Risk Management Framework Today

Formerly DIACAP Dimensions

... And Tomorrow

October, 2014
Volume 4, Issue 4

In this issue:

RMF Transition—What is the Real Timeline?

By Lon J. Berman, CISSP

Now that RMF is official DoD policy, every DoD system owner needs to begin planning their "transition" from DIACAP. In order to plan and execute the transition, system owners need the answers to three basic questions:

- What does the transition process entail?
- When do I need to begin the process?
- How long do I have to complete the process?

DoDI 8510.01 provides straightforward answers to question 1. The transition process includes:

- System categorization in accordance with CNSSI 1253
- Selection of a security control baseline from NIST SP 800-53; selection to be made in accordance with CNSSI 1253
- Tailoring and/or enhancement of the security control baseline in accordance with DoDI 8510.01 guidance
- Documentation of the security control baseline in a System Security Plan
- Approval of the baseline by the Authorizing Official or Representative
- Implementation of the security controls and enhancement in the approved baseline
- Independent assessment of compliance in accordance with the DoD component's process, using DoD assessment procedures based on NIST SP 800-53a
- Documentation of assessment results in a Security Assessment Report
- Development of a Plan of Action and Milestones (POA&M) in response to assessment findings
- Assessment of risk based on assessment results and POA&M
- Risk-based decision by the Authorizing Official (ATO)

When to start? DoDI 8510.01 states that DoD system owners can begin planning and executing their transition immediately.

How long to complete? Here's where things get messy. DoDI 8510.01 requires all systems to be completely transitioned by September, 2017. Various transition strategies are provided based on the system's current status in the DIACAP life cycle, but the bottom line is all systems were to begin transitioning at some level (and no new DIACAP activity to be started) by September, 2014. So, more than likely, you're already behind schedule!

Thankfully, DoD has already recognized that the transition timeline in DoDI 8510.01 was too ambitious. A revised transition timeline was released in the form of a memorandum dated October, 2014. It provides for a modest extension of the timeline for all of DoD to be fully transitioned (from September 2017 to mid -2018). The biggest change is that it allows system owners to actually go through one more cycle of accreditation under DIACAP before being forced to transition. The catch is that the longer you wait to initiate a new DIACAP (or reaccreditation), the shorter the maximum ATO duration can be.

See *Transition Time Line, Page 2*

Significant Update to NIST SP 800-53A

By Kathryn M. Farrish, CISSP

At long last, NIST has finally released a *draft* copy of the updated version of SP 800-53A, entitled *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. This is an important document in the RMF "document library" because it contains the "how to" for assessing compliance with the security controls in SP 800-53.

Several things are significant about this new edition. First of all, it is labeled as Rev4, even though the version it is about to replace is Rev 1. What's up with that? What happened to Rev 2 and Rev 3? Weird as it appears at first glance, there is actually a valid reason for "jumping" to Rev 4. This new version of SP 800-53A is written to correspond to the current version of SP 800-53, which also happens to be Rev 4! Presumably, subsequent revisions of the two documents will continue to bear identical Rev designations.

A small change on the cover page indicates the document is authored by NIST, along with the Joint Task Force Transformation Initiative (JTFTI). The fact that JTFTI has taken "ownership" of the document indicates it is intended for use across all "sectors" of the federal executive branch, to wit: DoD, federal "civil" departments/agencies, and the intelligence community. This document joins other NIST SP's such as 800-37, 800-39, and 800-53 in forming a "unified framework for information security."

Most significantly, the format and nomenclature of the assessment methods themselves has been altered. Instead of broadly-stated assessment objectives, the new document presents assessment objectives that are broken down into small, granular parts and sub-parts, each of which is uniquely numbered, as in the example below:

AC-1	ACCESS CONTROL POLICY AND PROCEDURES		
	ASSESSMENT OBJECTIVE: *Determine if the organization:*		
AC-1(a)(1)	AC-1(a)(1)[a]	*develops and documents an access control policy that addresses:*	
		AC-1(a)(1)[a][1]	*purpose;*
		AC-1(a)(1)[a][2]	*scope;*
		AC-1(a)(1)[a][3]	*roles;*
		AC-1(a)(1)[a][4]	*responsibilities;*
		AC-1(a)(1)[a][5]	*management commitment;*
		AC-1(a)(1)[a][6]	*coordination among organizational entities;*
		AC-1(a)(1)[a][7]	*compliance;*
	AC-1(a)(1)[b]	*defines personnel or roles to whom the access control policy are to be disseminated;*	
	AC-1(a)(1)[c]	*disseminates the access control policy to organization-defined personnel or roles;*	

Publication of the "final" version of NIST SP 800-53A Rev 4 is expected on or about 1 November 2014.

