Continuous Monitoring: What It Is, Why It Is Needed, and How to Use It

Sponsored by Tripwire

Continuous Monitoring: What It Is, Why It Is Needed, and How to Use It

June 2011

A SANS Whitepaper

Written by: *E. Eugene Schultz, Ph.D.*

Advisor: *Marcus H. Sachs, Director Emiratis, SANS Internet Storm Center*

Introduction

There's no denying that complying with annual Federal Information Security Management Act (FISMA)[1] audits is expensive and cumbersome. It is also understood that compliance to FISMA requirements does not accomplish the most important goal of improving overall security posture. The Department of State recently reported that it has spent approximately $133 million in six years on FISMA compliance.[2] On a larger scale, Delaware Senator Tom Carper estimates that complying with FISMA costs the U.S. government $2.3 billion annually—$1 billion of which goes directly into audit.[3]

Since its inception in 2002, FISMA has become a gigantic annual checklist that takes government organizations thousands of man-hours per year to prepare for and conduct audits against. Agencies and departments prepare for these audits by filling out forms, answering standard questions and creating large amounts of paperwork. FISMA auditors then evaluate this paperwork and write audit reports based on their evaluation of its completeness in addressing FISMA-mandated standards.

In addition to the checklist mentality around FISMA compliance, the focus on annual, point-in-time audits does not meet the needs of today's dynamic networks. End points, network devices, systems and applications, and security tools and processes that passed a FISMA compliance checklist yesterday could become noncompliant in the blink of an eye. Failure to patch a system, install a security update, or prohibit a user from downloading an application can all suddenly render secure systems vulnerable.

The government's answer to this problem is to develop a more continuous view into the state of devices and applications to maintain a more continuous compliant state. In April 2010, the Office of Management and Budget (OMB) released new guidelines calling on agencies and departments to provide FISMA auditors with real-time information about the state of their systems and networks. This new and far better approach includes the concept of continuous monitoring as defined in National Institute of Standards and Technology (NIST) Special Publication 800-137 rev 1 (NIST SP 800-137),[4] "Information Security Continuous Monitoring for Federal Information Systems and Organizations." Published in December 2010, this draft presents guidelines for applying NIST's Risk Management Framework (RMF) to Federal Information Systems.

Although there are many continuous monitoring guidelines and definitions in circulation (see Appendix A), this paper focuses on the NIST 800-137 guidelines.

---

1 FISMA: The Federal Information Security Management Act. Accessed at http://csrc.nist.gov/groups/SMA/fisma/overview.html.

2 J. Nicholas Hoover, "New Policy Revamps Agencies' Approach to FISMA Compliance," Dark Reading, April 22, 2010. Accessed at http://mobile.darkreading.com/9287/show/3fea49995065b81666bf7604a8f6e11e&t=e918e12ffe8307a7ebcac20d5b6b0c67.

3 Tom Carper, "**Opening Statement: "More Security, Less Waste: What Makes Sense for our Federal Cyber Defense.**" Testimony before Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, October 29, 2009. Accessed at http://carper.senate.gov/public/index.cfm/otherstatements?ID=4e4123f9-4742-4f1b-a18f-515fbb9d6d85.

4 http://csrc.nist.gov/publications/drafts/800-137/draft-SP-800-137-IPD.pdf

Benefits of Continuous Monitoring

The NIST Risk Management Framework (RMF) emphasizes the importance of near real-time risk management and continuous information systems authorization through strong and effective continuous monitoring processes. It also encourages the use of automation to give top-level management the critical information needed to make cost-effective, risk-based decisions that support their primary missions as well as their business processes.

Continuous monitoring applies to many of the RMF's six sequential steps for integrating information security and risk management processes to the NIST risk management hierarchy. Continuous monitoring indirectly supports all six controls, while directly supporting three controls (boldfaced below):

- **Categorizing information systems**
- Selecting security controls
- Implementing security controls
- **Assessing security controls**
- Authorizing information systems
- **Monitoring security controls**[5]

Monitoring directly assists in the first step of this process—categorizing information systems—from which organizations can derive the secondary benefit of selecting and implementing the proper security controls. Monitoring tools start their processes with initial discovery, usually through passive listening, to determine, among other things, what devices and applications are on the network and the type of traffic, data, and user access with which they're associated. This information helps organizations provide a baseline assessment to determine where they'll need to monitor—but by no means is a replacement for manual discovery processes such as talking to business units, and other such information-gathering options.

