Risk Management Framework Today

Formerly DIACAP Dimensions

… And Tomorrow

April, 2014
Volume 4, Issue 2

In this issue:

DoD (Finally) Begins Transition to RMF	1
Continuous Monitoring—It's Not (Just) About the Tools	2
Top Ten—What's "new" in RMF for DoD IT?	3
Security Control Spotlight—Overlays	4
Training for Today… and Tomorrow	5

DoD (Finally) Begins Transition to RMF

By Lon J. Berman, CISSP

The wait is over! RIP DIACAP!!

At long last, DoD has announced the start of transition from the legacy DIACAP Certification and Accreditation (C&A) Program to the Risk Management Framework (RMF). This transition is part of a broader effort to bring *all* Executive Branch departments and agencies … including DoD, the intelligence community and all "civil" departments/ agencies … into a "unified information security framework."

Two key documents were signed and released by DoD Chief Information Officer Teresa Takai in March, 2014:

- *New* DoD Instruction (DoDI) 8500.01, replacing DoD Directive (DoDD) 8500.1. The title has been changed from *Information Assurance* to *Cybersecurity*.

- *Revised* DoD Instruction (DoDI) 8510.01; title changed from *DIACAP* to *Risk Management Framework (RMF) for DoD Information Technology (IT)*.

So far, so good ... but wait a minute! What about DoDI 8500.2? For those new to the process, that's the document that contains all the "IA Controls" (security requirements) with which DoD systems are required to comply. Wouldn't that also need to be revised to fit into the new process? Well, the short answer is there will be no revised DoDI 8500.2 — DoD has decided to simply *rescind* it.

So how exactly is DoD going to implement a brand new information security framework without specifying requirements? It's easy—they've decided not to try and reinvent the wheel, but rather to leverage the extensive work of NIST, the National Institute of Standards and Technology, and CNSS, the Committee on National Security Systems.

A few of the key NIST and CNSS publications that are being "adopted" by DoD are:

- NIST Special Publication (SP) 800-53, Revision 4. This document contains an extensive "catalog" of Security Controls (requirements).

- NIST SP 800-37, Revision 1. This is the definitive Risk Management Framework document, describing the roles and responsibilities, life cycle process, etc.

- CNSS Instruction (CNSSI) 1253. This publication describes the methodology that DoD will use for categorizing systems and selecting security controls.

- NIST SP 800-53A Revision 2 . This document contains recommended assessment objectives and procedures for each of the Security Controls.

The change from DIACAP to RMF will eventually affect every DoD information system, including "DoD owned and operated" systems as well as processes and systems operated by industry partners on behalf of DoD. A phased approach is being adopted, such that every system will be *fully* transitioned in time for its *next* re-authorization (reaccreditation) date.

See *DoD Begins Transition, Page 2*

Continuous Monitoring—It's Not (Just) About The Tools

By Annette Leonard

Continuous Monitoring has long been recognized as a critical element in maintaining a strong security posture for any IT system. In spite of this, the risk management processes used in most federal agencies have traditionally been centered around mountains of paperwork, along with "point-in-time" assessments and approvals. With the ascension of RMF, continuous monitoring is finally getting the "emphasis" it deserves.

"With the ascension of RMF, continuous monitoring is finally getting the emphasis it deserves."

NIST Security Control CA-7 lays down the fundamental requirement for all information systems to be covered by a continuous monitoring program:

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

- A configuration management process for the information system and its constituent components
- A determination of the security impact of changes to the information system and its environment
- Ongoing security control assessments in accordance with the organizational continuous monitoring strategy
- Reporting the security state of the information system to appropriate organizational officials [*at an organization-defined frequency*]"

While automated tools are *necessary* to the organization's continuous monitoring program, they are not *sufficient*. Automation will only provide meaningful, actionable results when it is employed in the context of a comprehensive strategy and well thought out implementation program. NIST Special Publication 800-137 is an excellent resource for further information.

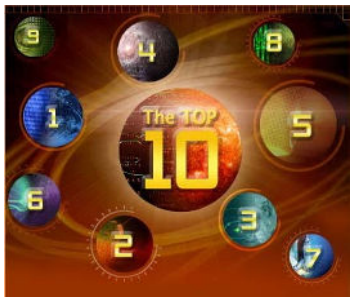
BAI provides an *Information Security Continuous Monitoring* training program that thoroughly covers the theory and practice of continuous monitoring. This training program is offered by on-site and on-line (instructor led) and is available for registration now! More information is available on the last page of this newsletter.

***DoD Begins Transition*, from Page 1**

Now that the official publications are on the ground, there is plenty of work still to be done by DoD to support the transition. The Knowledge Service website is in the process of being updated with RMF information, including the all-important assessment procedures for evaluating compliance with each of the controls. Also on the horizon is a major overhaul of the eMass tool to support the RMF workflow, NIST security control set, etc.

BAI is pleased to announce our newly-revised training program, including "*RMF for DoD IT—Fundamentals*" and "*RMF for DoD IT—In Depth*" courses. The RMF for DoD IT training program is offered both on-site and on-line (instructor led) and is open for registration *now*!

Please see the last page of this newsletter for schedule, cost, and other information about this exciting new training opportunity!



Top Ten—What's "new" in RMF for DoD IT?

By Lon J. Berman, CISSP

Now that DoD has "officially" begun its adoption of RMF, let's take a look at some of the things that are "new"!

10. **Cybersecurity.** The word "Cybersecurity" has been part of the government IT security discussion for several years, going back to a Presidential Directive in 2008. DoD has now adopted the term Cybersecurity in place of Information Assurance.

