# Risk Management Framework Today

*Formerly DIACAP Dimensions*

... And Tomorrow

March, 2015
Volume 5, Issue 1


In this issue:


| | |
|---|---|
| RMF Transition—What Do I Really Need to Know? | 1 |
| What are CCIs and Why Should I Care? | 2 |
| Top Ten—Getting Off to a Good Start | 3 |
| Security Control Spotlight—The PM Family | 4 |
| Training for Today... and Tomorrow | 5 |


## RMF Transition—What do I Really Need to Know?

By Lon J. Berman, CISSP

It's hard to believe it's been *a whole year* since the publication of DoD Instruction (DoDI) 8510.01 in March of 2014, which officially began the transition from the DIACAP process and IA Controls to the Risk Management Framework (RMF) and NIST Security Controls. While there are isolated pockets of progress to report, the fact is the major DoD components are just now beginning their transition in earnest.

DoD employees and contractors are now faced with the daunting tasks of adjusting to a new process *and* assessing their systems' compliance with a completely new baseline of controls. Most have come to the realization that some type of training is essential to their success. But what sort of training do they need?

First priority should be training that is centered around the *RMF for DoD IT* process and security controls. This type of training should provide a thorough understanding of:

- RMF Terminology
- RMF Roles and responsibilities
- RMF for DoD IT life cycle process
  - Categorize
  - Select
  - Implement
  - Assess
  - Authorize
  - Monitor
- RMF for DoD IT documentation
  - Security Plan (SP)
  - Security Assessment Report (SAR)
  - Plan of Action and Milestones (POA&M)
- NIST security controls and assessment procedures

OK, so I need to learn all about the RMF for DoD IT process and security controls. What about eMASS training? Won't that do the trick? After all, isn't eMASS the support tool that is becoming the "standard" across all (or nearly all) of DoD?

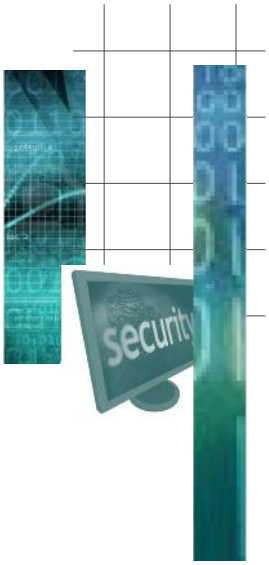
It is true that eMASS is the tool of choice for most DoD components. And, absolutely, learning how to "push the buttons" and operate eMASS is important. However, without a solid foundation in the RMF process and the NIST controls, eMASS training alone will not give you the understanding you need to tackle the job of getting your systems authorized in accordance with RMF. Ideally, you should *walk into* eMASS training with thorough knowledge of RMF for DoD IT. That's the only way you'll have the context within which to truly grasp what eMASS can do for your organization.

But wait. Doesn't eMASS training already include instruction in the RMF process and security controls? Generally speaking, the answer is NO … or, if any process training is included at all, it's absolutely minimal.

**The best approach is to get yourself thoroughly trained in RMF for DoD IT, and <u>then</u> get some eMASS training.**

That makes sense. Now, I see numerous sources to get RMF training. How do I know which ones are best? Well, a good start is to make sure they are offering "RMF for DoD IT" training, and not just generic "RMF" training. There are very significant differences.

See *Really Need to Know*, Page 2




## What Are CCIs and Why Should I Care About Them?

By Kathryn M. Farrish, CISSP

One of the more recent information security innovations is the Control Correlation Identifier, or CCI. Each CCI provides a standard identifier and description for "singular, actionable statements" that comprise a security control or security best practice.

The purpose of CCIs is to allow a high-level statement made in a policy document (i.e., a security control) to be "decomposed" and explicitly associated with the low-level security settings that must be assessed to determine compliance with the objectives of that specific statement.

Under the leadership of the Defense Information Systems Agency (DISA), a working group has been cataloging CCIs for the past several years. The collection has now been developed to the point that every assessment objective in the NIST SP 800-53A has been mapped to an individual CCI.