Continuous monitoring enables information security professionals and others to see a continuous stream of near real-time snapshots of the state of risk to their security, data, the network, end points, and even cloud devices and applications. Assessing security controls as well as ongoing monitoring of security controls are both directly assisted by continuous monitoring through vulnerability monitoring processes, which many organizations already have in place.

5 Although NIST SP 800-137 lists this step as "Monitoring Security Controls," the term "continuously" is implied.

Many systems, datasets, end points and applications are already being monitoring by system and security administrators with a variety of tools that can be leveraged in the continuous monitoring ecosystem. Most important are tools that can measure the vulnerability and compliance state of network devices and the security tools themselves, as well as integrate with other security toolsets. This gives organizations near real-time visibility into their compliance state and also aids in incident detection and response by providing additional information to the event management system, often a Security Information Event Management System (SIEM) or log management system.

In this way, continuous monitoring, when implemented through a log manager or SIEM for log and event collection and correlation, helps organizations separate real events from nonimpact events, as well as locate and contain events. Using continuous monitoring for event detection and for vulnerability detection is also becoming part of external discussions about what continuous monitoring includes. For example, the Consensus Audit Guidelines' Top 20 Security Controls for Effective Cyber Defense cites continuous monitoring of audit logs, continuous assessment, inventory and monitoring for secure configuration as top controls.[6]

The guidelines, developed by government defense and law enforcement agencies in conjunction with the SANS Institute, also list real-time monitoring of account activity, sensitive data movement, malware and threats as equally important components of the continuous monitoring process. This level of integration between vulnerability and event monitoring is critical, given that government entities such as defense agencies are top targets for attackers and hactivists, according to multiple reports.

Because the network is constantly being evaluated, continuous monitoring also greatly improves the level of situational awareness for IT managers. Situational awareness is a term coined by Mica Endsley, who describes the term as having a perception of elements in the environment, understanding the meaning of the elements in the environment, and applying the understanding to being able to project future states.[7] In other words, situational awareness is the awareness of current elements in the monitored environment that are relevant because they may potentially impact that environment today or in the future.

Situational awareness through full network visibility is a key means for mitigating risk. In testimony about real risk reduction to come about through continuous monitoring, the State Department reports a 90 percent improvement in its risk posture after implementing a continuous monitoring program.[8]

6 www.sans.org/critical-security-controls/

7 Mica R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems." In Human Factors Journal, March 1995, Volume 37(1), pages 32–64.

8 www.state.gov/documents/organization/156865.pdf

As an example of how continuous monitoring reduces risk, imagine a critical patch cycle that wasn't implemented on certain machines because of a gap in coverage left after an administrator was transferred to a different work group. Without continuous monitoring constantly evaluating the security state of these machines, this gap could go undiscovered until the next annual audit, making them susceptible to exploit. With continuous monitoring, this gap would be noticed during the next routine upgrade cycle, when the monitoring system checks for new patch levels.

Ultimately, continuous monitoring and the visibility it provides enable top-level management and key stakeholders to improve governance through ongoing evaluation of critical control factors. This also helps prevent a situation in which areas of risk get so far out of line over time that they pose excessive danger to the organization and also become far more difficult and expensive to correct.

Finally, if implemented early in the System Development Lifecycle (SDLC), continuous monitoring can reduce the costs involved with system and application maintenance. Cost improvements are also inevitable when monitoring is both continuous and as automated as possible, including the required reporting documents that support FISMA (potentially saving thousands of hours of labor that government organizations are currently spending to comply with FISMA). When compiled over time, the reports can also show auditors the improving state of security and risk management, while predicting other areas in need of improvement—something future iterations of compliance mandates will likely require.

