Bill Hargenrader, CISM, CEH, CISSP, is a senior lead technologist at Booz Allen Hamilton, where he is developing a next-generation cybersecurity workflow management software solution. He is working on his doctorate degree in information technology, focusing on the intersection of cybersecurity and innovation.

Information Security Continuous Monitoring

The Promise and the Challenge

Combining an organization-applicable risk framework with an all-encompassing control set and an information security continuous monitoring (ISCM) methodology provides for a holistic approach to compliance and risk management by providing controls across a wide array of areas with a high level of detail and guidance on tailoring.[1] An enterprise could apply this approach to risk management by assessing the organization, integrating the risk management framework and establishing a security baseline based on the security control standards. When the controls are continually monitored, assessed and addressed, the organization has taken a big step toward reducing its security risk potential.

There is an ongoing movement toward adopting ISCM at the federal level, as well as within the US Department of Defense (DoD), due to US Federal Information Security Management Act (FISMA) compliance requirements. Though the compliance issues are federal in nature, there are lessons to be learned and technology improvements that can be implemented in any industry, such as finance, utilities and health care. In 2013, the US Department of Homeland Security (DHS) presented all federal agencies with a blanket purchase agreement worth up to US $6 billion for reduced-cost continuous monitoring software.[2] The US Office of Management and Budget (OMB) has offered guidance on how continuous monitoring will be able to replace the current three-year accreditation cycles.[3]

Disponible également en français
www.isaca.org/currentissue

ISCM has the promise of being the next best thing for cybersecurity and risk management, but there are still some immaturities and challenges that exist in the methodologies and software. In this regard, three areas should be examined relating to ISCM. Those three areas are manual vs. automated logging, current technology available, and control sampling frequency.

BACKGROUND INFORMATION ON ISCM

The primary literature studied for this research on ISCM was developed by the US National Institute of Standards and Technology (NIST). "NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems."[4] NIST provides detailed guidance on implementing a risk management framework.[5] It also provides a detailed and broad control set for federal agencies to adopt—though any organization can adopt the controls as standards. A combination of the risk management framework, control set and the continuous monitoring implementation guidance can be used to set up a federally accepted continuous monitoring plan. Three key NIST Special Publications are described in **figure 1**.

Figure 1—Key NIST Special Publications Related to ISCM

Special Publication Title	Subject Matter
NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems	Guidance for applying enterprise-level risk management to an organization
NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations	A multitiered approach to risk management through control compliance. This approach includes security control structure, security control baseline and security control designations.
NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	A holistic, enterprise-level approach to setting a continuous monitoring strategy, implementing a program and executing the activities of the program

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

Some of the gaps in the research dealing with continuous monitoring are that the vast array of studies undertaken have been conducted in the area of audit, energy, medical and sensor network. This opens the possibility of transferring a technology or algorithm from a disparate field. For instance, the implementation of continuous auditing and decision processes to be included in the early design stages of emergency response processes[6] would have a strong correlation to designing continuous monitoring into a system from the start. Some advances could be orchestrated and pose the potential to leap ahead in the area of ISCM by modeling these other areas.

EVALUATION OF CONTINUOUS MONITORING RISK MANAGEMENT COMPLIANCE FRAMEWORK

Continuous monitoring is one of six steps in the Risk Management Framework (RMF).[7] When properly selecting a framework, it is critical to choose one that will effectively support operations as well as the controls that the organization uses for compliance.[8] The selection can be viewed across four areas of security, service, operations and governance. Information assurance (IA) exists in all of these areas as well, because the aim is to ensure that the mission can be completed and these four areas all play a role in a mission's effectiveness. There have been many updates on how to address risk management, but among the more prominent is NIST SP 800-37 combined with the NIST SP 800-53 and NIST SP 800-137. Together these documents thoroughly address the IA area of risk management and compliance, and do so in continuous fashion.

RISK MANAGEMENT FRAMEWORK REFERENCE

NIST SP 800-37 provides guidance for applying a risk management program to an organization. As the types of sophisticated, well-organized attacks have increased, the potential for higher levels of damage to national security has increased as well.[9] For organizations to understand their chances of becoming compromised and the damage done from that compromise, a system of continuous assessment of vulnerabilities, impacts, mitigations and residual risk acceptance should be adopted. Without a comprehensive system in place, an organization is essentially leaving itself open to chance. SP 800-37 provides for that system and a means of implementing it, but it is up to the organization to tailor and implement it effectively.

