Risk Management Framework Today

Formerly DIACAP Dimensions

… And Tomorrow

February, 2014
Volume 4, Issue 1

Find us on Facebook

LinkedIn

In this issue:

DoD Transition to RMF Imminent—Will You Be Ready?

By Lon J. Berman, CISSP

For quite some time, it's been well known that DoD would be making a 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."

So why the inordinate delay in getting things rolling at DoD? There are probably numerous reasons that have more to do with politics than information security and are known only to insiders at the office of the DoD CIO. Beyond that, however, it is safe to say that one of the factors is DoD's desire to ensure that all their ducks are in a row before "pulling the trigger" on the transition. That includes ensuring that there is an internally consistent set of supporting documents available, and that isn't quite true just yet.

In order to explain this, a little bit of background is in order. DoD's implementation of RMF will be based on publications of the National Institute of Standards and Technology (NIST) and the Committee on National Security Systems (CNSS). One of the key documents supporting RMF is NIST Special Publication (SP) 800-53, which contains the "catalog" of security controls. The most recent edition of this document is Revision 4. CNSS Instruction (CNSSI) 1253, which will likewise be one of the cornerstones of DoD RMF, is heavily dependent on NIST Special Publication 800-53, Revision 3. In other words, the NIST document and the CNSS document are "out of sync".

CNSS will soon be publising an updated edition of CNSSI 1253, which will correspond to NIST SP 800-53, Rev 4. At that point, CNSS and NIST will be "in sync" and the stage will be set for DoD to publish the updated versions of its own policies (i.e., DoD Directive 8500.01, and DoD Instructions 8500.02 and 8510.01) and officially set in motion the transition from DIACAP to "RMF for DoD IT".

It now appears the transition will begin in earnest sometime in the second quarter of 2014. DoD personnel and contractors at all levels will soon be on a mission to get themselves educated in RMF and begin the process of transforming their information security programs.

In order to provide DoD programs with the opportunity to "jump start" their knowledge of RMF and the transition process, BAI is pleased to offer our DoD RMF Training Program. This is a four-day program consisting of *DoD RMF Fundamentals* (one day), followed by *DoD RMF In Depth* (three days).

Whether you are new to the entire concept of security assessment and authorization (aka. certification and accreditation) or a seasoned DIACAP veteran looking for RMF and transition knowledge, this training program will give you practical knowledge and skills you can put to work immediately in your environment.

Registration is open for the DoD RMF training program at register.rmf.org. For additional information, please call us at 1-800-RMF-1903, or visit our website www.rmf.org.

Professional Certification Training

By Annette H. Leonard

DoD Directive 8570.01, entitled *Information Assurance Workforce Improvement Program*, provides the basis for an enterprise-wide solution to train, qualify, and manage the DoD Information Assurance (IA) workforce. The policy requires Information Assurance technical staff and management to be trained and qualified to a DoD-approved baseline requirement. The Directive's accompanying manual identifies the specific individual qualifications mandated by the Directive's enterprise-wide IA workforce management program.

All DoD employees and contractors with information assurance responsibilities are required to earn appropriate professional certification.

To support this policy, DoD provides a process that defines three levels of IA management personnel (IAM Levels I, II and III), three levels of IA technical personnel (IAT Levels 1, II, and III), as well as five categories of Computer Network Defense Service Provider (CNDSP) personnel (Analyst, Infrastructure Support, Incident Responder, Auditor and Manager).

Several certification options are available for each level/category. For example, personnel designated as "IA Management Level II" are required to earn one of the following certifications: CAP, GSLC, CISM, CISSP. CND Incident Responders are required to be certified as GCIH, CSIH or CEH.

"... DoD employees and contractors with information assurance responsibilities are required to earn appropriate professional certification."

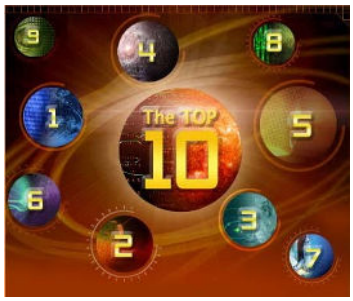
For additional information on these professional certification classes, please visit the BAI website at www.rmf.org, or call us at 1-800-RMF-1903.

Through our partnership with Integration Technologies Cyber Training (ITCT), a division of RPI Group, Inc. BAI is pleased to offer high-quality professional certification training. These classes are designed to provide knowledge and skills you can use in the workplace, while also preparing you for the certification exam. Initial class offerings include:

Certified Information Security Manager (CISM). Demonstrate your information security management expertise. The uniquely management-focused CISM certification promotes international security practices and recognizes the individual who manages designs, and oversees and assesses an enterprise's information security. This course focuses on advanced risk management and specific compliance and security management operations.

Certified Ethical Hacker (CEH). Become an Ethical Hacker! An Ethical Hacker is very similar to a Penetration Tester. The Ethical Hacker is a trusted individual usually employed with the organization or authorized by an organization to undertake an authorized attempt to penetrate networks and/or computer systems using the same methods and techniques as a Hacker.

Certified Information Systems Security Professional (CISSP). Prepare yourself for one of the most prestigious security certifications with superior prep materials and test-taking tips from the experts. Our experts provide you with real-world experience and cover all the material you need to prepare for the (ISC)2 CISSP exam with proven test taking tips and strategies.