In June, the DHS and Whitehouse announced changes in FISMA's FY 2011 Chief Information Officer FISMA Reporting Metrics" that requires agencies to report on their progress in automating the continued daily measurement and assessing their progress in implementing sensors. In a SANS Newsbytes, Alan Paller, director of research at SANS Institute, approved of the new guidelines adding, "What gets measured gets done."

What, How, and Where to Monitor

What to monitor, how to monitor and where to monitor can mean almost anything to any government IT department. So it's important to determine what needs to be monitored and set monitoring policies around those needs.

Start with Policy Requirements

In the SDLC, ensuring that the requirements analysis is done properly is the most important of all activities. If requirements are not valid and complete, all activity that follows will go in the wrong direction. Requirements analysis must begin with obtaining information about business needs and stating clearly what problem continuous monitoring program is intended to solve. This requires true understanding of the organization's business and operational processes and goals, as well as barriers (such as limited financial resources) to achieving these goals.

Define the functions that the processes and technical components the continuous monitoring effort will depend upon, then develop appropriate performance metrics for those functions. For example, a requirement might be 99.9 percent up time, with full functionality for each piece of technology in use, and an output latency of no greater than one second. The requirements analysis must also specify levels of compatibility between the different technology components involved in the monitoring program. Finally, the requirements analysis must also elucidate how each technology component, the physical environment, and any critical data gathered via logs and elsewhere must be secured. At a minimum, for example, all controls that monitor controls should be located in a locked server room with greatly restricted access and must require strong (e.g., biometric) authentication for everyone who uses them.

A good starting point is to conduct interviews with officials within the organization as well as with others in organizations that have similar goals and operations. Also read reports about incidents that have occurred in the past, collect and review any use cases that have been written, evaluate findings from recent internal and third-party audits and automated assessments, and review and evaluate organizational assets and risk management processes. The more thorough and accurate the requirements analysis is, the more effective the continuous monitoring effort will be.

Know What to Monitor and What Not to Monitor

Continuous monitoring does not require that everything—all systems, applications, networks, end points, infrastructure, security processes, and so on—be monitored everywhere and all the time.

In its documentation, NIST identifies a three-tiered impact system—low, moderate and high impact—to use when developing monitoring policies. An example of a low impact system might be a public web server serving up only public information and not taking in private information (although it could be argued that website monitoring is important to prevent intrusion). A high impact system, on the other hand, would include a central database cluster storing highly sensitive information related to U.S. intelligence efforts. Continuously monitoring the databases, traffic and clients/servers accessing the database should be a major focus of 24 x 7 x 365 monitoring.

Once it is determined what systems and processes need monitoring, policy should include events that would trigger these systems to send alerts. For example, permission changes, kernel modifications, and unauthorized changes to applications should all send alerts and the monitoring system should be set to look for correlating activities. One or two failed access attempts followed by a successful access request, on the other hand, may not be so important.

Determine Monitoring Intervals

Continuous monitoring does not imply true, real-time 24 x 7, nonstop monitoring and reporting. Instead, it means implementing monitoring and oversight processes that provide a clear picture of security state at a given time, while also providing a mirror of control effectiveness over time.

Routine scans can be conducted regularly, such as every five, 10 or 15 minutes, every hour or every day; and log data can be collected from the central manager at regular intervals. Information needed to monitor critical data, as well as the data processing resources and their controls, should be continuously collected. System administrators and/or security engineers should inspect the output of these tools as frequently as needed, based on the amount of risk associated with information and computing resources. Some events would require immediate action, for example any unauthorized changes to system configurations should be reported in near real-time and coordinated against other system information to check for authorization.