The process involves the following steps: Categorize information systems, select security controls, implement security controls, assess security controls, authorize information systems and monitor security controls. SP 800-37 revolves heavily around control assessment to determine the level of risk an organization is facing. The level of compliance or completeness with the established security controls can give leadership an idea of the overall risk level of the organization, as well as provide guidance on what areas should be improved through policy, technology or personnel.

SECURITY CONTROLS REFERENCE

Critical to the risk management framework are the controls that fit into that framework. SP 800-53 uses a multitiered approach to risk management through control compliance. This approach includes security control structures, a security control baseline and security control designations.[10] SP 800-53 works hand in hand with SP 800-37 in that the controls are overlayed on top of the risk management framework for an organization. The controls are selected based on the criticality and sensitivity of information owned by the system and are applied in a suggested order with identified higher priority controls first. The controls include identification and authentication, contingency planning, incident response, maintenance, risk assessment, and media protection, among many others.

INFORMATION SECURITY CONTINUOUS MONITORING REFERENCE

Continuous monitoring can be a ubiquitous term as it means different things to different professions. NIST SP 800-137 sets forth a standard to follow when applying the principle in the risk management framework utilizing the NIST control set. The primary process for implementing ISCM is to:[11]

- Define the ISCM strategy
- Establish an ISCM program

- Implement an ISCM program
- Analyze data and report findings
- Respond to findings
- Review and update the monitoring program and strategy

Factored into this is the use of manual and automated checks to provide continuous updates and feedback to the system as a whole.

Though these three NIST Special Publications form a solid foundation for continuous security monitoring, risk management and compliance, there are some areas that need to be addressed and reviewed for effectiveness. Automated technology drives the push for continuous monitoring and has been the focus of ISCM efforts;[12] however, only so many controls can be tracked via an automated process, which presents a potential gap in the control set for activities that are performed manually. There is also the matter of technology available. One of the largest federal ISCM projects has issued a suite of automated tools to provide this function. The question with these tools is how many controls they cover. And, there is the matter of control sampling frequency. NIST SP 800-137 offers guidance, but not specifics.

THE ADVANTAGES AND DISADVANTAGES OF THE MODEL: MANUAL VS. AUTOMATED PROCESSES

One of the advantages of the ISCM model is that it captures aggregate data from already-existing systems in automated fashion. This automated process provides for real-time, up-to-the-minute information to be collected and reviewed by leadership. One of the disadvantages of the model is that not all activities take place in an automated or networked fashion. It may not be easy to capture and log automatically, for example, when planning for acquisitions took place or that a policy was updated. In addition, there is no volume of federal guidance on manual logging. In NIST SP 800-137, manual checks and procedures are called out as needing to comply with the same level as automated checks.

One potential solution would be to provide a manual logging mechanism for actions completed. This could be a login interface to communicate when someone has finished backing up a server or performed a security sweep of a remote location server room. Sign-in sheets for access to controlled areas could also be automated, perhaps by signing in on a tablet that logs times and names and identifies unusual patterns of behavior, such as entry at a late hour that is against the norm. The review of advantages and disadvantages of physical vs. automated solutions can be complemented by a survey of current continuous monitoring solutions.

COMPARISON OF CONTINUOUS MONITORING SOFTWARE SOLUTIONS

Guidance from the OMB states that, "The continuous monitoring phase must include monitoring all management, operational, and technical controls implemented within the information system and environment in which the system operates including controls over physical access to systems and information."[13] In this regard, a table was created that lists all the DHS applications that are being offered to federal systems, as noted previously.[14] The software was reviewed online and categorized against the NIST control category and control type (**figure 2**).

After the data were collected and reviewed, a comparison table was created to show how many control types were used and how many were not used. A high-level estimate was made from these data of the effectiveness at total coverage of the currently offered automated solution.

CONTINUOUS MONITORING SOFTWARE ANALYSIS

Of the 21 control families, eight are covered by the DHS continuous monitoring software offerings. Additionally, there are numerous specific controls under the control types that are not covered. From a very high-level view, only 38 percent of control types are affected by software offering. This leaves room for future improvements. There are software solutions not on this list that cover some of the control categories. In addition, there currently is not a system that integrates the data feeds from each of these individual software packages.

