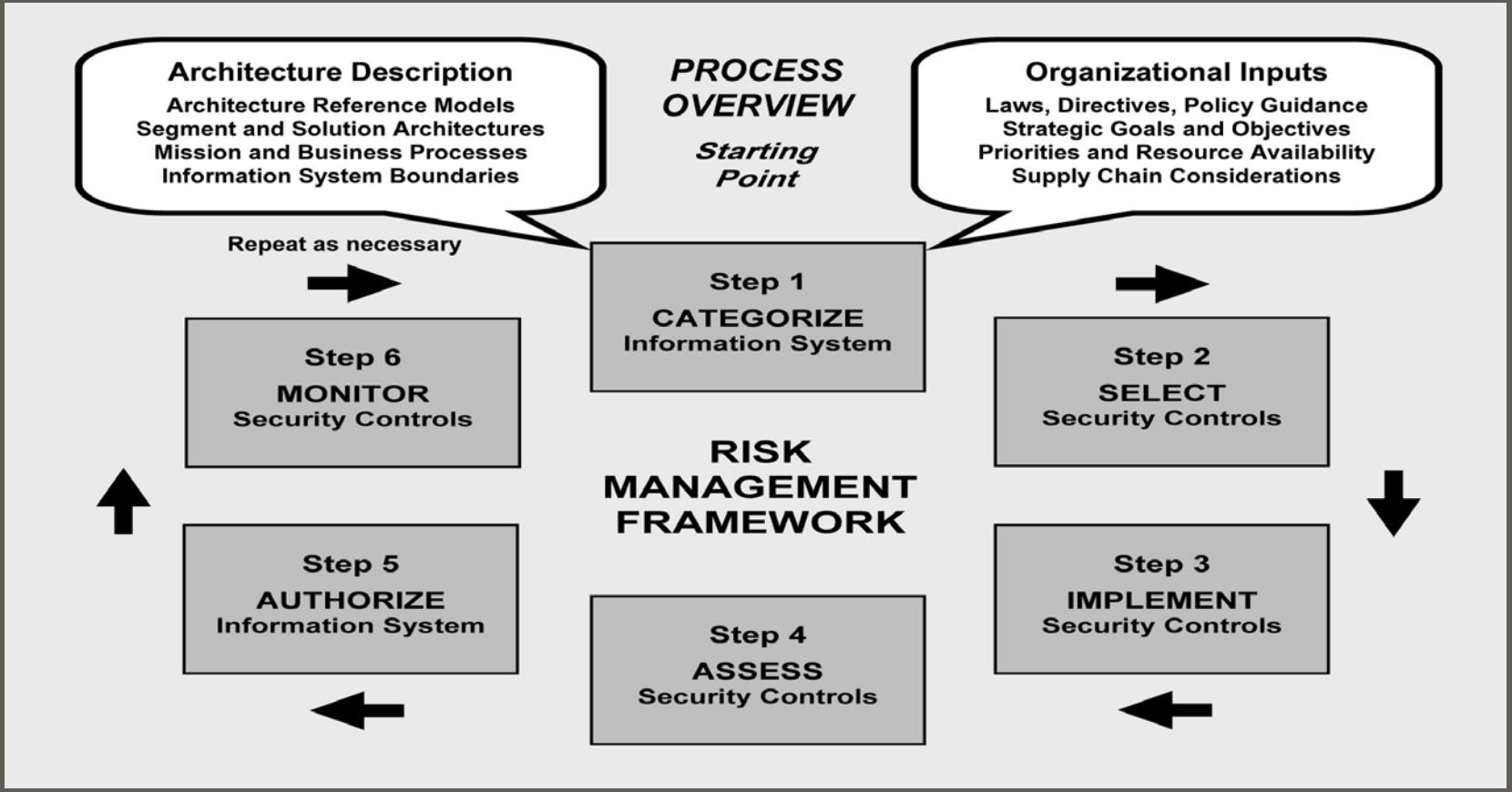
Continuous monitoring is one of six steps in the Risk Management Framework (RMF) described in NIST Special Publication 800-37, Revision 1, *Applying the Risk Management Framework to Federal* Information Systems . See Figure below.



- 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 determines the security impact of proposed or actual changes to the information system and its environment of operation.

- A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is an essential element of an effective security control monitoring program.

- 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.

- Documenting proposed or actual changes to an information system or its environment of operation and subsequently assessing the potential impact those changes may have on the security state of the system or the organization is an important aspect of security control monitoring and maintaining the security authorization over time. Information system changes are generally not undertaken prior to assessing the security impact of such changes.

- Subsequent to the initial authorization, the organization assesses a subset of the security controls (including management, operational, and technical controls) on an ongoing basis during continuous monitoring.

- The selection of appropriate security controls to monitor and the frequency of monitoring are based on the monitoring strategy developed by the information system owner or common control provider and approved by the authorizing official and senior information security officer.

- The assessment information produced by an assessor during continuous monitoring is provided to the information system owner and common control provider in an updated *security assessment report. The* information system owner and common control provider initiate remediation actions on outstanding items listed in the plan of actions and milestones and findings produced during the ongoing monitoring of security controls.

- Security controls that are modified, enhanced, or added during the continuous monitoring process are reassessed by the assessor to ensure that appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate the identified risk.

- To facilitate the near real-time management of risk associated with the operation and use of the information system, the organization updates the security plan, security assessment report, and plan of action and milestones on an ongoing basis.

- The updated security plan reflects any modifications to security controls based on risk mitigation activities carried out by the information system owner or common control provider. The updated security assessment report reflects additional assessment activities carried out to determine security control effectiveness based on modifications to the security plan and deployed controls.

- The updated plan of action and milestones: (i) reports progress made on the current outstanding items listed in the plan; (ii) addresses vulnerabilities discovered during the security impact analysis or security control monitoring; and (iii) describes how the information system owner or common control provider intends to address those vulnerabilities.

- The results of monitoring activities are recorded and reported to the authorizing official on an ongoing basis in accordance with the monitoring strategy. Security status reporting can be: (i) event-driven (e.g., when the information system or its environment of operation changes or the system is compromised or breached); (ii) timedriven (e.g., weekly, monthly, quarterly); or (iii) both (event- and time-driven).

- The authorizing official or designated representative reviews the reported security status of the information system (including the effectiveness of deployed security controls) on an ongoing basis, to determine the current risk to organizational operations and assets, individuals, other organizations, or the Nation.

- The authorizing official determines, with inputs as appropriate from the authorizing official designated representative, senior information security officer, and the risk executive (function), whether the current risk is acceptable and forwards appropriate direction to the information system owner or common control provider.

- By carrying out ongoing *risk determination and risk acceptance, authorizing officials* can maintain the security authorization over time. Formal reauthorization actions, if required, occur only in accordance with federal or organizational policies.

Question:

1) **If 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.

Question:

2) **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.

Question:

3) **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.

Question:

4) **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.

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.

Question:

5) **What security controls should be subject to continuous monitoring and how often?**

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.

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.