The following table shows NIST's recommendations for frequency of log monitoring and other related measures: [9]

CATEGORY	LOW-IMPACT SYSTEMS	MODERATE-IMPACT SYSTEMS	HIGH-IMPACT SYSTEMS
How Often to retain log data	1 to 2 weeks	1 to 3 months	3 to 12 months
How often to rotate logs	Optional (if performed, at least every week or every 25 MB)	Every 6 to 24 hours, or every 2 to 5 MB	Every 15 to 60 minutes, or every 0.5 to 1.0 MB
If the organization requires the system to transfer log data to the log management infrastructure, how frequently that should be done	Every 3 to 24 hours	Every 15 to 60 minutes	At least every 5 minutes
How often log data needs to be analyzed locally (through automated or manual means)	Every 1 to 7 days	Every 12 to 24 hours	At least 6 times a day
Whether log file integrity checking needs to be performed for rotated logs	Optional	Yes	Yes
Whether rotated logs need to be encrypted	Optional	Optional	Yes

Table 1: Recommended Frequency of Log Monitoring and Other Measures (From NIST SP800-92)

The higher the impact of a security breach, the more frequently log data and security controls need to be monitored. According to these guidelines, log data associated with low impact systems should be analyzed every one to seven days, log data associated with moderate impact systems should be analyzed every 12 to 24 hours, and log data associated with high impact systems should be analyzed at least six times every day.

9 Kent, Karen, NIST SP800-92, "Guide to Computer Security Log Management: Recommendations of the National Institute of Standards and Technology." Accessed at http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf.

Don't Forget the Cloud

With analysts predicting huge growth in cloud adoptions over the next few years, it is also important to develop your continuous monitoring program with the cloud in mind. Guidance from the Cloud Security Alliance (CSA)[10] and from NIST in NIST SP 800-114[11] calls for a concerted continuous monitoring effort of cloud service providers' (CSPs') environments, operations, and governance-related activities such as updating information security.

The CSA advises organizations to monitor and evaluate cloud chain of dependency, which involves mapping risks in connection with application program interfaces (APIs) and controlling any potentially security-related risks that could turn out to be severe. It also advises implementing a systematic vulnerability scanning and mitigation program for CSP systems and networks, a systematic configuration control program for CSP systems and networks, and continuously monitoring for data protection and unauthorized activities in the cloud. If you are using a public cloud service provider, understand that it is the CSP's responsibility to monitor its own log data (e.g., host audit logs, firewall logs, and so forth). Be sure to know the CSP's policies and establish alerting criteria and procedures.

Continuous Monitoring Is Not a FISMA Replacement

Regulations like FISMA will always be applicable to government IT operations. Rather than replacing compliance and audit (C&A), continuous monitoring will be the single most important support for C&A by providing deeper information that can be analyzed over time. The trending information, then, will become more important for compliance and for overall improvements in operations, security and risk posture. Security trending and improvement information will likely become major input requirements for future iterations of government IT system compliance mandates.

9 Kent, Karen, NIST SP800-92, "Guide to Computer Security Log Management: Recommendations of the National Institute of Standards and Technology." Accessed at http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf.

10 Cloud Security Alliance, "Security Guidance for Critical Areas." Accessed at https://cloudsecurityalliance.org/csaguide.pdf.

11 National Institute of Standards and Technology, "User's Guide to Securing External Devices for Telework and Remote Access." Accessed at http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf.

Bring Everyone On Board

Page 8 of the NIST guidelines for continuous monitoring contains a pyramid depicting three levels or tiers involved in continuous monitoring, including organization, mission/business process, and operational IT level. In the diagram, **Information Systems** are at the bottom of the pyramid, supporting the other two levels. Above IS, at the **organization level**, governance strategies and structures for assessing and managing security-related risk must be created. Above that, at the **mission and business process level**, missions and business processes must be prioritized according to an organization's objectives and goals, and a strategy for identifying and protecting critical information must be created.

Risk assessment, evaluation, treatment, acceptance and monitoring strategies must also be developed with multiple parties, including non-technical business managers, involved. The program should be able to identify, quantify and report control failures in other areas, such as when duplicate supplier or customer records exists, or when inappropriate multiple payments have been made in violation of separation of duty policies, or when purchases bypass purchase rules.

Manage Monitoring Output

Procedures should detail the steps to be performed in every critical monitoring-related task, including evaluating output from systems and devices. For example, procedures should list exactly what must be done to enter output data into CyberScope.[12] Introduced by the Department of Homeland Security (DHS), CyberScope is a highly interactive reporting tool designed to take FISMA reporting input, such as system audit log data, and create a spreadsheet supplied through a government portal/cloud to FISMA auditors.

