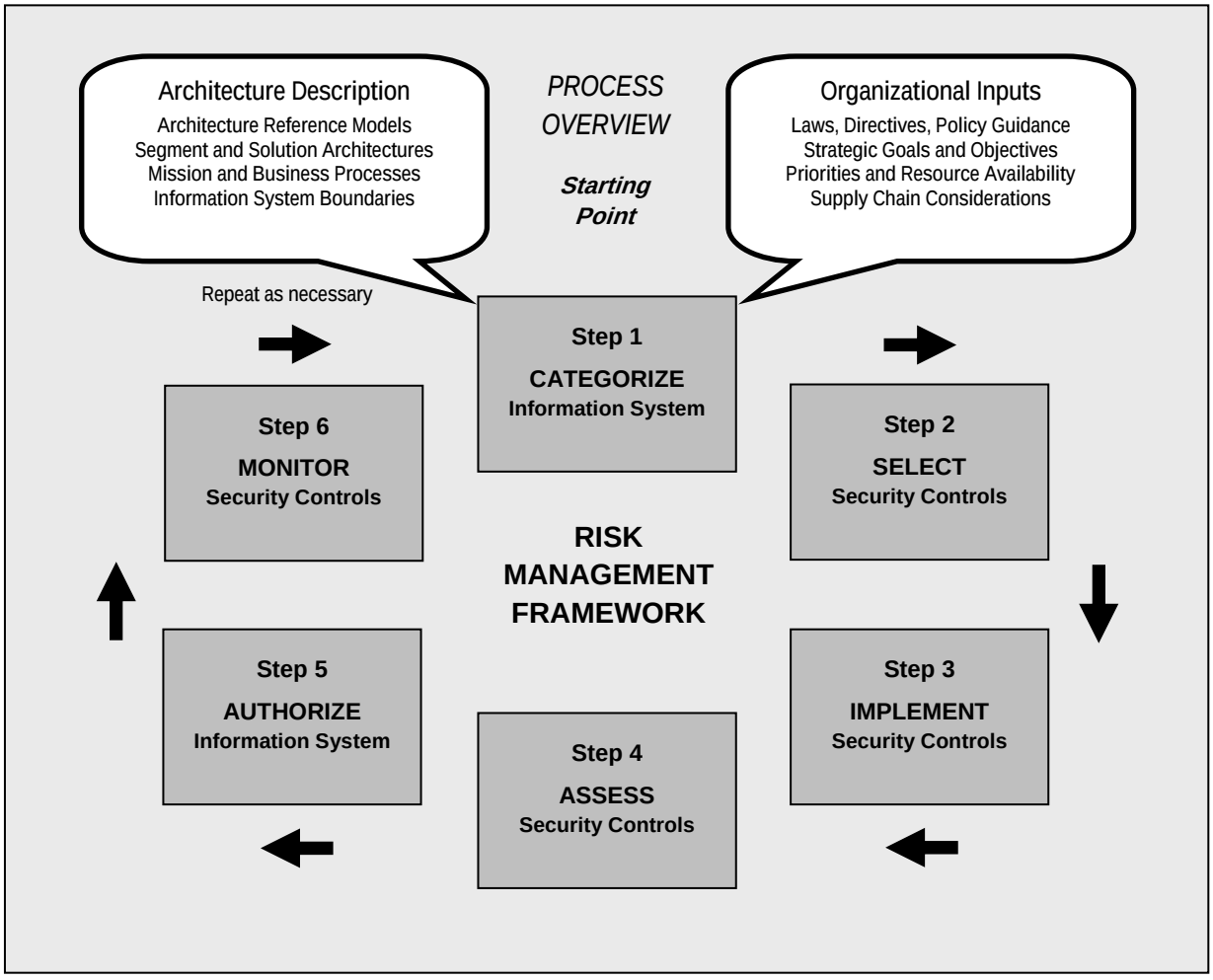
FREQUENTLY ASKED QUESTIONS

Continuous Monitoring

1. What is continuous monitoring?

Continuous monitoring is one of six steps in the Risk Management Framework (RMF) described in NIST Special Publication 800-37, Revision 1, *Applying the Risk Management Framework to Federal Information Systems* (February 2010). See Figure 1 below. The objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur. Continuous monitoring is an important activity in assessing the security impacts on an information system resulting from planned and unplanned changes to the hardware, software, firmware, or environment of operation (including threat space). Authorizing Officials' risk-based decisions (i.e., security authorization decisions) should consider how continuous monitoring will be implemented organization-wide as one of the components of the security life cycle represented by the RMF. The Federal Information Security Management Act (FISMA) of 2002, OMB policy, and the implementing standards and guidelines developed by NIST require a continuous monitoring approach.

FIGURE 1.



2. If my information system is subject to continuous monitoring, does that mean it does not have to undergo security authorization?

No. Security authorization, established in OMB Circular A-130 and reinforced by the risk management concepts in FISMA, requires the explicit review and acceptance of risk by an authorizing official on an ongoing basis. These risk-based decisions are based on security control assessments and continuous monitoring activities. Continuous monitoring does *not* replace the security authorization requirement for federal information systems. Rather, continuous monitoring is implemented as part of a holistic,, risk management and (defense-in-depth) information security strategy that is integrated into enterprise architectures and system development life cycles. The continuous monitoring program, developed and implemented by an organization as a component in the RMF security life cycle-based approach, becomes a consideration in the risk-based decisions (i.e., security authorization decisions) rendered by Authorizing Officials. Continuous monitoring also supports the FISMA requirement for conducting assessments of security controls with a frequency depending on risk, but no less than annually.

3. Why is continuous monitoring not replacing the traditional security authorization process?

Continuous monitoring in and of itself, does not provide a comprehensive, enterprise-wide risk management approach. Rather, it is a key component in the risk management process. NIST has been working with the Department of Defense, the Intelligence Community, and the Committee on National Security Systems to develop a unified information security framework for the federal government and its contractors. The fundamental tenet of the unified information security framework is an enterprise-wide risk management approach to information security that is life cycle-based and implemented across