Assured Compliance through Information Security Continuous Monitoring

Trey Breckenridge
Director, High Performance Computing
Mississippi State University

24 July 2018
Summary

Information Security Continuous Monitoring (ISCM) is defined by NIST as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. While monitoring for compliance is an objective in implementing an effective ISCM program, an effective ISCM strategy must also provide managers with a continuous means to assess overall security status in order to make informed and timely risk management decisions.
Continuous monitoring allows managers to maintain an ongoing state of compliance and awareness of current risks to organizational information systems over time in a highly dynamic environment with constantly changing threats, vulnerabilities, technologies, and processes.

It should help managers determine the effectiveness of risk responses, changes to information systems and their environment, and verify compliance with applicable laws, executive orders, regulations, policies, and guidelines.
ISCM Program Goals

Goals of an effective ISCM Program include:

- Maintain a current security status of all assets in the most efficient manner possible.
- Assist in making risk-based, strategic investments in IT and other security-related infrastructure.
- Identify redundancies and/or deficiencies in the existing information security program.
- Reduce the burden of compliance through the use of automation and predefined organizational processes.
- Leverage relationships with internal and external stakeholders to ensure a broad and relevant perspective on the information security program.
NIST SP 800-171 and ISCM

- Security requirement 3.12.3 states that organizations should “Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.”

- While continuous monitoring itself is an explicit requirement of NIST SP 800-171, an effective ISCM program necessarily overlaps with the entire “Security Assessment” family of controls.

- Ultimately, the continuous monitoring program should achieve a status of ongoing compliance with the requirements outlined in NIST SP 800-171.
Automating Continuous Monitoring

- The ISCM program should address and involve all facets of security including people, processes, and technology. That said, organizations should assess which portions of the ISCM program should or should not be automated.
- There is a wide range of tools available that can assist organizations with monitoring system level information. Managers should assess what existing capabilities they have, how that can fit into the ISCM program, and what security controls/requirements those tools address.
- Managers should consider ISCM tools that:
  - pull information from a variety of sources
  - use open specifications
  - offer a high degree of interoperability
  - support the overall compliance posture
  - Support viewing aggregate data while allowing analyst to drill down to the system-level
  - Are compatible with existing or planned SIEM tools
Tips for Implementing the ISCM

• Designate one individual or a specific set of individuals to manage the ISCM program and maintain the Continuous Monitoring (ConMon) plan.
• Develop a ConMon plan that provides a means to assess every security requirement/control on a recurrent basis.
• Have quarterly, semi-annual, or annual meetings with key staff to review the ISCM program status.
Important Questions

• How does my organization leverage people, processes, and technology to implement the Security Assessment family of security controls?

• How is my organization’s ISCM program complimenting other security requirements (e.g. updating the POA&M, SSP, or testing the incident response plan on a regular basis)?
Conclusion

• The ISCM program should provide a plan for monitoring systems, security relevant processes, and applicable security controls and/or requirements.

• The ConMon plan allows organizations to achieve a state of ongoing compliance where managers can maintain sufficient knowledge of the security state of the information systems under their purview. This information is used to make a determination as to whether or not the system is operating at an acceptable level of risk to the organization.

• Continuous Monitoring allows a means to provide ongoing updates to all relevant SSPs and POA&Ms.