CyberScope is an attempt to reduce the heavy load of having to send 100 separate spreadsheets and paper copies of the inspectors' general security audits to the Office of Management and Budget (OMB) via email. Unfortunately, 85 percent of federal security managers had not used CyberScope by the mandated OMB deadline of November, 2010.[13] NIST's attempt at standardizing security information through the Security Content Automation Protocol (SCAP) will help relieve some of the interoperability, correlation and translation problems preventing adoption.[14] As CyberScope and SCAP continue to develop and mature, monitoring vendors will better support this interface, making these reports much easier to fulfill.

12 Jeffrey Zients, Vivek Kundra, and Howard Schmidt, "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," October 21, 2010. Accessed at www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf.

13 J. Nicholas Hoover, "Feds Unlikely To Meet Cybersecurity Compliance Deadline," InformationWeek, October 11, 2010. Accessed at www.informationweek.com/news/government/security/227701081.

14 http://scap.nist.gov/

Conclusion

Complying with FISMA has become excessively burdensome and expensive for government organizations and hasn't much improved their security and risk management postures. FISMA audits only represent a point-in-time snapshot of the organization's risk posture, which could change as quickly as a user hits a 'Download Now' button or an administrator fails to patch properly.

Continuous monitoring replaces point-in-time audits with a continuous view of the state of the network, its systems (including security systems), data and access attempts. Continuous monitoring promises many benefits to government organizations, including reduced paperwork, lowered expense, full visibility into their risk posture, and ultimately, overall better information security programs.

Before starting a continuous monitoring program, it is imperative to know what continuous monitoring is, what it is not, and how to leverage tools already in place to provide monitoring data needed to fulfill requirements. Organizations have many of the monitoring-specific tools and security devices within their networks to produce logs. They also have log management and SIEM systems to tie the data together for better risk posture and event management. These components, along with strong monitoring policies, are instrumental in continuous monitoring efforts today and in the future as new requirements arise.

Appendix A: Regulations That Require Continuous Monitoring

Numerous regulations require or strongly recommend continuous monitoring, either specifically or by implication. These regulations are highlighted below.

NIST SP 800-137—NIST Special Publication 800-137 contains the U.S. government's base requirements for a continuous monitoring effort, as described throughout this paper.

NIST SP 800-53—NIST Special Publication 800-53 describes automated inspection items in connection with a CA-2 (security assessment), CA-4 (security certification) and CA-7 (continuous monitoring and vulnerability detection) continuous monitoring program. The prescribed frequency of monitoring is daily, but it may sometimes be hourly. An example of an automated inspection item would be automated determination of the integrity of system and application files and directories.

NERC/FERC CIP—NERC/FERC CIP-005-1-R1.6 states that "an electronic Security Perimeter should be established that provides . . . Monitor and Log Access 24X7X365." In other words, organizations must continuously monitor network and log access.[15]

ISO/IEC 27001—ISO 27001 provides a description of an information security management system that calls for continual process improvement in information security.[16] To accomplish this goal, an organization must continuously monitor its own security-related processes and improve according to feedback from objective measurements.[17]

FISMA/FISMA 2—FISMA and FISMA 2 also require continuous monitoring activities that include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting.

---

15 Standard CIP-005-1—Cyber Security—Electronic Security Perimeter(s), 2006, page 2.

16 International Standard ISO/IEC 27001, Information technology—Security techniques—Information security management systems—Requirements, 2005, page11.

17 Ibid, page 6.

About the Author

Eugene Schultz, Ph.D., CISM, CISSP is chief technology officer of Emagined Security and the author/co-author of books on UNIX security, Internet security, Windows NT/2000 security, incident response, and intrusion detection and prevention. He was also the co-founder and original project manager of the Department of Energy's Computer Incident Advisory Capability (CIAC).

SANS would like to thank its sponsor:

Last Updated: December 13th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CAUS	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Osaka 2018	Osaka, JP	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, SG	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Paris March 2018	Paris, FR	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	OnlineCAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced