Risk Management Framework Today

Formerly DIACAP Dimensions

... And Tomorrow

November, 2012
Issue 2, Volume 2

Continuous Monitoring Takes Center Stage

By Lon J. Berman

Continuous Monitoring is one of the cornerstones of the Risk Management Framework (RMF). The idea behind continuous monitoring is not new; it is simply being given much greater emphasis. The dynamic threat environment faced by all information systems demands continuous vigilance to guard against attack and compromise. Traditional "point in time" assessments are just not good enough anymore!

It is now generally accepted that, in the absence of a sustained and concerted effort, the security posture of any information system is bound to deteriorate over time.

NIST Special Publication (SP) 800-137 is dedicated to the subject of continuous monitoring. It defines Information Security Continuous Monitoring (ISCM) as "… maintaining ongoing awareness of information security, vulnerabilities and threats to support organizational risk management decisions." NIST then outlines a six-step process for implementation of continuous monitoring in any organization.

The six steps are:

- **Define** the ISCM strategy
- **Establish** an ISCM program
- **Implement** the ISCM program
- **Analyze** and **Report** findings
- **Respond** to findings
- **Review** and **Update** ISCM strategy and program

The recommended strategies are based on an organizational structure consisting of three "tiers":

- Tier 1 – Organization
- Tier 2 – Mission/Business Process
- Tier 3 – Information System

Cont. on page 6

Testing for Windows STIG Compliance

By Kathryn M. Farrish

DoD requires information systems to comply with "all applicable Security Technical Implementation Guides (STIGs)." For Windows-based computers, this has traditionally been accomplished by utilizing the Gold Disk, a security tool developed and distributed by the Defense Information Systems Agency (DISA).

Recently, however, DISA has shifted its strategy away from development and maintenance of security tools, instead focusing on publishing lists of vulnerabilities in machine-digestible format using the Security Content Automation Protocol (SCAP). Their stated expectation is that end users will have access to commercial vulnerability scanning tools that can be leveraged in conjunction with the DISA-published SCAP content. For example, DISA now publishes a "Windows 7 Automated Benchmark". This SCAP file contains specification for each of the OS settings mandated by the STIG, and the steps needed to test for compliance.

Cont. on page 2

In this issue:

Testing for Windows STIG Compliance

(Continued from page 1)

In order to test a Windows 7 workstation for compliance with the STIG, a DoD or contractor site will need to "feed" the automated benchmark file into a commercially available scan engine, such as eEye Retina, McAfee Policy Auditor, or Tenable Security Center, which will then provide a compliance report.

DISA currently publishes automated benchmarks for numerous Windows versions:

- Windows 7
- Windows Vista
- Windows XP
- Windows Server 2003**
- Windows Server 2008**
- Windows Server 2008R2**

** Note there are both DC (Domain Controller) and MS (Member Server) versions of these benchmarks

Also available are benchmarks for Internet Explorer and for the following UNIX-family systems:

- AIX
- HP-UX
- Red Hat
- Solaris

Additional automated benchmarks are anticipated for databases such as Oracle and Microsoft SQL Server, and web servers such as Apache and Microsoft Internet Information Server (IIS).

In recent months, the US Navy's SPAWAR directorate has released a tool designed specifically for measuring STIG compliance using the DISA automated benchmarks. This tool is called Security Compliance Checker (SCC) and is available through the DISA information assurance website or directly from SPAWAR (see URLs below). SCC requires minimal training and produces easy-to-read output that groups the findings based on the specific Windows tools and input screens needed to address them. It even provides a global "percentage rating" to readily show your progress toward full compliance. SCC versions are available for Windows, as well as UNIX-family systems (RedHat, Debian, and Solaris).

Terms of use are as follows: "[SCC] is designed to review computer security settings and can be installed on any U.S. Federal Government computer or any computer that is mandated to comply with U.S. Federal Government security regulations such as OMB M-08-22, FISMA, HIPPA, NIST FDCC, NIST USGCB, DISA STIGs and IRS."

