Risk Management Framework Today

… and Tomorrow

July, 2017
Volume 7, Issue 3

In this issue:

Continuous Monitoring Today—And Tomorrow

By Lon J. Berman, CISSP, RDRP

Step 6 of the Risk Management Framework (RMF) is entitled "Monitor Security Controls". Many security professionals would argue it is the *most important* step, since monitoring is what transforms RMF from yet another "point in time" evaluation to a true life cycle process. It has been more than three years since the official adoption of RMF, yet no Information Security Continuous Monitoring (ISCM) policy, procedure or guidance has been published by DoD.

Security control CA-7 states:

"The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of [Assignment: organization-defined metrics] to be monitored;

b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;

c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

e. Correlation and analysis of security-related information generated by assessments and monitoring;

f. Response actions to address results of the analysis of security-related information; and

g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]."

For each of the Control Correlation Identifiers (CCIs) comprising this control, the RMF Knowledge Service provides the following Implementation Guidance and Assessment Procedure:

"Future DoD-wide Continuous Monitoring guidance to be published"

Many system owners (and independent assessors!) interpret this to mean CA-7 can legitimately be declared as "Not Applicable" pending publication of DoD-wide guidance.

Is this really the end of the story (for now)? Can we just put the whole ISCM "thing" on the back burner until DoD finally publishes some guidance?

For the sake of your program's mission … not to mention our Nation's security … *I sincerely hope not!*

That's all nice to say, but how can you be expected to establish an effective ISCM program when there is no guidance available?

The answer is that, in reality, there is no shortage of available continuous monitoring guidance – both from DoD and elsewhere. And, beyond that, many technical tools that can be leveraged in support of your ISCM program are already available from DoD.

DoDI 8510.01 (RMF for DoD IT) lays out the system owner's responsibilities for RMF Step 6 (Monitor Security Controls). These include:

- Determining the security impact of proposed changes to the system
- Monitoring the system and environment for security-relevant events
- Periodically assessing of security control implementation
- Reporting significant changes in security posture to the Authorizing Official
- Assessing security controls annually
- Conducting remediation activities based on the results of ongoing monitoring and assessment activities
- Updating the system POA&M on a regular basis

NIST SP 800-37 provides additional guidance on Step 6 activities.

NIST SP 800-137, entitled "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations", is an entire volume dedicated to Continuous Monitoring. It covers topics such as: development of monitoring strategies and monitoring plans, selection of metrics and assessment frequencies, security status reporting, and monitoring program evaluation.

Other government publications supporting continuous monitoring activities include:

See *Continuous Monitoring*, Page 2

"... CSF is not the same as RMF, and it is not a "rip and replace" of RMF..."

Cybersecurity Framework (CSF) as it relates to Risk Management Framework (RMF)

By P. Devon Schall, CISSP, RDRP

I recently attended the Cybersecurity Framework (CSF) Workshop from May 16-17 at NIST in Gaithersburg, Maryland. The workshop proved to be informative in relation to how government and industry are implementing the guidance issued by President Obama in Executive Order 13636. This EO outlines the responsibilities of Federal Departments and Agencies in *Improving Critical Infrastructure Cybersecurity*. President Trump's executive order issued on May 11, 2017 titled, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* reinforced EO 13636 and directly referenced CSF. CSF is a complicated framework, the scope of this article will be to outline concerns about CSF as it relates to RMF.

1. What the heck is CSF? I am just now learning how to do RMF, why is NIST throwing another three-letter framework acronym at me?

Rest assured, I had similar concerns. At a very basic level, CSF is not the same as RMF, and it is not a "rip and replace" of RMF. The writers of CSF assured me that RMF is not going by the wayside and it is a separate framework than RMF. CSF is voluntary guidance based on existing cybersecurity practices to help organize and manage risks. CSF is holistic and targeted toward federal agencies as well as the private sector. Similarities to RMF are a multi-step security lifecycle as well as common language. Additional technical information about CSF can be found in NIST Cybersecurity Framework Draft 1.1.

2. How will CSF change RMF?

I asked this exact question to the folks at NIST. They indicated that those already doing RMF could voluntarily use aspects of CSF to strengthen their RMF activities, and we may see some aspects of CSF implemented in future updates to RMF.

