to distributing the organization-specific continuous monitoring guidance, the information security program office should consider training the individuals involved in the continuous monitoring process. Training ensures that the organization-specific guidance and tools, templates, and techniques are applied consistently throughout the organization and that the individuals involved in the continuous monitoring process

understand clearly how the continuous monitoring process is expected to be implemented within the organization and their specific roles and responsibilities.

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 support tools. Organizations should integrate these technologies into their information security programs as resources are available.

In addition to vulnerability scanning tools, system and network monitoring tools, and other automated support tools that can help to determine the security state of an information system, organizations can employ automated security management and reporting tools to update critical documents in the authorization package (i.e., the security plan, security assessment report, and plan of action and milestones). These documents should be considered living documents and updated accordingly based on actual events that may affect the security of the information system.



Determine Need for Tools to Support Continuous Monitoring

The organization should determine their organizational needs and the specific requirements that the automated support tools should meet along with criteria for selecting those tools. The requirements and selection criteria should be carefully considered and validated prior to acquiring an organizational tool. Tools to support all phases of the Risk Management Framework are available through the OMB Information System Security Line of Business, other government organizations, and from third-party vendors.

Acquire Continuous Monitoring Tools

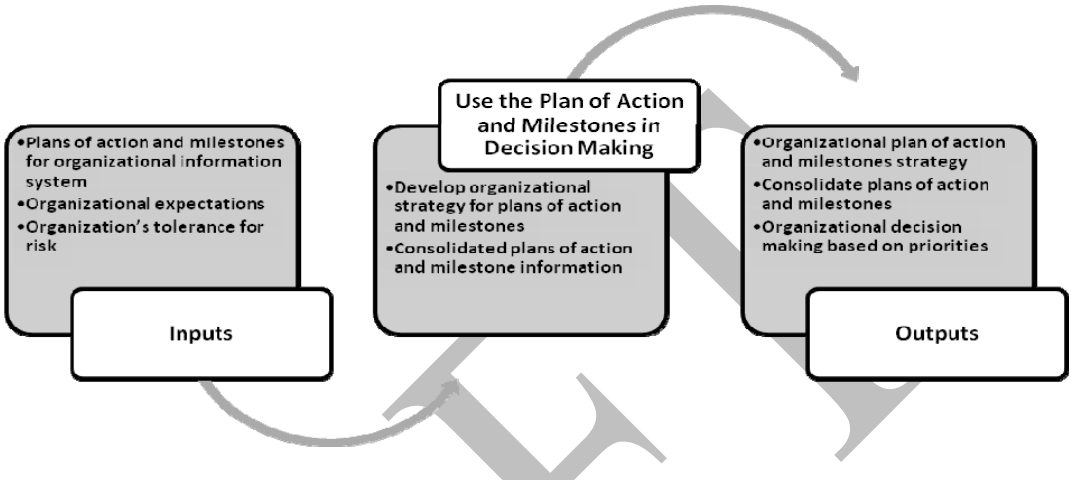
The information security program office should work closely with their contracting organization and follow all federal government and organizational regulations when acquiring tools to support the Risk Management Framework.

Provide Training and Support for Organizational Continuous Monitoring Tools

If an organization acquires one or more tools to support the implementation of the Risk Management Framework, the information security program office (or other designated organization) should provide training and support to the information owners/information system owners that are expected to use the automated system. The training can range from a formal training class, online guidance or blogs, or a help desk to answer questions. The training should be sufficient to meet the needs of the organization based on the size of the organization, the current level of organizational knowledge of the Risk Management Framework and support tools, geographic distribution of users, and available organizational resources.

USE THE PLAN OF ACTION AND MILESTONES IN DECISION MAKING

Assuming most information systems have more vulnerabilities than available resources can address, the organization should define a strategy for developing plans of action and milestones that facilitates a prioritized approach to risk mitigation that is consistent across the organization. The information security program office is typically responsible for developing the organizational strategy regarding plans of action and milestones.



Develop Organizational Strategy for Plans of Action and Milestones

The plan of action and milestones describes the specific measures that are planned: (i) to correct weaknesses or deficiencies noted in the security controls during a security control assessment; and (ii) to address known vulnerabilities in the information system or the organization's information security program. The information security program office should develop an organizational strategy to manage plans of action and milestones that addresses:

- The security categories of their information systems;
- The specific weaknesses or deficiencies in the organization's information system security controls;
- The importance of the identified security control weaknesses or deficiencies (i.e., the direct or indirect effect that the weaknesses or deficiencies may have on the overall security state of the information system and hence on the risk exposure of the organization);
- The information owner/information system owner's proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g., prioritization of risk mitigation actions, allocation of risk mitigation resources); and
- The organization's rationale for accepting certain weaknesses or deficiencies in the security controls.

