Risk Management Framework Today ... And Tomorrow

Formerly DIACAP Dimensions

July, 2014
Volume 4, Issue 3

In this issue:

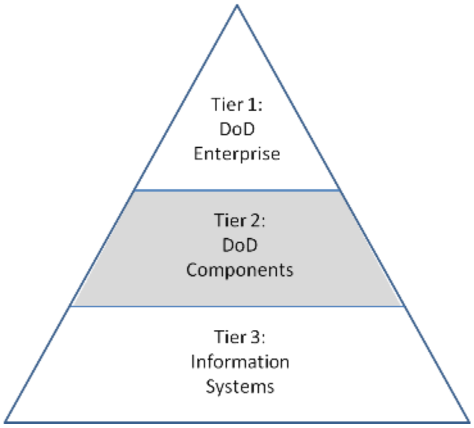
DoD Programs "Gear Up" for Transition to RMF

By Lon J. Berman, CISSP

With the publication of revised DoD Instruction 8510.01, adoption of the Risk Management Framework (RMF) by DoD is now official.

DoD programs big and small have gotten busy planning their strategies for transitioning from DIACAP to "RMF for DoD IT". Let's take a look at some of the efforts currently underway across the DoD landscape to "gear up" for RMF.

As you may know, the principles underlying RMF stem from a series of documents published by the National Institute of Standards and Technology (NIST). NIST utilizes a three-tier model to illustrate the risk management process in a large organization. DoD interprets the three-tier model as follows:



Beyond publication of DoDI 8510.01, what other activities are taking place at Tier 1 (DoD Enterprise) in support of the RMF transition?

- RMF Knowledge Service. For the past couple of months, DoD has slowly been adding content to the Knowledge Service (KS) website, including security control information, guidance on the RMF process steps, etc. KS is available at the following URL: **https://rmfks.osd.mil.**

- eMASS. DoD is in the process of enhancing the Enterprise Mission Assurance Support System (eMASS) to include the RMF workflow, NIST security controls, etc.

- STIGs. DISA is in the process of revising many of the Security Technical Implementation Guides (STIGs) to include references to applicable NIST security controls.

- Continuous Monitoring. DISA is in the process of developing CMRS, a Continuous Monitoring and Risk Scoring system that will assist DoD system owners in meeting RMF continuous monitoring requirements.

Tier 2 (DoD Components) are also busy planning for the transition to RMF.

- Component-specific policies and guidance (e.g., Army, Air Force, Navy and Marine Corps security policies) are being revised to cover Assessment and Authorization (formerly Certification and Accreditation) in accordance with RMF.

- Under the leadership of the component Security Control Assessor (SCA, formerly CA), assessment teams are being prepared to conduct independent testing of systems for compliance with the NIST security controls in accordance with RMF.

See *DoD Programs Gear Up, Page* 2

Comparing Training Delivery Methods

By Annette Leonard

With the "standardization" of risk management practices across DoD, federal civil agencies and the intelligence community, we are seeing a substantial increase in demand for RMF training. At the same time, we are seeing a wider variety of training delivery methods than ever before. Let's take a look at the pros and cons of these various methodologies.

Traditional classroom-based training is alive and well. A knowledgeable trainer in front of a classroom is capable of creating an immersive learning environment that is hard to beat. Not only can the instructor directly impart knowledge, but he/she can facilitate interaction among the students that further enhances the experience for everyone. The principal disadvantage of classroom-based training is the cost, and this is primarily due to travel expenses.

"Modern technology ... in the hands of an experienced instructor ... can deliver a training experience that rivals the traditional classroom."

Modern technology now provides us an alternative in the form of online, instructor-led training. Students can take their training in the comfort of their own home or office, thus reducing travel costs to zero. In the hands of an experienced instructor, the combination of web conferencing, audio conference bridge and "webcam" technologies can deliver a training experience that rivals the traditional classroom.

Opportunities for active learning can be further enhanced by combining traditional classrooms with online "distance learners" in a hybrid training environment.

Finally, there is computer-based training (CBT). CBTs range from simple Powerpoint slide shows to sophisticated Learning Management Systems (LMS). CBT can typically be delivered at a lower cost than classroom or online instructor-led training, and can normally be delivered "on demand" to each student. The downside is that there is little, if any, opportunity to ask questions, and no ability to "network" with classmates. Studies have shown that the greater the learner's involvement in the active learning process, the greater the level of content acquisition. Thus retention of knowledge is typically lower with CBT than with instructor-led methods.

The bottom line is that there is no one "right" methodology for training delivery. It is important to understand the advantages and disadvantages of each in order to choose wisely.

DoD Programs Gear Up, from Page 1

- Authorizing Officials (AOs, formerly DAAs) are being re-trained as necessary.

And last, but by no means least, Information System Owners (Tier 3) are gearing up, too.

- System Owners and their support staff are familiarizing themselves with DoD, CNSS and NIST publications that directly support RMF.
- System Owners are beginning to plan for re-categorizing their systems (using CNSSI 1253 in place of MAC and CL) and developing appropriate security control baselines.
- System Owners are arranging for their teams, both DoD employees and Contractors, to receive relevant training in RMF.

Be ready for busy times ahead!

Top Ten—Ensuring a Smooth Transition

By Lon J. Berman, CISSP

Now that DoD has “officially” begun its adoption of “RMF for DoD IT”, let’s take a look at some of the things *your* organization can do to ensure a smooth transition.