FREQUENCY OF CONTROL ASSESSMENT

Sampling frequency factors that should be taken into consideration are risk level, changes in the control item (often intermittent), and whether the control is in an open or incomplete state.[15] Risk level is how much of an impact there would be if a vulnerability related to the control were exploited. The thresholds and timing have to be set by the organization's leadership and by that of the overarching governing agency body.

A public web server may have a higher risk level than a file server on the domain located securely within the enclave; the chances are lower of it being attacked, and there would be less impact if it were taken offline. In this way, public servers may

Figure 2—NIST SP 800-53 Control Count Cross-reference by Family			
Count 1	**Control Family Not Covered by DHS Applications**	**Count 2**	**Control Family Covered by DHS Applications**
1	Planning	1	System and information integrity
2	System and service acquisition	2	Risk assessment
3	Security assessment authorization	3	Incident response
4	Program management	4	Asset management
5	Personnel security	5	Audit and accountability
6	Physical and environmental	6	Configuration management
7	Contingency planning	7	Malware detection
8	Maintenance	8	Identity access
9	Media protection		
10	Awareness and training		
11	Identification and authentication		
12	Audit and accountability		
13	System and communications protection		

be chosen to be sampled more frequently. The sensitivity of the data would have to be taken into consideration as well. If the file server contains US Social Security numbers, it could require a higher sampling frequency than the public web server.

Certain controls, such as reauthorizing user access annually, may have to be sampled only twice a year for a particular program if that process occurs only once a year. It would be a waste of resources, computing power and storage to sample that control every minute, day or week. The spectrum for controls most likely ranges from a scale of annually, to every second year. Developing a road map for an organization, or a standard best practices timeline, would save time and energy. It will also facilitate buy-in from the user community. If they are being asked to report something more frequently than they know they have to, the whole concept of continuous monitoring could gain a bad reputation in the organization.

CONCLUSION

ISCM has a major positive impact on improving risk management and compliance across many industries and bodies, including the US federal government, the DoD, and commercial and financial organizations. The technology available today goes a long way toward improving security, though temperance should be used when conveying what problems this solves as there are some glaring holes in what is currently available. Future research could include looking for a solution to fill the gaps in control coverage, such as a physical logging mechanism, to input workflow activities into an automated system for aggregation. Establishing best practices for the control sampling frequency provides the necessary timing for the manual logging. One final proposed change to the model would be to connect both the continuous monitoring solution to a single dashboard for managing overall risk. Working from this model would be able to show organizations which areas are being continuously monitored and which areas still need to be tracked the traditional way. Though the promise of ISCM is great, there are many challenges to overcome to realize complete implementation. The only way to overcome those challenges is to get started on implementing ISCM and to share the lessons learned with the cybersecurity community.

ENDNOTES

[1] National Institute of Standards and Technology, Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," USA, 2013, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*

[2] Bennett, C.; "With $6 Billion Continuous Monitoring Contract, DHS Takes 'Next Leap' in Cybersecurity," Fedscoop, 2013, *http://fedscoop.com/with-6-billion-continuous-monitoring-contract-dhs-takes-next-leap-in-cybersecurity/*

[3] Zients, J. D.; "Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," Office of Management and Budget, 2012, *www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf*

[4] National Institute of Standards and Technology, Special Publication 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," USA, 2011, p. 3, *http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf*

[5] National Institute of Standards and Technology, Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," USA, 2010, *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf*

[6] Chumer, M.; R. Hiltz; R. Klashner; M. Turoff; "Assuring Homeland Security: Continuous Monitoring, Control & Assurance of Emergency Preparedness," *Journal of Information Technology Theory and Application*, 2004, vol. 6(3), p. 1-24, *http://search.proquest.com.library.capella.edu/docview/200008540?accountid=27965*

[7] *Op cit*, NIST 2010

[8] Schlarman, S.; "Selecting an IT Control Framework," *Information Systems Security*, 2007, 16(3), p. 147-151

[9] *Op cit*, NIST 2010

[10] *Op cit*, NIST 2013

[11] *Op cit*, NIST 2011

[12] US Department of Homeland Security, "Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS)," Federal Network Security Branch, 2010, *https://www.dhs.gov/continuous-asset-evaluation-situational-awareness-and-risk-scoring-reference-architecture-report*

[13] *Op cit*, Zients, p. 11

[14] US Department of Homeland Security, "BPA Awardees and Tool Suites," *Federal Times*, 2013, *http://apps.federaltimes.com/projects/files/bpa_awardees.pdf*

[15] *Op cit*, NIST 2011