three hierarchical tiers within an organization (i.e., governance, mission/business process, and information system). The RMF, the central construct in NIST Special Publication 800-37, employs a security life cycle approach when considering information system security. The six-step RMF fundamentally transformed the previous Certification and Accreditation (C&A) process to provide emphasis on “front-end” and “back-end” security. The ongoing determination and acceptance of information system security-related risks remains the primary responsibility of Authorizing Officials and for which they are held accountable. Continuous monitoring activities contribute to helping Authorizing Officials make better risk-based decisions, but do not replace the security authorization process.

4. What is front-end security and how does it differ from back-end security?

Front-end security, exemplified by the first three steps in the RMF (security categorization, security control selection, and implementation), focuses on building security into information technology products and systems early in the system development life cycle. The initial steps are also linked to the organization’s enterprise architecture and information security architecture. Better front-end security results in fewer weaknesses and deficiencies in information systems, directly translating to a lesser number of vulnerabilities that can be exploited by threat sources. Back-end security, exemplified by the last three steps in the RMF (security control assessment, information system authorization, and continuous monitoring), focuses on the effectiveness of the implemented security controls, the determination and acceptance of risk, and the ongoing monitoring of the security state of the information system. The RMF overall provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.

5. What is NIST doing to provide greater emphasis on front-end security?

NIST is developing two important guidance documents that address information system security engineering and application-level security. These publications will provide organizations with best practices in building and acquiring more secure information technology products and systems. The guidance can be used by organizations to provide specification language to contractors and vendors in federal acquisitions.

6. If continuous monitoring does not replace security authorization, why is it important?

A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static and occasional security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to senior leaders. Senior leaders can use this information to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of their information systems. A continuous monitoring program allows an organization to track the security state of an information system on an ongoing basis and maintain the security authorization for the system over time. Understanding the security state of information systems is essential in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes.