DISA: https://iase.disa.mil

SPAWAR: www.public.navy.mil/spawar/Atlantic/ProductsServices/Pages/SCAP.aspx

Top Ten Continuous Monitoring Considerations

By Robert E. Lee, Jr.

The latest "buzzword" in the information security industry is "continuous monitoring." Everyone seems to be talking about the need for "near real time" assessment of security posture. Many organizations have attempted to address this very legitimate need by deploying a hodgepodge of monitoring tools and attempting to somehow sort through the resulting mountain of disjointed information to try and extract meaningful, actionable intelligence. Oftentimes, the results are both frustrating and disappointing. Organizations that start with a carefully-crafted continuous monitoring *strategy* are much more likely to be successful in their efforts. "Growing pains" are inevitable, but good strategy will ensure the pain stays well below the organization's threshold of frustration.

This month we present the Top Ten considerations for developing a continuous monitoring strategy and program.

10. Organizational structure. An effective continuous monitoring program relies on good communication throughout the organization, "horizontally" as well as "vertically". Understanding the organizational structure is critical for establishing and maintaining appropriate lines of communication.

9. Roles and responsibilities. Everyone's responsibilities should be clearly defined so there is no ambiguity and no excuse for saying "I didn't realize that was my job".

8. Organizational risk tolerance. Management must determine, *and clearly document*, what is considered "acceptable risk".

7. IT landscape. In order to ensure effective monitoring, the organization's IT landscape must be thoroughly understood. This includes not only hardware and software, but also the physical and logical interfaces and interconnections among these assets.

6. Resource availability. Federal departments and agencies typically provide enterprise-level resources that can be leveraged to enhance the continuous monitoring efforts of all organizations within the enterprise. A thorough understand of the services offered by the enterprise is critical to deploying a cost-effective continuous monitoring program.

5. Policies and procedures. Like any other business process, the continuous monitoring program should be supported by written policies and procedures. Where appropriate, templates should be developed to streamline information flows.

4. Assessment frequencies. In order to effectively monitor security posture, organizations must determine assessment frequencies that are appropriate to the organization and consistent with its risk tolerance.

3. Reporting. Reporting must be designed to maximize effective communication of information in a way that is easily understood by its intended audience and provides *actionable* intelligence.

2. Education and training. Training will make all the above steps go more smoothly, and serve to minimize errors and false starts. System and process owners must determine the types of training needed, the personnel who will need to attend, and the preferred delivery modality (e.g., classroom training at a vendor's training center, "on site" training", or web-based training).

1. Funding and management support. Process owners must ensure management "buy in", assess the costs of implementing the complete continuous monitoring program … not just licensing of automated tools … and submit any necessary funding requests. As is the case for so many other things, "when it comes to funding, earlier is

IA Control Spotlight—Dissecting a NIST Security Control

By Betsy K. Taylor

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization:

a. Monitors physical access to the information system to detect and respond to physical security incidents;

b. Reviews physical access logs [*Assignment: organization-defined frequency*]; and

c. Coordinates results of reviews and investigations with the organization's incident response capability.

Supplemental Guidance: Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.

Control Enhancements:

(1) The organization monitors real-time physical intrusion alarms and surveillance equipment.

(2) The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.

References: None.

Priority and Baseline Allocation:

P1	LOW PE-6	MOD PE-6 (1)	HIGH PE-6 (1) (2)

NIST Security Controls are new to many of us that are accustomed to working in the DoD environment. In order to effectively make the transition from DIACAP to RMF, we need to quickly become accustomed to reading and working with them. You probably still have fond, or not so fond, memories of dissecting a frog in high school biology class. Well, that's exactly what we're about to do. Here, then, is the "anatomy" of a NIST Security Control.

The ID of the control is PE-6; this tells you this is the sixth control in the Physical and Environmental (PE) family. The name of the control is "Monitoring Physical Access". Below the name is the actual statement of the control. In this case, there are three elements, annotated (a), (b) and (c). Notice that element (b) contains something called an "Assignment". What this means is that NIST does not provide a specific frequency for reviewing physical access logs; rather, this is something that needs to be determined by the organization. This is called an "organization-defined parameter" and there are a multitude of them within the various NIST controls.