10. **Publications.** Organizations should ensure they are using the latest copies of relevant publications. This includes not only DoD issuances (DoDI 8500.01 and DoD 8510.01) but also CNSSI 1253 and NIST Special Publications such as NIST SP 800-37 and NIST SP 800-53. Organizations should also obtain access to the RMF Knowledge Service (https://rmfks.osd.mil) as a source of supplemental guidance.

9. Training. Organizations should ensure that their employees and contractors receive appropriate RMF training (www.rmf.org).

8. **Categorization.** Organizations should begin the task of re-categorizing their systems in accordance with CNSSI 1253. Three separate categorization levels (for Confidentiality, Integrity and Availability) will replace the DIACAP MAC and CL.

7. **Security Control Baseline.** Once each system is re-categorized, organizations should develop an appropriate security control baseline, using NIST SP 800-53, organization-defined parameters, and other tailoring guidance. Any relevant overlays (see below) should be included.

6. **Overlays.** Organizations should determine if there are any security control overlays relevant to their specific community of interest. If so, these should be incorporated into the security control baselines.

5. **Security Plan.** Organizations should begin drafting a Security Plan for each system.

4. **Gap Analysis and Remediation.** Once security control baselines and initial Security Plans have been established, organizations should conduct a self-assessment and identify any compliance gaps resulting from new or changed controls. Plans for addressing any identified compliance gaps should be developed. This is particularly important because additional funding or other resources may be required.

3. **Continuous Monitoring Plan.** Organizations should begin developing plans for continuous monitoring of security controls, in accordance with DoDI 8510.01 and NIST SP 800-137.

2. **Assessment and Authorization.** Organizations should coordinate with their specific DoD component to determine if there have been any changes to the process of arranging for independent assessment (validation) of security controls. Organizations should also coordinate with their specific DoD component to determine if there has been any change to the AO (formerly DAA) assigned to their systems.

1. ANTICIPATE CHANGE. Organizations should understand RMF is still very much a “work in progress” within DoD. Changes to policies and guidance are to be expected as the process rolls out. Relevant DoD and DoD Component websites and publication sites should be regularly monitored for updates. Regular visits to the RMF Knowledge Service (KS) are a good starting point.

Security Control Spotlight—Organization-Defined Parameters

By Kathryn M. Farrish, CISSP

Under RMF, NIST SP 800-53 is the primary source for security controls. If we compare these controls to the DoDI 8500.2 IA controls used in DIACAP, several obvious differences can be seen. Most notable among these differences is the fact that many of the NIST controls are not "complete" as published, but require some "fill in the blanks". These "blanks" are called Organization-defined Values or Organization-defined Parameters. Here is an example taken directly from NIST SP 800-53:

AU-11 Audit Record Retention

The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

As you can see, this control is not truly "complete" until the required retention period is filled in.

"Many of the NIST controls are not 'complete' as published, but require some 'fill in the blanks.'"

Many other controls require two or more "Assignment" parameters to be filled in before the control can be considered "complete".

A few controls contain a different type of organization-defined parameter called a "Selection". In these cases, the organization is not required to "fill in the blank", but rather to choose from a set of alternatives. For example:

AC-20 Use of External Information Systems

Enhancement (2). The organization [*Selection: restricts; prohibits*] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

In this case, one of the two alternatives is chosen in order to "complete" the control.

So how is a System Owner supposed to figure out what values to fill in? Like a lot of things in this business, it's a simple question with a somewhat complicated answer.

- CNSSI 1253 contains a list of organization-defined values for some (but by no means all) of the controls. For example:

  AU-11
  "A minimum of 5 years for Sensitive Compartmented Information and Sources and Methods Intelligence Information
  AND
  A minimum of 1 year for all other information (Unclassified through Collateral Top Secret)"

- DoD has indicated they plan to publish a list of organization-defined values on the RMF Knowledge Service website, however this has not been done as of the publication date of this newsletter

- DoD Components or command-level information security policies may provide additional organization-defined values. For example, component-level policies provide specific requirements for passwords, such as minimum length and complexity. These requirements enable organization-defined parameters to be filled in for controls such as IA-5

- Information security policies for individual systems may also provide organization-defined values (e.g., backup frequencies)

Any organization-defined parameters not covered by one of the above will remain at the discretion of the System Owner. It is highly recommended that the System Owner document the organization-defined values (and the rationale for their choice) in the System Security Plan.

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 <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 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 half of calendar year 2014 are as follows:

RMF for DoD IT (Fundamentals and In Depth)

- **21-24 JUL (Online Personal Classroom™)**
- **18-21 AUG (Colorado Springs <u>and</u> Online Personal Classroom™)**
- **22-25 SEP (Huntsville <u>and</u> Online Personal Classroom™)**
- **20-23 OCT (Colorado Springs <u>and</u> Online Personal Classroom™)**
- **17-20 NOV (Huntsville <u>and</u> Online Personal Classroom™)**
- **8-11 DEC (National Capital Region <u>and</u> Online Personal Classroom™)**

RMF for Federal Agencies (Fundamentals and In Depth)

- **8-11 SEP (Washington, DC <u>and</u> Online Personal Classroom™)**
- **3-6 NOV (Washington, DC <u>and</u> Online Personal Classroom™)**

Information Security Continuous Monitoring

- **5-8 AUG (Online Personal Classroom™)**
- **30 SEP-2 OCT (Washington, DC <u>and</u> Online Personal Classroom™)**
- **2-4 DEC (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.