Risk Management Framework Today

Formerly DIACAP Dimensions

... and Tomorrow

May, 2016
Volume 6, Issue 2

In this issue:

Security Control Baseline "Tabletop Review"

By Lon J. Berman, CISSP

In the last issue of *RMF Today and Tomorrow*, we walked "step by step" through the process of creating a Security Control Baseline. step-by-step. Now let's take a look at some strategies for reviewing the Security Control Baseline and creating "action plans" for implementation.

The "Raw Materials"

An effective review starts with the right materials. You'll need two spreadsheets to work with:

- Security Controls
- Assessment Procedures (CCIs)

Using the Security Controls Explorer in the RMF Knowledge Service (https://rmfks.osd.mil), you can create these spreadsheets simply by entering your system categorization levels for Confidentiality, Integrity and Availability.

The Security Controls spreadsheet has a row for each control and control enhancement in the baseline. The Assessment Procedures spreadsheet shows the "breakdown" of each control (or control enhancement) into one or more assessment objectives. Note that each assessment objective is also identified by a Control Correlation Identifier (CCI).

These spreadsheets can also be used to record the results of the tabletop review. At a minimum, there should be columns for:

- Compliant, Non-compliant or NA
- Responsibility
- Implementation/justification
- Documentation Reference

Strategy for Review

The general strategy for the review is to systematically go through each of the controls in the baseline (using the related assessment procedures as additional supporting material) and make a determination of applicability, responsibility, compliance, and documentation.

For each control (and/or control enhancement) in the baseline:

1. Understand the intent

Read and understand the general intent of the control. Take note of any Organization-defined Values that may need to be filled in (see below).

2. Assess inheritance

If your system is hosted at a data center or equivalent, determine if the control can be inherited. Your hosting site should be able to provide a list of controls you can inherit—typically these would include physical, environmental and network controls.

3. Assess overall applicability and responsibility

Determine if the control applies to your system. Certain controls reference specific technologies (e.g., wireless access or public website access) that may not be a part of your system. If the control is deemed "Not Applicable", develop a short justification (typically a sentence or two).

If the control is deemed applicable, make a determination as to the individual or organization responsible for implementing/documenting it.

See *Tabletop Review*, Page 2

Risk Management Framework Today
... and Tomorrow

Enhance your RMF Training Experience with TrainPlus!™

By Annette Leonard

Picture this. You've just completed your RMF training. You spent four days in class learning and doing. So much information and guidance has come your way that at times you felt like you were drinking from a fire hose! Now, at last, you're sitting in the relative peace and quiet of your vehicle, or on an airplane, heading for home. And then it hits you—that question you should have asked during the class!

Or maybe it happens like this. You're back in the office working on your own system's RMF, using the skills you learned in your recent class. Everything is going swimmingly—until you hit an unforeseen snag, and you're thinking "Gosh, I sure wish my RMF instructor was here to see this—he/she would definitely have some helpful information for me."

TrainPlus! to the rescue!

TrainPlus! is a monthly teleconference conducted by one of BAI's RMF subject matter experts. This is your opportunity to raise that forgotten question or discuss that snag in your progress with RMF. It's also an opportunity to network and learn from others … and for others to learn from you!

Every student who attends a BAI RMF training program will receive an invitation to a TrainPlus! session a few weeks after the class. If you previously attended RMF training with BAI and might have missed your opportunity to attend TrainPlus!, please contact us at 1-800-RMF-1903 for an updated invitation. We look forward to your participation in a TrainPlus! session soon.

"… systematically go through each of the controls in the baseline and make a determination of applicability, responsibility, compliance and documentation."

***Tabletop Review* from Page 1**

4. Review each Assessment Procedure (CCI) comprising the control

4a. Read and understand the general intent of the CCI; take note of any organization-defined values that are provided by DoD (typically in the form of a sentence beginning with "DoD has defined…").

4b. Note any CCI that is considered "automatically compliant" by DoD.

4c. Determine applicability. In some cases, one or more CCIs may be NA even though the control as a whole is considered applicable.

4d. Is the capability reference by the CCI implemented within your system?

- If YES, write a short statement (a sentence or two) explaining how the CCI is implemented within your system.
- If NO, mark the CCI as "Non-compliant (not implemented)"; further action will be required to remediate or mitigate this finding.

4e. Is the capability referenced by the CCI documented in an existing Plan or SOP?

- If YES, make note of the relevant document name and paragraph/ section number (be as specific as possible).
- If NO, mark the CCI as "Non-compliant (needs documentation)"; further action will be required to identify the relevant document and revise appropriately.

Expect to spend considerable time on the tabletop review, but do not allow yourself to get bogged down on a particular control or CCI. If responsibility or compliance cannot be readily determined, make a note of this and move on.

Top Ten—RMF "Lessons Learned"

By Lon J. Berman, CISSP

I recently had the pleasure of consulting for a DoD program that successfully navigated the RMF process and received a full three year Authorization to Operate (ATO).

In lieu of … or in addition to … a victory party, the team decided it would be productive to conduct an After-Action Review.

This edition of the RMF Top Ten highlights some of their "lessons learned" in the area of Project and Resource Management.

10. Assign writers/owners for controls and CCIs as soon as categorization is complete and controls are identified.

9. Develop a tracking mechanism early to track progress of CCI completion.

8. Establish a common approach to addressing controls for the entire program – writing styles can vary widely.

7. Establish roles and responsibilities, and do NOT underestimate the time required to prepare documentation, process, and input into eMASS.

6. Establish weekly meetings to track progress and raise issues. Track action items to completion.

5. Encourage team members to receive training in the RMF process itself (in addition to training on the eMASS tool).

4. Establish roles and responsibilities, and do NOT underestimate the time required to prepare documentation, process, and input into eMASS.

