Risk Management Framework Today

Formerly DIACAP Dimensions

... And Tomorrow

Fedruary, 2013
Volume 3, Issue 1

Find us on Facebook

LinkedIn

In this issue:

"Personal Classroom" Brings RMF Training to You

By Annette H. Leonard

Budget crises have become a way of life in government, and there is no sign of relief anytime soon. More than ever, Federal and DoD programs need to find ways to perform their missions efficiently in the face of limited resources. It is well known that a better trained workforce is able to perform more efficiently, but, sadly, the training and travel dollars needed to make that happen are hard to come by.

BAI to the rescue! Our Personal Classroom™ can help your organization make efficient use of training funds without the need for travel. Personal Classroom training combines the best features of web-based learning and traditional instructor-led classes. With just a personal computer and telephone, students can fully participate in our live, instructor-led training experience.

Some of the key benefits of Personal Classroom training are:

Significantly Reduced Cost—by completely eliminating travel expenses, Personal Classroom training enables many organizations to realize dramatic cost savings, frequently on the order of 50%.

Increased Efficiency—Personal Classroom training improves organizational efficiency by minimizing staff downtime such as travel days. No longer does a four-day training program entail a full week out of the office.

Improved Morale—Personal Classroom training eliminates disruptions to personal and family life caused by travel—no more leaving home on Sunday to make a Monday morning training class.

Increased Flexibility—Personal Classroom training enables more flexible scheduling of your staff for training.

Personal Classroom training is now available for both of our Risk Management Framework (RMF) training programs:

DIACAP RMF (recommended for DoD employees and contractors)—*includes DIACAP (legacy DoD process) and transition to RMF (new DoD process)*.

FISMA RMF—recommended for employees and contractors of Federal "civil" departments and agencies—*includes RMF only*.

Personal Classroom training for these courses is available in two different delivery formats:

Full-day sessions. Personal Classroom attendees can remotely join in full-day sessions at most of our regularly scheduled training programs in Huntsville, Colorado Springs, and Washington, DC/ National Capital Region.

Half-day sessions. "Modular" classes, broken down into half-day sessions, are available for Personal Classroom attendees only.

Registration is now open for Personal Classroom training at http://register.rmf.org.

For additional information, please call us at 540-808-1050, or e-mail rmf@rmf.org.

RMF in DoD—When Will the Other Shoe Drop?

By Robert E. Lee, Jr., CISSP, CAP

It is a *fact* that DoD is committed to adoption of the Risk Management Framework (RMF) as a successor to the DIACAP Certification and Accreditation (C&A) process. Over the past several years, DoD has played a leading role in the Joint Task Force Transformation Initiative Interagency Working Group. The Joint Task Force is the developer of the RMF concept and the key RMF-related publications, e.g., NIST Special Publications 800-37 and 800-53. So there is no question RMF will soon be the "law of the land" within DoD programs.

The question everyone is asking is "how soon?" While a definitive, precise answer is perhaps known only to a few trusted insiders at DoD, the currently-available evidence points to a more general answer of "soon enough that everyone needs to start planning *now*."

Here are a few "frequently Asked Questions" about the DIACAP-to-RMF transition:

Which DoD publications are being updated as part of the transition?
DoD Directive (DoDD) 8500.01, currently entitled "Information Assurance, is being revised and re-issued under the new title of "Cybersecurity". DoD Instruction (DoDI) 8500.02 (currently "Information Assurance Implementation") will be re-issued as "Cybersecurity Implementation". *Do you see a pattern here? It appears DoD has embraced the term "cybersecurity" rather than the more traditional "Information Security" or "Information Assurance".* Sure enough, DoDI 8510.01, the old DIACAP instruction, is expected be called "Cybersecurity Risk Management Framework for DoD IT."

So the DoD will be officially using the name "Cybersecurity RMF?"
Currently that appears to be the case, although it is still not a certainty. What is most likely is that "RMF" will be the vernacular, regardless of the "official" name adopted by DoD.

"...there is no question RMF will soon be he 'law of the land' within DoD programs."

When can we expect these publications to be released?
Our sources tell us these publications are in the final stages of "formal coordination", with publication expected in the first and second quarters of calendar year 2013.

Which other documents will be required to support these publications?
The existing DoDI 8500.2 includes the full set of IA controls for DoD systems. This will no longer be the case in the revised edition. Rather, it will reference National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, along with Committee on National Security Systems Instruction (CNSSI) 1253, as the authoritative sources for the security control set. It should be noted a revised edition of NIST SP 800-53 has been released in "Final Draft" form and is open for comments prior to official publication in April, 2013.

What are some ways DoD programs can plan and be ready for the start of the transition?
Read the publications of the Joint task Force, NISP SP 800-37 and 800-53, along with CNSSI 1253. These documents will give you insight into the RMF roles and responsibilities, life cycle process and documentation. Most importantly, you will learn about the NIST security controls (requirements) that are the very heart and soul of RMF. While it is true DoD may introduce a minor change here and there, the basic principles and practices of RMF implementation are already well documented in these publications. Better yet, consider attending one of our DIACAP RMF training programs. This course will teach you what you need to know about RMF, as well as providing practical guidance on making an effective transition from DIACAP.

DON'T PANIC — PREPARE!

Top Ten—Terminology Changes

By Lon J. Berman, CISSP

The Joint Task Force Transformation Initiative is responsible for creating an information security framework "for the entire federal government." This mission entails getting all departments and agencies, whether DoD, Federal, or Intelligence, onto the "same page" when it comes to security of their information and the systems that process it.

