Continuous Monitoring of Information Systems

Christopher Furton

Syracuse University

Continuous monitoring plays a vital role in ensure information systems maintain a level of security throughout the lifecycle. According to the Nation Institute of Standards and Technology (NIST), continuous monitoring is defined as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support operational risk management decisions" (Dempsey, Johnson, Jones, Orebaugh, Scholl, & Stine, 2010). The objective is to conduct ongoing monitoring of the security of an organization's networks, information, and systems, and respond by accepting, avoiding/rejecting, transferring/sharing, or mitigating risk as situations change" (Dempsey, Johnson, Jones, Orebaugh, Scholl, & Stine, 2010). The process of continuous monitoring is important in many different industries, but this paper will discuss the role it plays in the Department of Defense (DoD).

Within the DoD, continuous monitoring can help organization comply with mandates from the Federal Information Systems Management Act (FISMA) (Executive Office of the President, 2010). FISMA drives organizations to comply with Certification and Accreditation (C&A) processes. For C&A to be successful, organizations must maintain the security controls set forth and verify that the system is maintained at the authorized risk level. Since the primary tasks of continuous monitoring (1. configuration management and control, 2. security control monitoring, and 3. status reporting and documentation) directly correspond with C&A requirements, the resulting near-real time monitoring and reporting of the system status contributes to FISMA compliance by maintaining system accreditation (OnPoint, NA).

Besides the role that continuous monitoring has in the C&A process and FISMA compliance, continuous monitoring provides for significant advantages in terms of overall security posture. When implemented, continuous monitoring can help with many functions of information security and information technology such as change management, configuration

management, log monitoring, network monitoring, patch management, risk management, and vulnerability scanning (OnPoint, NA). If well-designed, continuous monitoring can also be involved with administrative process such as external reporting requirements and inventories (Dempsey, Johnson, Jones, Orebaugh, Scholl, & Stine, 2010).

Another key benefit of continuous monitoring involves the relationship with risk and how the output of continuous monitoring can help shape organizational decisions. Risk decisions affect overall operational security as well as system accreditation decisions. Utilizing continuous monitoring to provide inputs to the risk decisions can improve decisions by providing more complete and accurate information specifically when conducting security impact analyses prior to implementing a change (Dempsey, Johnson, Jones, Orebaugh, Scholl, & Stine, 2010).

Although continuous monitoring offers many advantages, the implementation can be challenging. As noted in a report from the Inspector General of the National Aeronautics and Space Administration, accurate inventory lists and lack of a control to provide for 100 percent assurance that all assets were part of the monitoring were a barrier to effective continuous monitoring of IT security controls (NASA Office of Audits, 2010). In addition to difficulty in getting a continuous monitoring solution in place, it is possible that failures could occur and go undetected due to blind reliance on the system.

Regardless of some of the disadvantages, the future of ensuring systems are kept current and that reporting of system state is automated looks promising. In early 2011, the Department of Homeland Security (DHS) has published a Request for Information (RFI) to industry to perform market research on capabilities and industry interest in continuous monitoring. The general requirements set forth by DHS is indicative of interest especially since the RFI details a

very comprehensive list of general requirements from vulnerability assessment to performance reporting (Department of Homeland Security, 2010).

In summary, continuous monitoring offers great promise for the future of managing information system security. Specifically for the federal government, the principles of continuous monitoring can help with compliance to law as well as achieve certification and accreditation. When leveraged, continuous monitoring can help managers make better risk decisions. There are some disadvantages, but with the industry involvement sought by DHS, the future of continuous monitoring looks good.

References

Dempsey, K., Johnson, A., Jones, A. C., Orebaugh, A., Scholl, M., & Stine, K. (2010). *Information Security Continuous Monitoring for Federal Information Systems and Organizations.* U.S. Department of Commerce. Gaithersburg: National Institute of Standards and Technology.

Department of Homeland Security. (2010, December 8). Information Security Continuous Monitoring Capability Request for Information (RFI). Washington DC, USA.

Executive Office of the President. (2010, April 21). *FY2010 Reporting Instructions for the Federal Information Systems Management Act and Agency Privacy Management.* Washington, D.C.

NASA Office of Audits. (2010). *Audit of NASA's Efforts to Continuously Monitor Critical Information Technology Security Controls.* Office of Inspector General.

OnPoint. (NA). *Continuous Monitoring White Paper.* Arlington: OnPointCorp.

About the author

Author: Christopher Furton

Website: Http://christopher.furton.net

Certified professional with over 12 years of Information Technology experience and 8 years of hands-on leadership. An expert in cyber security with both managerial and technical skills proven throughout a career with increasing responsibility and performance expectations. Known ability to translate complex information for universal understanding. Detail-driven, results-focused leader with superior analytical, multitasking, and communication skills. Well-versed in industry best practices including Project Management and IT Service Management. Currently holding active CISSP, CEH, ITIL Foundations, Security+, and Network+ certifications.

Visit the auhor's blog:
IT Management Perspectives - https://christopherfurton.wordpress.com/

Social Sphere:

LinkedIn | Twitter | Google+ | Quora | Wordpress | Flavors.me

Slide Share | Tumblr | YouTube | Pinterest | About.me | Vimeo