The current list of CCIs can be downloaded in XML format (viewable in a web browser such as Internet Explorer). The URL for downloading is: http://iase.disa.mil/stigs/cci/Pages/index.aspx.

DISA encourages feedback from the information security community; a comment form is provided for that purpose.

Here is an example of a CCI:

*CCI: CCI-001239*
*Status: Draft*
*Contributor: DISA FSO*
*Date: 2009-09-22*
*Type: Technical*
*Definition: The organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, web accesses, removable media or other common means or inserted through exploitation of information system vulnerabilities.*
*References: NIST SP 800-53 SI-3.a*
*NIST SP 800-53A SI-3.1(ii)*

DISA is also in the process of revising numerous Security Technical Implementation Guides (STIGs) to include references to CCIs that correspond to each of the recommended configuration settings.

With the success of the CCI effort comes some hope that at least a portion of the effort associated with RMF assessment can be automated!

> *"...DoD has mapped CCIs to each one of the assessment objectives in NIST SP 800-53A ..."*

---

***Really Need to Know*, from Page 1**

Also, **make sure the training vendors you are considering are teaching the entire class from the "DoD perspective"**, which should include:

- DoD policies
- Similarities and differences between DIACAP and RMF
- DIACAP-to-RMF transition guidance

Some training providers claim they teach a single RMF course that meets the needs of DoD as well as other departments and agencies. Don't believe them.

Lastly, consider the provider's overall training approach. Vendors whose primary mission is to prepare students for certification tests may not offer practical guidance, case studies and class exercises appropriate to students who will need to put their training into practice in the "real world" of DoD IT.

## Top Ten—Getting Off to a Good Start

By Annette Leonard

> *"The beginning is the most important part of the work."*
> — *Plato*, *The Republic*

Before rushing headlong into the RMF fray, DoD system owners should take the time to ensure they get off to a good start. Mistakes made at the beginning of the effort can be very costly to correct later in the life cycle.

Here, then, is our "Top Ten" list of things you should do to "hit the ground running" with your RMF transition effort.

**10. Glossary.** RMF is replete with new or revised terminology and acronyms. Get yourself a copy of CNSSI 4009, the National Information Assurance Glossary. This will be an invaluable reference for those times when you run into an unfamiliar term or find yourself in a friendly "dispute" over something you encounter in a policy document or memo.

**9. Document Library.** Start building a library of RMF reference documents. Remember, unlike previous DoD processes, RMF relies heavily on documents from sources outside DoD. Here is a good starting list for your library:

- DoDI 8500.01, DoDI 8510.01
- CNSSI 1253
- NIST SP 800-37
- NIST SP 800-53, NIST SP 800-53A.

**8. Component Policies.** Check with your DoD Component (Air Force, Army, Marine Corps, Navy, etc.) cybersecurity office to see if there are any policies or instructions related to RMF. If so, add them to you document library.

7. **Authorizing Official(s).** Make sure you know who will be signing the authorization (accreditation) for your system(s) under RMF. It may or may not be the same individual (DAA) who signed your DIACAP ATO.

**6. RMF Knowledge Service.** Make sure you can access the RMF Knowledge Service (KS). This website is DoD's "authoritative source" for all things RMF.

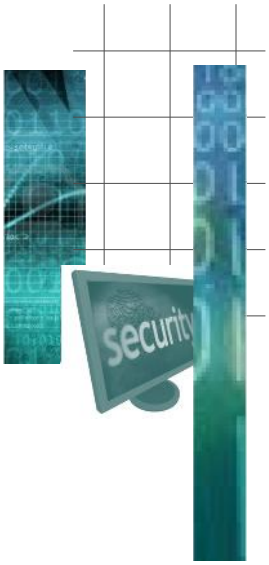
**5. Automated Tool.** Make sure you have an account and can log into the automated tool that your component or command will be using to support RMF. In many cases, this will be the DoD enterprise tool eMASS.