Consolidate Plan of Action and Milestones Information

Organizations should consolidate information from all of their systems' plans of action and milestones to determine if there are common weaknesses or deficiencies that are shared among the organization's information systems. Common weaknesses or deficiencies may require a common solution that is best addressed by the information security program office by implementing new or stronger common security controls, providing additional training, clarifying organizational security guidance, or providing security engineering advice at various stages of the system development life cycle.

Make Decisions Using Plans of Action and Milestones

Organizations may decide to allocate the vast majority of risk mitigation resources initially to the highest impact information 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 or business operations. In general, the plan of action and milestones strategy should always address the highest priority weaknesses or deficiencies within their prioritized systems.

DETERMINE WHEN REAUTHORIZATION DECISIONS ARE NEEDED

Most, if not all, routine changes to information systems or their operating environment should be handled by the organization's continuous monitoring program. The risk executive (function) and senior agency information security officer provide an organizational perspective on risk to the authorizing official. Ultimately, the authorizing official makes the reauthorization decision for each information system within their purview.

Obtain Organizational Risk Tolerance

The authorizing official, senior agency information security officer, and information owners/information system owners receive a statement of organizational risk tolerance from the risk executive (function). The risk executive (function) establishes the organization's tolerance for risk and the overall risk mitigation strategy. In addition, the risk executive (function) input may include previously established overarching organizational risk guidance, specific organization-wide mission and business requirements, dependencies among information systems including aggregated risks from current information systems, and other types of risks not directly associated with the information system.

Analyze Security Documentation

The authorizing officials and senior agency information security officer receive updated security plans, security assessment reports, and plans of action and milestones along with the periodic security status reports from information owners/information system owners. The accuracy and timeliness of the updates to these documents influences ongoing security-related actions and decisions by the organization's senior leaders. With accurate information readily available, the senior leaders should be able to analyze the current security state of an information system.

Determine if a Proposed Change is Significant

Changes to the information system could have a significant impact on the security of the organization and those changes should be thoroughly reviewed with an analysis of the change's impact on the security of the system. In some cases, the change could have a significant impact on the information system that could trigger a need to reauthorize the system. The following are potential changes that could have a significant impact on the security of the organization and be evaluated for a possible reauthorization decision:

- Installation of a new or upgraded operating system, middleware component, or application;
- Modifications to system ports, protocols, or services;
- Changes to the environments in which the system resides;
- Installation of new or upgraded hardware platform or firmware components; or
- Modification to cryptographic modules or services.

Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reauthorization 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 risk arising from the information system changes.

Incorporate Organizational Risk Information in Reauthorization Decisions

The organizational risk information should be balanced with the system specific information (in critical security documents) when making reauthorization decisions. The authorizing official makes the reauthorization decision based on the content of the authorization package, security status reports, and any additional inputs received from the organization's risk executive (function).

Validate Need for Reauthorization

To ensure that the organization's mission, business, and operational needs are fully considered, the authorizing official should meet with the information owners/information system owners prior to issuing a reauthorization decision to discuss the assessment results, the terms and conditions of the authorization, and any other factors affecting the organization at large.

Document the Reauthorization Decision

The authorizing official documents the reauthorization actions in the authorization decision document and transmits the updated security authorization decision to the information owner/information system owner and other key organization officials, as required by the organizational guidance.

MONITOR STEP SUMMARY

A critical aspect of the security authorization process is the post-authorization period involving the continuous monitoring of an information system's security controls (including common controls). The inevitable changes to the information system or its environment of operation, and the resulting potential adverse impacts of those changes, require a structured and disciplined process capable of monitoring the effectiveness of security controls on a continuous basis in order to maintain an acceptable security state. Information system monitoring activities are most effective when integrated into the broader life cycle management processes carried out by the organization and not executed as stand-alone, security-centric activities.

The products resulting from implementing a continuous monitoring program for the organization include the following:

- Organization-wide guidance on how to implement continuous monitoring processes that are consistent with NIST SP 800-37;
- Tools and templates to support the organization's continuous monitoring process;
- Training on the organization's continuous monitoring process and tools;
- Organizational risk tolerance guidance; and
- Consolidated plan of action and milestones as a tool for organization security decision making.

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