7. Who should be involved in continuous monitoring activities?

Organizations are required to develop a continuous monitoring strategy for their information systems and environments in which those systems operate. A robust continuous monitoring program that derives from that strategy requires the active involvement of information system owners and common control providers, mission and business owners, chief information officers, senior information security officers, and authorizing officials.

8. What role does automation play in continuous monitoring?

Automation, including the use of automated support tools (e.g., vulnerability scanning tools, network scanning devices), can make the process of continuous monitoring more cost-effective, consistent, and efficient. Many of the security controls defined in NIST Special Publication 800-53—especially in the technical families of Access Control, Identification and Authentication, Auditing and Accountability, and Systems and Communications Protection—are good candidates for monitoring using automated tools and techniques (e.g., the Security Content Automation Protocol). Real-time monitoring of implemented technical controls using automated tools can provide an organization with a much more dynamic view of the security state of those selected controls. It is also important to recognize that with any comprehensive information security program, all implemented security controls, including management and operational controls, must be regularly assessed for effectiveness, even if the monitoring of them is not easily automated. Sophisticated adversaries have been exploiting and continue to exploit the weakest controls, and true security for an information system or an organization is dependent on all controls remaining effective over time.

9. How is NIST promoting the use of automation for continuous monitoring activities?

NIST continues to develop, with its government and industry partners, a range of technologies and processes that employ automation to support security status discovery (i.e., situational awareness) and continuous monitoring activities. For example, the Security Content Automation Protocol (SCAP) project improves the automated application, verification, and reporting of information technology product-specific security configuration settings, enabling organizations to identify and reduce the vulnerabilities associated with products that are not configured properly. Security automation seeks to improve the

availability and accuracy of the most current threat and attack data available, not only by creating standardized methods for identifying and referencing threats and vulnerabilities, but also by providing the fundamental methods by which that data can be collected and shared quickly. This data can then be used to adapt security controls to real-world, real-time situations, which can change rapidly. Such automation also facilitates timely data collection, aggregation, analysis, data feeds and reporting to senior officials at the operational, mission/business process, and governance tiers of the organization.

10. Why is the holistic approach to risk management using the RMF important?

Effective risk management can be achieved by placing equal emphasis on all six steps of the RMF from security categorization and security control selection to continuous monitoring. Adversaries continuously launching a range of cyber attacks from simplistic to sophisticated, respect only one thing: the strength of an organization's defenses. Strength of defenses is a function of the selected security controls, the quality of control development and implementation, and the effectiveness of control operations. NIST security standards and guidelines have long advocated risk-based processes and continuous monitoring for federal information systems. NIST publications have also emphasized the concept of balanced information security, flexibility of security control implementation, defense-in-depth, and a holistic approach to organizational information security programs. Continuous monitoring is an important activity and is most effective when implemented as part of a comprehensive RMF. It is one of many tools in an organization's arsenal that can be employed to strengthen the defenses of the information systems supporting core missions and business processes.

11. What security controls should be subject to continuous monitoring?

Organizations develop security plans containing the required security controls for their information systems and environments of operation based on mission and operational requirements. All security controls deployed within or inherited by organizational information systems are subject to continuous monitoring. NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, provides a comprehensive, state-of-the-practice catalog of management, operational, and technical security controls based on the most current threat and attack information available. This security control catalog facilitates a defense-in-depth protection capability that includes people, processes, and technologies—a mutually reinforcing set of safeguards and countermeasures to address threats from cyber attacks, human error, and natural disasters.

12. How often should security controls be monitored?

Organizations have the flexibility in current legislation, policies, standards, and guidance to monitor and assess their security controls at a frequency that most effectively manages risk. Some security controls (e.g., vulnerability and network scanning) may require monitoring much more frequently than other controls which may tend to be more static in nature (i.e., less subject or susceptible to change). As long as all security controls selected and implemented by the organization are assessed for effectiveness during the required authorization cycle to demonstrate security due diligence, OMB and FISMA requirements are satisfied.