3. Project Manager and ISSO must understand RMF and ATO process completely, stay abreast of progress, and meet with the System Owner regularly (recommend weekly) on status, risks, and mitigation strategies.

2. Assign a full-time ISSO and include in this role in program budgeting processes, if not already included.

1. Assign a Project Manager to track performance in terms of scope, cost, and schedule. Based on required documentation and updates, etc., build a master schedule and use it to track progress.

In future editions of RMF Today … and Tomorrow we'll take a look at some of their other "lessons learned." Here is a short preview:

- ◊ Recommend beginning categorization process 1 year prior to ATO expiration date.
- ◊ Once security control baseline has been established, conduct an initial "triage" and walk-through of controls to a) ensure intent of each control is clearly understood, and b) identify controls inherited from hosting enclave, controls that are N/A, etc.
- ◊ If resources are available, encourage pre-validation with team that will conduct the validation.
- ◊ Schedule independent validation about 4 months prior to ATO expiration.
- ◊ Get on the eMASS ASI (system outage) announcement list; do not work in eMASS during ASIs, even if the system appears to be online (observation is that data is lost if saved during an ASI).

Security Control Spotlight—Inheritance

By Kathryn M. Farrish, CISSP

"...inheritance ... eliminates the need for redundant validation of compliance..."

Security Control Inheritance is one of the most powerful tools available to facilitate the RMF process. Unfortunately, it is not always very well understood, and, as a result, is often misapplied.

CNSSI 4009 defines Security Control Inheritance as "a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides."

The classic example of inheritance involves a system that is hosted at a departmental or agency data center. Such a system will inherit numerous security controls from the data center, typically those involving physical security (door locks, guards), environmental security (fire protection, power, air conditioning) and network boundary defense (firewall, network intrusion detection). All of these controls are maintained by the data center and are included in the data center's authorization (accreditation) boundary.

The big benefit of inheritance is that it eliminates redundant validation of compliance—the compliance of the "providing system" (data center) automatically inures to the benefit of the "receiving system" (hosted customer system).

In order for a system owner to claim inheritance of one or more controls from another system, the following three conditions must be met:

1. The control must be implemented and maintained outside the boundary of the "receiving system"

2. The "providing system" must have an Authorization to Operate (ATO)

3. The "providing system" must have a contractual obligation to provide the specified controls; this is typically in the form of a Memorandum of Agreement (MOA) or Service Level Agreement (SLA)

Some frequent misunderstandings of these "rules of thumb" are:

◊ Attempts to claim inheritance of controls that are implemented inside the receiving system's boundary. For example, some data centers offer optional services such as patching and maintaining operating systems for their hosted customers. This would not be considered as inheritable since it is taking place within the receiving system's boundary.

◊ Attempts to claim inheritance of controls from hosting providers that do not have ATO (e.g., commercial collocation sites). Government-sponsored programs such as FedRAMP have been established to enable commercial providers to obtain formal ATO so their customers can inherit from them.

◊ Attempts to claim inheritance when there is no clear-cut contractual obligation on the part of the "providing system".

It is worth noting that inheritance can be a "two edged sword"—in the event the "providing system" is non-compliant on any of its inheritable controls, these risks are also carried by each "receiving system".

System owners who utilize the eMASS tool can leverage functionality that allows them to identify and request inheritance from their "providing system". Once such a request is accepted, the "receiving system's" eMASS record is automatically linked to the "providing system".

Contact Us!

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

Phone: 1-800-RMF-1903
Fax: 540-808-1051
Email: rmf@rmf.org

Training for Today … and Tomorrow

BAI currently offers <u>three</u> training programs:

- **RMF for DoD IT** – recommended for DoD employees and contractors that require detailed RMF knowledge and skill training; covers the new RMF life cycle and NIST security controls, the CNSS enhancements, *and* the 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 employees and contractors (non-DoD); covers RMF life cycle and NIST security controls. 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.

Regularly-scheduled classes through September, 2016 are as follows:

RMF for DoD IT (Fundamentals and In Depth)

- **23-26 MAY 2016 (Online Personal Classroom™)**
- **13-16 JUN 2016 (Colorado Springs)**
- **20-23 JUN 2016 (Online Personal Classroom™)**
- **11-14 JUL 2016 (National Capital Region)**
- **18-21 JUL 2016 (Online Personal Classroom™)**
- **8-11 AUG 2016 (Huntsville)**
- **15-18 AUG 2016 (Online Personal Classroom™)**
- **12-15 SEP 2016 (Colorado Springs)**
- **19-22 SEP 2016 (Online Personal Classroom™)**

RMF for Federal Agencies (Fundamentals and In Depth)

- **6-9 JUN 2016 (Online Personal Classroom™)**

Information Security Continuous Monitoring

- **PLEASE CALL**

For the most up-to-date training schedule, pricing information, and any newly-added class dates or locations, please visit http://register.rmf.org.

Online registration and payment is available at http://register.rmf.org. Payment arrangements include credit cards, SF182 forms, or purchase orders.

Classroom training. We offer regularly-scheduled classroom training at our training centers in Colorado Springs, Huntsville, National Capital Region* (Washington, DC area) and Virginia Beach. **Note our new National Capital Region location in the Pentagon/Crystal City area.*

Online Personal Classroom™ training. This method enables you to actively participate in our regularly-scheduled instructor-led classes from the comfort of your home or office.

On-site training. Our instructors are available to present one or more of our training programs at *your* site. All you need is a group of students and a suitable classroom or conference room. Cost is dependent upon class size, so please contact us at 1-800-RMF-1903 (763-1903) to request an on-site training quotation.
Note: we can also provide Online Personal Classroom™ training to a "private" group of students from *your* organization.