> *"...assessment objectives are broken down into small, granular parts and sub-parts, each of which is uniquely numbered..."*

***Transition Time Line*, from Page 1**

- Systems receiving DIACAP accreditation (or re-accreditation) between now and mid-2015 (calendar year) can receive a maximum of 2 ½ years ATO
- Systems receiving DIACAP accreditation between mid-2015 and early 2016 can receive a maximum 2 year ATO
- Systems receiving DIACAP accreditation beyond early 2016 can receive a maximum 18 months ATO

As you can see, there are clear incentives for transitioning sooner rather than later.

The revised timeline memo is posted on the RMF Knowledge Service (https://rmfks.osd.mil).

Top Ten—Sources of RMF Policy and Guidance

By Annette Leonard

RMF-related policies and guidance come from a plethora of sources within the seemingly-convoluted federal landscape. We believe a good understanding of these sources will be helpful as you move forward in your RMF implementation. Here, then is our "Top Ten" list of RMF policy and guidance providers.

10. US Congress. The Federal Information Security Management Act, or FISMA, was passed by Congress in 2002. FISMA mandates each federal department and agency to establish and maintain an information security program that includes things such as: periodic assessments of risk and annual reporting of security status. Much of the government's information security activity can be directly or indirectly traced to the provisions of FISMA.

9. Office of Management and Budget (OMB). OMB, an arm of the White House, is specifically tasked to be the implementer/ enforcer of FISMA and the developer of supporting mandates, such as OMB A-130. OMB A-130 calls for explicit information security approval of systems prior to implementation and is the basis of the traditional "Certification and Accreditation" (C&A) programs that exist throughout the federal landscape.

8. National Institute of Standards and Technology (NIST) - Federal Information Processing Standard (FIPS) Publications. NIST is specifically tasked by FISMA to be the developer of implementation guidance. Certain NIST publications are considered federal mandates. Two in particular, FIPS 199 and FIPS 200, are connected to RMF.

7. National Institute of Standards and Technology (NIST) - Special Publications (SP). These NIST publications are considered as non-mandatory guidance, but are available for adoption by the various departments and agencies as part of their (mandatory) security policies. Key RMF-related publications include NIST SP 800-37 (RMF life cycle), NIST SP 800-53 ("catalog" of security controls), and NIST SP 800-53A (assessment methods).

6. Joint Task Force Transformation Initiative (JTFTI). This group includes representatives from DoD, civil departments/agencies, and the intelligence community, and is chartered to develop a "unified information security framework" (i.e., RMF). JTFTI is co-author of the key RMF-related publications from NIST.

5. Committee on National Security Systems (CNSS). This organization is chartered specifically to address the unique information security requirements of systems designated as National Security Systems (NSS). These are systems that process classified or intelligence information, and/or support military operations. The key RMF-related publication is CNSS Instruction (CNSSI) 1253, which lays out the process for categorization and security control selection for NSS.

4. DoD Chief Information Officer (CIO). In March 2014, the DoD CIO published the two key policy documents that kicked off DoD's transition to RMF. DoD Instruction (DoDI) 8500.01, entitled "Cybersecurity" presents the overarching policy, while DoDI 8510.01, entitled "RMF for DoD IT" lays out DoD's adoption and adaptation of RMF.

3. DoD Senior Information Security Officer (SISO). The DoD SISO is responsible for overseeing the RMF Technical Advisory Group (TAG), which is responsible for maintaining the RMF Knowledge Service (RMF KS) website (the "authoritative source" for DoD RMF information).

2. Defense Information Systems Agency (DISA). DISA is specifically tasked with developing technical guidance and validation procedures for DoD information systems. In this capacity, DISA publishes a plethora of Security Technical Implementation Guides (STIGs), along with automated tools that provide assistance in assessing STIG compliance.