13. Are there any risks associated with continuous monitoring?

Organizations should exercise caution in focusing solely on continuous monitoring at the expense of a holistic, risk-based security life cycle approach. Without the appropriate planning for security controls (preferably early in the system development life cycle) and the correct implementation of those controls, the value of continuous monitoring is greatly diminished. This is because the near real-time,

ongoing monitoring of weak and/or ineffective security controls resulting from flawed information security requirements can result in a false sense of security.

14. How can common controls and automation reduce the cost and resources required for security control implementation, assessment, and continuous monitoring?

Organizations can significantly reduce the resources required for security control implementation, assessment, and continuous monitoring by maximizing the use of enterprise-wide *common controls*. Common controls are a security capability provided by the enterprise that can be inherited by multiple information system owners without each owner having to fully repeat the process. Examples of common controls include infrastructure-related controls for physical and personnel security. Common controls can also be deployed in information systems, for example, in boundary protection and incident response systems deployed at key network entry points. An effective selection and implementation of common controls as part of steps two and three in the RMF can facilitate more consistent and cost-effective security across the enterprise. The use of automation to determine the effectiveness of deployed security controls (e.g., using the tools, techniques, and content associated with the Security Content Automation Protocol [SCAP] initiative), can also contribute to cost-effective information security. Automation, however, cannot be used to assess and monitor all security controls (e.g., the management, operational, and technical controls that are not sensitive to automation).

15. How can organizations address advanced persistent cyber threats?

To address the advanced persistent cyber threat requires a multi-pronged effort by organizations. First, it requires a major change in strategic thinking to understand that this class of threat cannot always be kept outside of the defensive perimeter of an organization. Rather, this is a threat that in all likelihood, has achieved a foothold within the organization. This situation requires that organizations employ methods to constrain such threats in order to ensure the resiliency of organizational missions and business processes. Second, it requires the development and deployment of security controls that are intended to address the new tactics, techniques and procedures (TTPs) employed by adversaries (e.g., supply chain attacks, attacks by insiders, attacks targeting critical personnel). NIST Special Publication 800-53, Revision 3, includes many new security controls and enhancements (most not selected in any of the control baselines) that are specifically intended to address some of these TTPs. Finally, to enable cyber preparedness against the advanced persistent cyber threat, organizations must enhance risk management and information security governance in several areas. These include, but are not limited to: (i) development of an organizational risk management and information security strategy; (ii) integration of information security requirements into the organization's core missions and business processes, enterprise architecture, and system development life cycle processes; (iii) allocation of management, operational, and technical security controls to organizational information systems and environments of operation based on an enterprise security architecture; (iv) implementation of a robust continuous monitoring program to understand the ongoing security state of organizational information systems; and (v) development of a strategy and capability for the organization to operate while under attack, conducting critical missions and operations, if necessary, in a degraded or limited mode.

16. Are continuous monitoring activities only applicable during the monitoring step in the RMF?

No. Continuous monitoring capabilities are most valuable as security tools, providing on-demand, real-time visibility into the security state of deployed information systems (post authorization). However, if available and where possible, continuous monitoring capabilities can also be effectively used during the pre-deployment RMF security control assessment step as an important link between front-end and

back-end security. Program managers and information system owners can, and are encouraged to, employ continuous monitoring capabilities to couple security control implementation with security control assessment, using a variety of iterative life cycle development models.

17. Where can organizations obtain additional information on continuous monitoring?

Information on continuous monitoring for information systems and associated environments of operation can be obtained in NIST Special Publication 800-53, Revision 3 and NIST Special Publication 800-37, Revision 1. NIST is also developing additional guidance on continuous monitoring that will be available in the near future in Special Publication 800-137, targeted for release in the summer 2010.