An unenviable task, to say the least … but well worth the effort for the obvious benefits to the cybersecurity mission, not to mention the side benefit to all of us as citizens and taxpayers.

What better place to start than with the terminology itself? Here then, are the top ten terminology changes (or new terms) we will all be embracing as part of the transition to RMF.

10. **Control Deficiency Level** (I, II, III) replaces Severity Category (I, II, III) as a metric for security weaknesses uncovered in formal reviews or through continuous monitoring.

9. **Security Control Assessor** replaces Certification Agent or Agent of the Certifying Authority as the name of the individual/organization independently reviewing security control compliance of a system.

8. **Risk Executive (Function)** [NEW] is the name of the individual/organization responsible for establishing uniform standards for risk tolerance across an organization.

7. **Authorization Boundary** replaces Accreditation Boundary

6. **Information System Owner** replaces Program Manager/System Manager.

5. **Common Control Provider [NEW]** is the individual/organization responsible for implementing controls that benefit (are inherited by) one or more connected systems.

4. **Security Control Assessment*** replaces Certification.

3. **Security Authorization*** replaces Accreditation.

2. **Authorizing Official (AO)** replaces Designated Accrediting Authority (DAA).

1. **Cybersecurity** replaces Information Assurance.

If you're still hungry for more terminology, you can always download CNSSI 4009 (http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf), the government's official glossary of information security / information assurance / cybersecurity terms. In this document you'll find old terminology, new terminology, and everything in between … plus a dictionary of acronyms specific to our industry. It has been suggested that if there were a bar catering to information security professionals, a copy of CNSSI 4009 would be kept handy to help settle bar bets!

* Alas, adoption of this new terminology means the end of the road for Certification and Accreditation (C&A). It's been a good run of 25+ years, but, still we're going to miss our old friend C&A. Somehow Assessment and Authorization (A&A) just doesn't have quite the same ring to it. At least not yet!

Security Control Spotlight—Documentation

By Betsy K. Taylor, CAP

In this issue, we are going to begin a departure from our usual focus on a single control or control family to talk about the types of documentation most often cited as evidence of compliance with assigned security controls. As they prepare for independent assessment or validation, many organizations scramble to collect relevant documentation or even to draft new documentation to address perceived gaps. Perhaps this short tutorial will help bring some order to this often chaotic process.

Let's start by defining three types of documentation:

Policy—policies define what an organization does. For example, there may be a backup policy that states the organization maintains backup copies of data in order to protect against data loss. Policies should be simple and high-level, and should not dictate methodology or supporting detail on implementation. In most organizations, policy documents carry formal signature of a senior executive and are subject to strict configuration and change control.

Procedure—procedures, sometimes called standard operating procedures or SOPs, define how the organization carries out its policies. For example, a backup SOP might explain how backup schedules are determined, where backup tapes are stored, etc. While changes to SOPs should still be controlled, it should entail a simpler and more agile process than the one for policies. SOPs are typically "owned" by the group directly responsible for carrying out the process and do not normally require executive-level signature.

Assurance—assurance documentation includes a wide variety of evidence that the organization is following its procedures. Copies of backup schedules and logs of successfully-completed backups might be used to show the backup SOP is in use. Other examples of assurance documentation are network diagrams, hardware and software inventories, audit logs, training records, access lists, etc.

Ideally, most if not all of this documentation should be developed and maintained as part of normal system life cycle activity. RMF should not be the sole reason for developing good policies, procedures and assurance documents. One of the roles of RMF activity is to uncover documentation gaps so that they can be corrected and integrated into normal operations.

To summarize, policy says "this is what we do", procedures (SOPs) say "this is how we do it", and assurance documentation says "see, we're actually doing it!"

Next time we'll look at how these three types of documentation tie to control families and individual controls.

"RMF should not be the sole reason for developing and maintaining good policies, procedures and assurance documentation."

Contact Us!

RMF Today … and Tomorrow is a publication of BAI Information Security Consultants, 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 from DIACAP to RMF. 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 classes through mid-May, 2013, are as follows:

DIACAP RMF Fundamentals (One-day)	DIACAP RMF In-Depth (Three-day)
4 Feb (H)	5-7 Feb (H)
11 Feb (NCR)	12-14 Feb (NCR)
25 Feb (CS)*	26-28 Feb (CS)*
18 Mar (NCR)*	19-21 Mar (NCR)*
25-26 Mar**	27 Mar-5 Apr**
8 Apr (H)*	9-11 Apr (H)*
22 Apr (CS)*	23-25 Apr (CS)*
6 May (NCR)*	7-9 May (NCR)*

Classes marked * are also available for attendance via Personal Classroom training.

Classes marked ** are "modular" classes (divided into half-day sessions) for Personal Classroom (online) students only.

FISMA RMF Fundamentals (One-Day)	FISMA RMF In-Depth (Three-Day)
11 Mar (DC)*	12-14 Mar (DC)*
29 Apr (DC)*	30 Apr-2 May (DC)*

Information Security Continuous Monitoring (ISCM) (Three-day)
19-21 Feb (DC)
5-7 Mar (H)
26-28 Mar (CS)
14-16 May (DC)

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

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.

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. Please contact us to request an on-site training quotation.

Personal Classroom™. This method enables you to actively participate in an instructor-led class from the comfort of your home or office. Classes marked * are available for online attendance via Personal Classroom. Those marked ** are "modular" classes (divided into half-day sessions) available by Personal Classroom only.