Top Ten Things That Will Stay the Same

By Lon J. Berman, CISSP

As DoD begins its transition from DIACAP to RMF, everyone is naturally focused on all the things that will be changing—everything from terminology to documentation to security controls.

Thankfully, not everything is changing!

For this month's Top Ten List, we thought it would be interesting to take a look at some of the things that will not be changing with the advent of RMF in DoD.

10. **DoDI 8510.01.** DoD Instruction 8510.01 will remain the governing document for the security life cycle process. It is currently being revised to reflect RMF rather than DIACAP as the "official" DoD process.

9. **DIACAP Knowledge Service.** The DIACAP Knowledge Service will remain the authoritative source for security-related information and guidance. RMF-oriented content is currently being added.

8. **Major Change.** Systems will still need to be reauthorized (reaccredited) when a "major change" to the system takes place. The individual who signed the ATO will still have the final say on whether or not a proposed change is "major".

7. **Contractor Owned/Operated Systems.** IT-based processes "outsourced" to contractor-owned systems will still require ATO.

6. **Independent Assessment.** DoD systems will still require independent assessment (in accordance with DoD Component policies and procedures) in order to receive ATO.

5. **System Registration.** Information systems will be still need to be registered with the IA program, in accordance with DoD Component policies and procedures.

4. **Plan of Action and Milestones (POA&M).** POA&Ms will continue to be used to report and track security weaknesses of information systems, and to manage corrective actions.

3. **Configuration Standards.** DISA Security Technical Implementation Guides (STIGs) will continue to be the official DoD standards for configuring operating systems, databases, web servers, network devices, etc..

2. **Training and Certification.** DoD Instruction 8570.1 (or its planned successor) will still be in force. DoD employees and contractors having any sort of IA responsibility will still be required to hold appropriate professional certification.

1. Approval to Operate (ATO). All information systems owned by DoD, or operated on behalf of DoD, will still need ATO from a senior DoD official. The process leading to ATO will be changing (RMF rather than DIACAP). Even the title of the person signing it will change (Authorizing Official rather than DAA), but the fundamental concept of risk-based decision ("balancing" or residual risk against mission need) will be unchanged.

Security Control Spotlight—Documentation

By Kathryn M. Farrish, CISSP

In the previous issue of RMF Today, we defined three types of documentation that are typically used as evidence of compliance with security controls.

Policy—policies define what an organization does.

Procedure—procedures, sometimes called standard operating procedures or SOPs, define how the organization carries out its policies.

Assurance—assurance documentation provides operational evidence that the organization is in fact following its procedures.

Now we'll turn our attention to the ways in which these three types of documentation tie to security control families and individual controls.

NIST SP 800-53 organizes the Security Controls into 17 control families, each of which covers a management, operational or technical "subject area", such as Access Control, Incident Response, Maintenance, or System and Communications Protection. Each family is identified by a 2-letter code, sub as AC for Access Control, or MP for Media Protection.

> ***"In all cases, the first control in each family specifies the Policies and Procedures that need to be in place."***

Within each family are a set of security controls. The smallest families have only 5 or 6 controls, while the largest has over 40. In all cases, however, the first control in the family specifies the Policies and Procedures that need to be in place. For example control AC-1 is entitled "Access Control Policy and Procedures", IR-1 is "Incident Response Policy and Procedures", etc.

The text of the control provides the details on the types of policies and procedures that are required. Many of these "XX-1" controls come with supplemental guidance that provides further amplification. For example, control AC-1, "Access Control Policies and Procedures" states:

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:
   1. Access control policy [*Assignment: organization-defined frequency*]; and
   2. Access control procedures [*Assignment: organization-defined frequency*].

You'll notice three places in this control where organization-defined parameters must be filled in. This enables the control to be flexible enough to be used across the broad spectrum of departments and agencies.

Procedures are required as evidence for many of the controls beyond "XX-1". For example, one provision of AC-2 states:

The organization … requires approvals by *[Assignment: organization-defined personnel or roles]* for requests to create information system accounts.

Clearly some sort of SOP is required as evidence of compliance with this control. Additionally, some sort of assurance documentation is required to show that the procedure is in fact being followed, perhaps a log of account requests showing approval/ denial, or copies of completed account request forms with appropriate approval signatures on them.

Next time, we'll look at the wide variety of assurance documentation that can be used to establish compliance with management, operational and technical controls.

Training for Today … and Tomorrow

BAI currently offers three training programs:

- **DoD RMF** – recommended for DoD employees and contractors that require detailed RMF knowledge and skill training; 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. The 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 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 through June, 2014 are as follows:

Date	Training Program	Location
18-20 FEB	Information Security Continuous Monitoring (ISCM)	Washington, DC and Personal Classroom
3-6 MAR	DoD RMF Fundamentals and In Depth	National Capital Region and Personal Classroom
24-27 MAR	FISMA RMF Fundamentals and In Depth	Washington, DC and Personal Classroom
14-17 APR	DoD RMF Fundamentals and In Depth	Personal Classroom
22-24 APR	Information Security Continuous Monitoring (ISCM)	Washington, DC and Personal Classroom
19-22 MAY	DoD RMF Fundamentals and In Depth	Colorado Springs, CO and Personal Classroom
2-5 JUN	FISMA RMF Fundamentals and In Depth	Washington, DC and Personal Classroom
23-26 JUN	DoD RMF Fundamentals and In Depth	Huntsville, AL and Personal Classroom

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.

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