Below the control text is some supplemental guidance to assist the organization in implementing the control. For this control, the supplemental guidance is short, but for others it is quite lengthy.

PE-6 contains two optional Control Enhancements that are to be applied under certain circumstances as described below. This control also contains a "placeholder" for references, but none are provided. For other controls, a list of relevant reference documents from, NIST, DoD, or other sources, is provided.

The shaded box at the bottom provides several items of information. The "P1" at the left side is a suggested "implementation priority" and can range from P1 (highest priority) to P3 (lowest priority). Some controls are marked "P0" which means NIST has not provided a suggested priority.

The remainder of the shaded box shows how the control is to be applied for each of the three system categorization baselines. In this case, systems categorized as Low are expected to implement PE-6 without any enhancements, Moderate systems are expected to implement PE-6 along with enhancement (1), while High systems must implement PE-6 along with enhancements (1) and (2). NOTE: if the control is *not* required at a particular baseline level, it will be shown as "Not Selected".

Once you get acclimated to this format, you'll find it very easy to work with … and much less slimy than a frog!

Ongoing Authorization—Reality or Fantasy?

By Lon J. Berman

"Continuous monitoring" is the buzzword of the day in federal information security circles. Organizations everywhere are talking about the need to keep tabs on their security posture in a "near real time" fashion. The conversation almost always includes disdainful references to point-in-time assessments, paper drills, and other such allegedly "worthless" exercises.

No reasonable security professional doubts that, *with carefully planning and implementation*, continuous monitoring can significantly enhance the security posture of federal systems and information.

Another perceived benefit of continuous monitoring is the eventual sunset of re-accreditation (or re-authorization) of information systems. Traditionally, systems required re-authorization at least every three years (per OMB Circular A-130). However, NIST Security Control CA-6 states, ""To reduce the administrative burden of the three-year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible as the basis for rendering a reaccreditation decision." In other words, authorizing officials have the latitude to simplify the reaccreditation process by leveraging information provided by the continuous monitoring process. OMB has taken this a step further in its instructions for FISMA reporting, stating "Continuous monitoring programs thus fulfill the three year security reauthorization requirement, so a separate reauthorization process is not necessary."

This concept is called "ongoing authorization" It appears "all" we need to do is to show the authorizing official (DAA) that we're doing effective continuous monitoring, and reaccreditation becomes a thing of the past. Sounds great in theory, but there are several reasons to temper the "end zone celebration" on this one. First of all, continuous monitoring is a young, immature craft, and very few system owners can legitimately claim to have implemented it fully and effectively. Secondly, many departments and agencies have yet to "embrace" the concept of ongoing authorization.

Lastly, and perhaps most importantly, there is some evidence to suggest there may be flaws in the concept. The evidence comes not from the world of information security, but from the "real world" of manufacturing and distribution. Traditionally, manufacturers and distributors relied on point-in-time inventories to assess the availability of products. The result was all-to-frequent backorders, overstocks, etc. In the past 20-30 years, automated inventory management has become the norm, as sales and order processing systems are linked to automated inventory systems. Many in the industry experimented by doing away with point-in-time inventories altogether, but, in the long run, they learned that periodic physical inventory is still a necessity. There is some chance that the same will be found to be true for information security, and we will end up in a world where point-in-time assessment and continuous monitoring coexist.

Stay tuned!

Continuous Monitoring Takes Center Stage

(Continued from page 1)

The role of automation in continuous monitoring is discussed as it relates to numerous Security Automation Domains, including:

- Vulnerability and patch management
- Event and incident management
- Malware detection
- Asset management
- Configuration management
- Network management
- License management
- Information management
- Software assurance

NIST SP 800-137 is intended to complement the baseline set of RMF publications, including SP 800-37 (Risk Management Framework), SP 800-39 (Organizational Risk Management), and SP 800-53 (Recommended Security Controls).