9. **A&A.** With the adoption of RMF, the term "Assessment" will replace "Certification", and "Authorization" will replace "Accreditation". Certification and Accreditation (C&A), which has been a cornerstone of DoD IT security for 20 years or more, will henceforth be known as Assessment and Authorization (A&A).

8. **Types of DoD IT.** DoD now views the overall IT landscape as a collection of Major Applications, Enclaves, Platform IT (PIT), IT Services, and Products. PIT is further subdivided into PIT Systems and PIT. Some of these require assessment and authorization, while others require only assessment.

7. **Categorization.** DoD will now categorize systems as High, Moderate or Low for each of the three security objectives (Confidentiality, Integrity, Availability). This is in accordance with CNSS Instruction 1253, and replaces the Mission Assurance Category (MAC) and Confidentiality Level (CL).

6. **Authorizing Official.** Senior DoD officials responsible for accepting risk and authorizing systems for operation will henceforth be known as Authorizing Official (AO) rather than Designated Approving Authority (DAA).

5. **Old titles make a comeback.** IA Managers and IA Officers will once again be referred to as Information System Security Managers/Officers (ISSM/ISSO). Many of us have been in the field long enough to remember when those were the titles of choice.

4. **Security Plan.** A security plan will be required of every DoD IT or PIT System, including, at a minimum, an overview of the security requirements for the system and the security controls in place or planned to meet those requirements.

3. **Security Control Assessor (SCA).** This is the name now given to the individual or organization responsible for independently testing the security controls of DoD IT systems

2. **Continuous Monitoring.** RMF for DoD IT places greater emphasis on the process for ongoing monitoring of security posture. System Owners will be required to develop and receive approval for monitoring plans early in the life cycle. In some cases, systems with robust continuous monitoring programs will be eligible for "ongoing authorization" in lieu of periodic re-authorization.

1. THE NAME. Risk Management Framework (RMF) for DoD Information Technology (IT) ... "RMF for DoD IT" … is the name DoD has given to this new process for managing life cycle risk, replacing DoD Information Assurance Certification and Accreditation Process (DIACAP). This is significant because there has been so much speculation and rumor for so long, and several other names, like *DIARMF* and *Cybersecurity RMF*, have been tossed about. That's all in the past now … "RMF for DoD IT" it is! It doesn't exactly roll off the tongue like DIACAP (or its predecessor DITSCAP) did, but we'll all get used to it. More than likely it will come to be called just "RMF" for short.

Security Control Spotlight—Overlays

By Kathryn M. Farrish, CISSP

In a previous Security Control Spotlight, we introduced the concept of *organization-defined parameters* that departments and agencies can use to "fill in the blanks" and make the NIST SP 800-53 controls truly "their own". In this edition, we're going to take a look at Security Control Overlays, an even more powerful concept that takes customization to a whole new level.

So what in the world is an Overlay? If you're thinking about those hours of "killin' time" in the Atlanta airport, you're not even close—that would be a Layover. That said, however, next time you find yourself whiling away a perfectly good morning or afternoon at good ole ATL, you might consider bringing along a printed copy of one of those new DoD Instructions, or one of the NIST Special Pubs. Better yet, download the whole bunch of 'em to your Kindle or tablet computer and be ready for good reading on the go.

"Overlays facilitate uniformity of security baselines for specific technologies or communities of interest."

OK, back to the concept of a Security Control Overlay. NIST SP 800-53 Revision 4 defines an overlay as "a fully specified set of security controls, control enhancements, and supplemental guidance derived from the application of tailoring guidance to a security control baseline". Overlays facilitate government-wide uniformity of security baselines for specific technologies or communities of interest.

Overlays can complement the initial security control baselines in numerous ways:

1. Entire security controls can be added or eliminated
2. Security control applicability and interpretation can be provided for specific technologies, environments, types of missions, operating modes, industry sectors or regulatory environments
3. Community-wide organization-defined parameters can be provided
4. Additional supplemental guidance can be provided

NIST SP 800-53 Appendix I provides a template for overlay development for non-National Security Systems, while CNSSI 1253 Appendix K provides a similar template for use in the National Security arena. The NIST template provides for eight sections in the overlay:

- Identification
- Overlay Characteristics
- Applicability
- Overlay Summary
- Detailed Overlay Control Specifications
- Tailoring Considerations
- Definitions
- Additional Information or Instructions

Development of overlays requires close cooperation between information security professionals and subject-matter experts in the particular community of interest.

As the implementation of RMF expands from its Federal Civil Agency "core" into DoD, the intelligence community, and beyond (i.e., state and local government, private industry), we can expect to see numerous overlays developed to provide customized, and customizable, baselines for a variety of applications.

It's not "one size fits all", but rather "many sizes to fit many".

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

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 second quarter of calendar year 2014 are as follows:

Date	Training Program	Location
14-17 APR	RMF for DoD IT Fundamentals and In Depth	Personal Classroom
6-8 MAY	Information Security Continuous Monitoring (ISCM)	Washington, DC and Personal Classroom
19-22 MAY	RMF for DoD IT Fundamentals and In Depth	Colorado Springs, CO and Personal Classroom
2-5 JUN	RMF for Federal Agencies Fundamentals and In Depth	Washington, DC and Personal Classroom
23-26 JUN	RMF for DoD IT Fundamentals and In Depth	Huntsville, AL and 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. Please visit **www.rmf.org** for the latest training schedule, including any new dates or locations.

Classroom training. We offer regularly-scheduled classroom training at our training centers in Colorado Springs, Huntsville, and Washington, DC/National Capital Region.

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.