See *Cybersecurity Framework (CSF)*, Page 3

***Continuous Monitoring*, from Page 1**

- NIST SP 800-92, "Guide to Computer Security Log Management"
- NIST SP 800-55, "Performance Measurement Guide for Information Security"
- "US Government Concept of Operations (CONOPS) for Information Security Continuous Monitoring (ISCM)", published by the Joint Cybersecurity Performance Metrics Working Group

DoD has developed numerous tools to support continuous monitoring. These include:

- Assured Compliance Assessment Solution (ACAS) – an enterprise vulnerability scanning and reporting tool
- Host-based Security System (HBSS) – a suite of commercial products that include malware protection and host-based intrusion detection/prevention
- SCAP Compliance Checker (SCC) – a tool that facilitates scanning of operating systems and other software for compliance with DoD Security Technical Implementation Guides (STIGs)
- SCAP benchmarks – content developed by Defense Information Systems Agency (DISA) to support STIG compliance scanning (using SCC) of various commercial software products
- STIG viewer – software tool to facilitate "manual review" of operating systems, database management systems, web servers, etc., for STIG compliance

System owners are encouraged to leverage the above resources to implement a continuous monitoring program *now*. When DoD (finally) gets around to publishing their long-awaited Continuous Monitoring Policy/Guidance document, it will most likely take only minor adjustments to bring your ISCM program into complete compliance.

Between now and then, you'll sleep better!

Registered DoD RMF Practitioner (RDRP)

By Lon J. Berman, CISSP, RDRP

BAI Information Security is pleased to announce the upcoming launch of a new program called *Registered DoD RMF Practitioner (RDRP)* - a network of security professionals specializing in supporting RMF in DoD programs. The requirements to join RDRP are very minimal:

Step 1: Attend 4 days or more of RMF for DoD IT training.

Step 2: Complete the 50 question "RMF for DoD IT Competency Test" with a passing score of 70%.

Step 3: Remit the initial credentialing fee (No cost if you've completed BAI's RMF 4-day training program within the past 12 months).

Your next question may be, why would I want to join the RDRP registry? We feel that being part of the RDRP registry not only adds value to your resume, but it also shows employers and government officials that you have a comprehensive understanding of RMF as it is implemented within DoD.

Another dynamic of RDRP that is worth thinking about is how it relates to The National Initiative for Cybersecurity Education Workforce Framework (NCWF), which is currently in an early draft. The mission of NCWF is to enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge. A major part of NCWF is to define the cybersecurity workforce and identify the training and professional development required by mapping cybersecurity skills to seven cybersecurity categories. These categories are: Securely Provision (SP), Operate and Maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Analyze (AN), Collect and Operate (CO), and Investigate (IN). BAI's courses and RDRP map directly to the family Securely Provision (SP) which includes the specialty area of Risk Management (RM) mapping to a variety of in demand work roles. Over 20 agencies and federal departments worked in partnership to develop NCWF, and I imagine, it will play a more significant role in career development and qualification once a final draft is issued.

For additional information on RDRP, keep an eye on BAI's website and follow the BAI LinkedIn page for announcements. For more on The National Initiative for Cybersecurity Education Workforce Framework (NCWF), review Draft NIST Special Publication 800-181 or join the NICE Working Group (NICEWG) hosted by NIST.

Cybersecurity Framework (CSF), From Page 2

The future integration was described to me as "RMF with a CSF flair". I do not anticipate CSF to immediately impact RMF, but I do think we'll see CSF language in NIST SP 800-53 Rev. 5.

3. How will CSF impact my ATO?

At this point, RMF activities and current ATO's will not be impacted by CSF. CSF is a framework targeted in strengthening cybersecurity posturing for organizations and has many overlaps with RMF, but it is not going to change your current pursuit of an ATO.

Overall, CSF is an interesting framework, and it is encouraging to see the Trump administration recommending its usage. The framework is appealing as being holistic and applicable to businesses of any size. The initial draft is an approachable government document which I highly recommend reading.

Security Control Spotlight— Inheritance from a FedRAMP Approved CSP

By Kathryn M. Daily, CISSP, RDRP

In a previous issue, security control inheritance from an external system hosted at a departmental or agency data center was discussed. In this article, we are going to discuss inheritance from a FedRAMP Approved Cloud Service Provider (CSP) such as Amazon Web Services (AWS), Microsoft Azure, etc.

FedRAMP is an assessment and authorization process for cloud computing products and services. Federal agencies have been directed to use FedRAMP approved cloud computing products and services to ensure that a minimum level of security is provided by the CSP. Like federal information systems, FedRAMP approved CSPs receive an ATO for a period of 3 years, and they go through the A&A process again, or when there is a major change. As with inheriting from another information system, the benefit of using a FedRAMP approved CSP is that it eliminates redundant validation of compliance—the compliance of the "providing system" (CSP) automatically inures to the benefit of the "receiving system" (hosted customer system).

"...This inheritance makes YOUR A&A process much less painful..."