BAI has now expanded its training portfolio to include a three-day program dedicated to Information Security Continuous Monitoring (ISCM). The course includes thorough coverage of policies and procedures, based on NIST SP 800-137, as well as practical guidance on organizational communication, automated tools, etc.

ISCM training is available on a regularly-scheduled basis at our various training locations, as well as "on-site" for a group of students at *your* location.

BAI Launches "Personal Classroom" Training

By Lon J. Berman

If you're in need of DIACAP RMF, FISMA RMF or Continuous Monitoring training but lack the schedule flexibility and/or travel budget to attend one of our regularly-scheduled classes, we now have an exciting new option for you!

BAI will soon begin offering "Personal Classroom" training that combines the best features of traditional instructor-led classes *and* web-based training. Using your PC and telephone, you can actively participate in an instructor-led class from the comfort of your home or office. Courses are divided into 2 to 3 hour modules, making it easy to fit into your busy schedule.

Classes are forming now for training programs beginning in January, 2013. Please call us at 540-808-1050 to reserve your space or for more information.

Contact Us!

RMF Today … and Tomorrow is a publication of BAI DIACAP/RMF/FISMA Resource Center, Fairlawn, Virginia.

Phone: (540) 808-1050
Fax: (540) 808-1051
Email: RMF@RMF.ORG

Training for Today … and Tomorrow

BAI now offers three training programs:

- **DIACAP RMF** – recommended for DoD employees and contractors; covers the legacy DIACAP and DoD IA controls, the new RMF and NIST security controls, the CNSS enhancements, *and* the transition process. Program consists of a one-day "Fundamentals" class, followed by a three-day "In Depth" class.
- **FISMA RMF** – recommended for federal "civil" agency employees and contractors, as well as the intelligence community; covers RMF, NIST security controls and CNSS enhancements. Program consists of a one-day "Fundamentals" class, followed by a three-day "In Depth" class.
- **Information Security Continuous Monitoring (ISCM)** – recommended for all; prior knowledge of RMF recommended. This is a three day "In Depth" program.

Regularly-scheduled training dates through March, 2013 are as follows:

DIACAP RMF Fundamentals (One-day)	DIACAP RMF In-Depth (Three-day)
4 Feb 2013 (H)	5-7 Feb 2013 (H)
11 Feb 2013 (NCR)	12-14 Feb 2013 (NCR)
25 Feb 2013 (CS)	26-28 Feb 2013 (CS)
18 Mar 2013 (NCR)	19-21 Mar 2013 (NCR)

(H) - Huntsville, AL (CS) - Colorado Springs, CO
(NCR) - National Capital Region (Ashburn, VA)
(DC) - Washington DC

FISMA RMF Fundamentals (One-Day)	FISMA RMF In-Depth (Three-Day)
3 Dec 2012 (H)	4-6 Dec 2012 (H)
28 Jan 2013 (DC)	29-31 Jan 2013 (DC)
11 Mar 2013 (DC)	12-14 Mar 2013 (DC)

Information Security Continuous Monitoring (ISCM) (Three-day)
19-21 Feb 2013 (DC)
5-7 Mar 2013 (H)
26-28 Mar 2013 (CS)

On-line registration and payment for all scheduled classes is available at **http://register.rmf.org**. Payment arrangements include credit cards, SF182 forms, or purchase orders. Please visit **www.rmf.org** for the latest training schedule, including any new dates or locations.

On-site training. For customers in other locations or those with specific scheduling requirements, we offer the option of "on-site" training. All you need is a group of students (normally 8-10 or more) and a suitable classroom facility. We offer a substantial discount over the normal "per student" fee. Our "on-site" training fee includes all instructional services, training materials, and instructor travel expenses. Most importantly, you will avoid the travel expenses of sending your people to training away from the office. Please contact us to request an on-site training quotation.

Personal Classroom training. Starting in January, 2013, Personal Classroom training will be available. This method enables you to actively participate in an instructor-led class from the comfort of your home or office. Classes are forming now! Please call us at 540-808-1050 for additional information.