1. Your DoD Component. While RMF is a highly standardized process, there are still important elements that are controlled at the component level. For example, each component implements its own process for vetting and appointing Authorizing Officials (AO, formerly known as DAA), and for conducting independent assessment (aka. Validation) of information systems.

Security Control Spotlight—By the Numbers

By Lon J. Berman, CISSP

In this issue's "Spotlight", we're not going to focus on any specific controls or families, but rather on a comparison of RMF controls and DIACAP controls.

The majority of DoD information systems are currently categorized under DIACAP as "MAC II Sensitive" or "MAC III Sensitive". These categorizations equate roughly to "Confidentiality-Moderate, Integrity-Moderate, Availability-Moderate" or "Confidentiality-Moderate, Integrity-Moderate, Availability-Low".

Per DoDI 8500.2, a total of 100 IA controls are applicable to a MAC III Sensitive system, while 106 are applicable to a MAC II Sensitive system. Consulting the DIACAP Knowledge Service, we find a total of 148 Assessment Procedures for a MAC II Sensitive system and 161 for a MAC II Sensitive system.

If we go through the same process under RMF, using CNSSI 1253 to do the control selection and NIST SP 800-53 as the "catalog" of controls, we find the total number of controls applicable to the "Moderate-Moderate-Low" baseline is approximately 160. Approximately 170 are applicable to the "Moderate-Moderate-Moderate" baseline. However, this does not take into account the control enhancement, which, for all intents and purposes, are like controls in themselves. The total number of applicable controls *and* enhancements or the "Moderate-Moderate-Low" baseline is about 380, and about 400 for the "Moderate-Moderate-Moderate" baseline.

Are you frightened yet?

Now, let's go one step further and count the number of assessment procedures (NIST SP 800-53A, Rev 4) required to cover all these controls and enhancements. Let's just say the number exceeds 1,500 for both the "Moderate-Moderate-Low" and "Moderate-Moderate-Moderate" baselines.

Is there *any* good news in all of this? Well, maybe just a little bit. It's not quite fair to equate RMF assessment procedures with DIACAP assessment procedures. The RMF assessment items are much more granular, so, even though there are 10 times as many assessment procedures, there's probably *not* 10 times the effort required to do an RMF assessment as there is for a DIACAP validation of the same system. Also, because the RMF assessment procedures are so granular, there is much more opportunity to use automated procedures for at least some fraction of them.

All that said, however, it is clear the level of effort associated with RMF promises to be significantly greater than it was for DIACAP. Just how much greater remains to be seen as DoD systems begin transitioning to RMF.

Everyone from top-level management down to the cybersecurity "boots on the ground" need to be mindful of the "adventure" that awaits us.

"...the level of effort associated with RMF promises to be significantly greater than it was for DIACAP."

Training for Today … and Tomorrow

BAI currently offers three training programs:

- **RMF for DoD IT** – recommended for DoD employees and contractors that require detailed RMF knowledge and skill training; covers the new RMF 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)** – recommended for all; prior knowledge of RMF recommended. This is a three day "In Depth" program.

Regularly-scheduled classes for the remainder of 2014 and early 2015 are as follows:

RMF for DoD IT (Fundamentals and In Depth)

- **17-20 NOV 2014 (Online Personal Classroom™)**
- **8-11 DEC 2014 (National Capital Region and Online Personal Classroom™)**
- **26-29 JAN 2015 (Online Personal Classroom™)**
- **23-26 FEB 2015 (Colorado Springs and Online Personal Classroom™)**
- **16-19 MAR 2015 (Huntsville and Online Personal Classroom™)**
- **13-16 APR 2015 (National Capital Region and Online Personal Classroom™)**

RMF for Federal Agencies (Fundamentals and In Depth)

- **2-5 FEB 2015 (Online Personal Classroom™)**

Information Security Continuous Monitoring

- **2-4 DEC 2014 (Online Personal Classroom™)**
- **10-12 MAR 2015 (Online Personal Classroom™)**

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

On-line 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, and Washington, DC/National Capital Region.

Online Personal Classroom™ training. This method enables you to actively participate in an instructor-led class 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 (normally at least 8-10) and a suitable classroom facility. Cost per student is dependent upon class size, so please contact us at 1-800-RMF-1903 (763-1903) to request an on-site training quotation.

Contact Us!

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

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