This inheritance makes YOUR A&A process much less painful. For one, Maintenance, Media Protection and Physical and Environmental are completely inherited. Prior to FedRAMP, the Security Control Assessor (SCA) had to visit the data center to check the "gates, guards and guns" every single time, even if that specific assessor had previously visited that data center. That is no longer necessary. The FedRAMP ATO takes care of all of that. In addition, there are several "shared controls" where the CSP provides the capability to fulfill the control, and provided that the customer configured the mechanism appropriately, the control is compliant. One example of this is the Access Control family. AWS provides a tool called Identity and Access Management (IAM) that enables you to securely control access to AWS services and resources for your users. IAM provides the capability to be compliant with much of the Access Control family.

AWS also provides CloudTrail, which provides the capability to be compliant with most of the Audit and Accountability family. You can obtain the System Security Plan for the CSP you choose, which documents the details of the implementation for each of the shared and inherited controls.

At https://marketplace.fedramp.gov you can see all available CSPs, their service models (SaaS, Iaas, PaaS, etc) and the impact level (high, moderate or low). Currently there are 67 CSPs that are 'In Process' and 86 that are approved. You can also fill out the Package Access Request Form which will get you a copy of their FedRAMP artifacts (SSP, ATO, etc). Keep in mind a government employee will need to request the package on behalf of a contractor.

FedRAMP

Contact Us!

RMF Today … and Tomorrow is a publication of BAI Information Security, Fairlawn, Virginia.

Phone: 1-800-RMF-1903
Fax: 540-518-9089
Email: rmf@rmf.org

Training for Today … and Tomorrow

Our training programs:

- **RMF for DoD IT** – recommended for DoD employees and contractors that require detailed RMF knowledge and skill training; covers the RMF life cycle, documentation, security controls, and transition from DIACAP to RMF. The program consists of a one day "Fundamentals" class, followed by a three day "In Depth" class.
- **RMF for Federal Agencies** – recommended for Federal "civil" agency (non-DoD) employees and contractors; covers RMF life cycle, NIST security controls and documentation. Program consists of a one day "Fundamentals" class, followed by a three day "In Depth" class.
- **Information Security Continuous Monitoring (ISCM)** – open to all, however prior knowledge of RMF is recommended. This is a three day "In Depth" program.
- **Certified Cloud Security Professional (CCSP)** – recommended for government employees and contractors working (or planning to work) in the cloud environment, this five-day training program will prepare students for the CCSP certification examination given by ISC2
- **eMASS eSSENTIALS** – recommended for government employees and contractors working (or planning to work) in the DoD environment, this one-day training program provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS (in a simulated environment) is used to reinforce the practical skills needed to use eMASS.

Our training delivery methods:

- **Traditional classroom** – regularly-scheduled training programs are offered at various locations nationwide, including Colorado Springs, Huntsville, National Capital Region (Pentagon/Crystal City area), Pensacola and San Diego.
- **Online Personal Classroom™** – regularly-scheduled training programs are also offered in an online, instructor-led format that enables you to actively participate from the comfort of your home or office
- **On-site training** – our instructors are available to deliver any of our training programs to a group of students from *your* organization at *your* site; please contact BAI at 1-800-RMF-1903 to discuss your requirements

Regularly-scheduled classes through September, 2017:

RMF for DoD IT—4 day program (Fundamentals and In Depth)

- **Huntsville ▪ 7-10 AUG**
- **Colorado Springs ▪ 11-14 SEP ▪ 4-7 DEC**
- **San Diego ▪ 18-21 SEP ▪ 11-14 DEC**
- **National Capital Region ▪ 2-5 OCT**
- **Pensacola ▪ 6-9 NOV**
- **Online Personal Classroom™ ▪ 17-20 JUL ▪ 14-17 AUG ▪ 18-21 SEP ▪ 16-19 OCT ▪ 13-16 NOV ▪ 11-14 DEC**

RMF for Federal Agencies—4 day program (Fundamentals and In Depth)

- **Online Personal Classroom™ ▪ 21-24 AUG**

Information Security Continuous Monitoring—3 day program (In Depth class only)

- **Online Personal Classroom™ ▪ 25-27 JUL**

Certified Cloud Security Professional (CCSP)—5 day program

- **Online Personal Classroom™ ▪ 24-28 JUL**
- **National Capital Region ▪ 25-29 SEP**

eMASS eSSENTIALS—1 day program

- **Online Personal Classroom™ ▪ 26 JUL ▪ 30 AUG ▪ 27 SEP ▪ 25 OCT ▪ 15 NOV ▪ 13 DEC**

Registration for all classes is available at https://register.rmf.org

Payment arrangements include credit cards, SF182 forms, and Purchase Orders.