Risk Management Framework Today

Formerly DIACAP Dimensions

... And Tomorrow

June 2011
Issue 1, Volume 1

Find us on Facebook

LinkedIn

C&A Transformation = Newsletter Transformation

By Lon J. Berman

As you probably know, there is an ongoing effort to standardize the practice of Certification and Accreditation (C&A) across DoD, civilian, and intelligence agencies. The end result of this "transformation" will be a unified process and control set based on the Risk Management Framework (RMF) published by the National Institute of Standards and Technology (NIST). In keeping with this spirit of transformation, your newsletter is undergoing a transformation, too. *DIACAP Dimensions* is now *RMF Today... and Tomorrow*!

DoD is just now beginning the transformation process, so we will continue to provide helpful guidance on DIACAP implementation as we always have. Beyond that, we will now be including features on the status of the transformation, as well as insight into the roles and responsibilities, life cycle process, and security controls that comprise the RMF. We will also offer practical guidance on preparation and execution of the transition from DIACAP to RMF. Some of this new content will be aimed at a broader audience, to include civilian and intelligence agencies in addition to DoD. Our goal is to help you with the IA program of today, while helping you prepare for the IA program of tomorrow!

As we proceed down this path, please keep in mind this is *your* newsletter. If there is information you would like to see, please e-mail us at newsletter@rmf.org and we will do our best to accommodate your request. General comments and questions are also welcome.

In this issue:

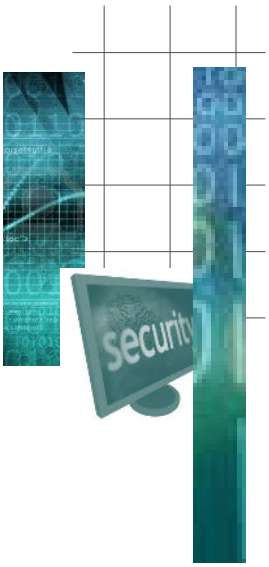
DIACAP Training Comes to Southern California!

By Kathryn Farrish

At long last, DIACAP Training will be available in Southern California! DIACAP Resource Center has entered into a partnership with New Horizons Computer Learning Centers of Southern California (NHSoCal) to offer our complete DIACAP training program (DIACAP Fundamentals and DIACAP In Depth). Classes will initially be offered in San Diego (July and September, 2011) and Anaheim (August, 2011), with the possibility of expansion to additional NHSoCal locations.

These new training sites will be convenient to a multitude of DoD and contractor facilities in Southern California. The savings in travel costs will be a welcome thing for those working under tight training budget constraints (and, these days, that's just about everyone!).

New Horizons Southern California is part of the world's largest independent IT training company. We are excited about this partnership and look forward to teaching at their state-of-the art facilities.



Status of DIACAP Transformation

By Lon J. Berman

At a recent IA Symposium, DoD presented the following high-level goals for their C&A transformation:

1. Define a common set of trust (impact) levels and adopt and apply them across the Intelligence Community (IC) and DoD. Organizations will no longer use different levels with different names based on different criteria.
2. Adopt reciprocity as the norm, enabling organizations to accept the approvals by others without retesting or reviewing.
3. Define, document, and adopt common security controls, using NIST Special Publication (SP) 800-53 as a baseline.
4. Adopt a common lexicon, using CNSS Instruction 4009 as a baseline thereby providing DoD and IC a common language and common understanding.
5. Institute a senior risk executive function, which bases decisions on an "enterprise" view of risk considering all factors, including mission, IT, budget, and security.
6. Incorporate information assurance (IA) into Enterprise Architectures and deliver IA as common enterprise services across the IC and DoD.
7. Enable a common process that incorporates security within the "lifecycle" processes and eliminate security-specific processes. The common process will be adaptable to various development environments.

Implementation will be facilitated by publication of the following documents: DoDD 8500.01 (IA Policy), DoDI 8500.2 (IA Implementation), DoDI 8510.01 (DoD IA Risk Management Framework). No firm timeframe has been given for publication of these documents, other than "Calendar Year 2011". *RMF Today (and Tomorrow)* will endeavor to keep you up-to-date on the latest developments within DoD. Stay tuned!

Is C&A Dead?

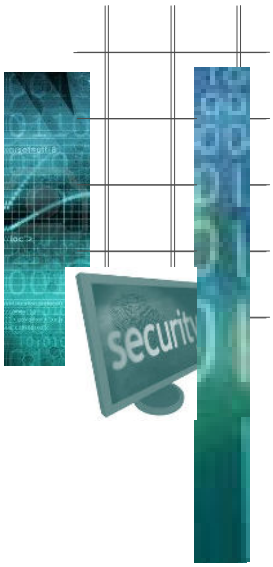
By Kathryn Farrish

"… You can be assured, C&A is absolutely not going away!"

Several times over the past few months, I have heard statements made that imply Certification and Accreditation (C&A) is "going away". I think I can best respond by quoting Mark Twain's reaction to an "obituary" that was published in 1897: "Reports of my death are greatly exaggerated".

Although some IT folks may wish otherwise, you can be assured C&A is absolutely not going away! In fact, the requirement to formally authorize systems for operation, based on an assessment of compliance with security controls, is a fundamental part of the Risk Management Framework (RMF).

That said, however, it is true that the *term* C&A is being phased out. In RMF terminology, "Certification" becomes "Assess Security Controls" and "Accreditation" becomes "Authorize Operation". These are Steps 4 and 5 of the 6-step RMF life cycle. I'm sure it will take quite a while for the term C&A to fade from everyday use. Who knows, perhaps someday we might hear it called A&A (Assess and Authorize)?