**4. System Boundaries and Inheritance.** Take the time to confirm your system boundaries and inheritance relationships with hosting providers, etc.

**3. Information Content.** Make sure you understand the types of information stored and processed by your system(s) and who the information owners are. These individuals will be critical to the success of the system categorization effort.

**2. Information Security Support.** Make sure you have an Information System Security Manager (ISSM) or Information System Security Officer (ISSO) on your team to provide support.

**1. Training. Make sure you and the other members of your team are trained, both in the RMF for DoD IT process itself, and in any automated tools (e.g., eMASS) you will be using to document your efforts.**




## Security Control Spotlight—The PM Family

By Lon J. Berman, CISSP

The Beatles were comprised of how many musicians? Easy, right? They were called the "Fab Four", so there were definitely 4. Now Google "the fifth Beatle" and see what you get. Ditto for "sixth sense". When I eat at a Thai restaurant and the waitress asks how hot I want my food—on a scale of 1 to 5—I usually answer "6".

If you've looked through NIST SP 800-53 Rev 4, you probably saw that there are 17 families of controls from which the various baselines are to be built. Yet, if you ask a group of "subject matter experts" how many control families there are, some people will answer 18.

Like most apparent paradoxes, there's a somewhat logical explanation for this seemingly bizarre discrepancy.

When NIST first put together SP 800-53, there really were 18 families of security controls. The 18th family was "PM", or "Program Management". It was filled with controls dealing with various aspects or establishing and operating an organization's information security program. Some of the controls in the PM family include:

- PM-1 Information Security Program Plan
- PM-2 Senior Information Security Officer
- PM-3 Information Security Resources
- PM-4 Plan of Action and Milestones Process
- PM-5 Information System Inventory
- PM-7 Enterprise Architecture
- PM-8 Critical Infrastructure Plan
- PM-9 Risk Management Strategy
- PM-13 Information Security Workforce

*"...When NIST first put together SP 800-53, there really were 18 families of security controls."*

These controls are clearly aimed at the organizational level, and not at individual information systems. In fact, NIST included a "disclaimer" to that effect:

**Deployed organization-wide.**
**Supporting information security program.**
**Not associated with security control baselines.**
**Independent of any system impact level.**

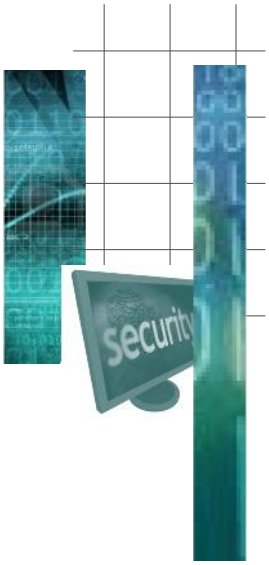
Despite everything, the PM family of controls remained in the main body of SP 800-53 through several revisions. Finally, it dawned on the authors that these controls just didn't belong with the other 17 families; they were moved to a separate Appendix (Appendix G, to be exact) and removed from the recommended baselines of controls.

Some suggested the PM family of controls had been "demoted" or "Plutoed". The fact is they were simply moved to where they made more sense.

End of story? Not quite.

In the DoD world, some versions of eMASS were found to be putting the PM controls right back into the baselines for all system categorization levels.

So, that's the story of the PM family of controls … at least so far! If anyone ever asks you how many control families there are, give them your best answer (17), but just remember—"Men are from Mars, women are from Venus, and security controls—at least the Program Management ones—are from Pluto."




## 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 second quarter of 2015 are as follows:**

**RMF for DoD IT (Fundamentals and In Depth)**

- **13-16 APR 2015 (National Capital Region and Online Personal Classroom™**
- **4-7 MAY 2015 (Huntsville and Online Personal Classroom™)**
- **15-18 JUN 2015 (Colorado Springs and Online Personal Classroom™)**

**RMF for Federal Agencies (Fundamentals and In Depth)**

- **6-9 APR 2015 (Online Personal Classroom™)**

**Information Security Continuous Monitori**

- **21-23 APR 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