Top Ten—Preparing for C&A Transformation

By Lon J. Berman

Our latest Top Ten list focuses on ways to prepare yourself for the transformation from DIACAP as we know it today to DoD's implementation of RMF.

10. Download a copy of the Committee on National Security Systems (CNSS) Instruction 4009, "Information Assurance Glossary". This is an invaluable reference document that will help you understand the new terminology being introduced with the transformation.

9. Visit the National Institute of Standards and Technology (NIST) website (http://csrc.nist.gov) and download a copy of Special Publication (SP) 800-37 (Revision 1), "Guide for Applying the Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach".

8. Download and familiarize yourself with NIST SP 800-53, "Recommended Security Controls for Federal Information Systems".

7. Download and familiarize yourself with the key CNSS publications, including CNSSP 22, "Information Assurance Risk Management Policy for National Security Systems", and CNSSI 1253, "Security Categorization and Control Selection for National Security Systems" (https://www.cnss.gov).

6. Obtain access to the DIACAP Knowledge Service (https://diacap.iaportal.navy.mil – DoD CAC or ECA certificate required), and download a copy of the security control "map" that compares DoDI 8500.2 IA Controls with NIST SP 800-53 controls.

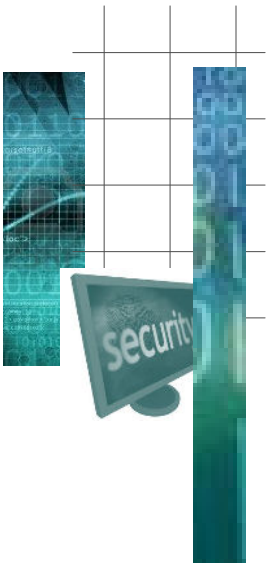
5. Visit the NIST "FISMA Implementation Project" website (http://csrc.nist.gov/groups/SMA/fisma/index.html) for technical guidance and RMF-related news; you can also subscribe to the CSRC Publications Mailing List (http://csrc.nist.gov/publications/subscribe.html) for notification of updates to NIST RMF publications.

4. Monitor your DoD Component collaboration site (e.g., AKO for Army) for component-specific guidance on C&A transformation.

3. Monitor the DIACAP Knowledge Service for publication of updated DoD Instructions 8500.2 (IA Controls) and 8510.01 (DIACAP/RMF).

2. Visit the DIACAP Resource Center and/or FISMA Resource Center websites for C&A transformation news and training opportunities. The DIACAP training curriculum (www.diacap.net) has been enhanced to include information on the transition process. DoD employees and contractors wishing to gain more detailed knowledge of RMF should consider attending FISMA RMF training (www.fisma1.net).

1. Above all, DON'T PANIC. DoD's transition from DIACAP to RMF will be "evolutionary, not revolutionary." Although details have yet to be released by DoD, they have provided assurance that provisions will be made for existing DIACAP-accredited systems and for new systems currently in the midst of the DIACAP process in pursuit of their initial accreditation.



IA Control Spotlight—Configuration Management

Configuration management (CM) focuses on establishing and maintaining consistency of a system or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. For information assurance, CM can be defined as the management of security features and assurances through the control of changes made to hardware, software, firmware, documentation, test, text fixtures, and test documentation throughout the life cycle of an information system.

"Configuration Management focuses on establishing and maintaining consistency of a system or product's performance…."

Regardless of the C&A process your organization falls under, CM policies and procedures will need to be developed. The CM policies and procedures should include: roles, responsibilities, processes and procedures of the CM process for your organization. NIST CM-3 and DIACAP DCCB require the establishment of a Configuration Control Board (CCB) to provide oversight of the CM process. Members should be chosen from the functional, operational and managerial groups within the organization and there must be a security representative included as a voting member. The documentation should include the organizational definition of a configuration item (CI) and also what types of changes to the information system will be controlled. You want to avoid having every change to the IS go through the configuration management process. Adding a user is a change to the IS that will affect the security posture, but do you really want the CCB to vote every time a new user is added? Probably not. Another procedure that needs to be outlined is now changes are presented to the CCB, how changes are approved/denied by the CCB, and how to document the CCB decision. During the certification of the system, the security control assessor/validator will want to review CCB meeting minutes, so it's important to note that meeting minutes must be kept.

Both NIST and DIACAP require software libraries to be maintained by the CCB. Procedures should include who has access to the software libraries, and who has the authority to push changes approved by the CCB from the test/dev environment to the production environment (NIST CM-5; DIACAP ECPC, DCSL). This access list should be reviewed on a regular basis and modified as needed to ensure least privilege and an audit process should be outlined to review activities associated with configuration-controlled activities.

Another responsibility of the CCB is to maintain the IS baseline. This includes hardware and software inventories and baseline configuration settings (NIST CM-2; DIACAP DCHW, DCSW) . Each IS should be built and configured from a documented baseline that reflects the most restrictive mode consistent with operational requirements. Configuration settings that will inhibit the functioning of the system (i.e., ports, protocols, services, software, hardware, etc) must be documented with an explanation of why this setting differs from the organizational baseline and what risk mitigation has been implemented to safeguard the deviation (NIST CM-6; DIACAP DCCS, ECSC).

While this is not an all-encompassing plan of action, it will definitely get you on the right track to implementing a well-rounded Configuration Management program.

Training for Today … and Tomorrow

Since DoD is just at the early stages of its C&A transformation, we are continuing to offer our "traditional" DIACAP training program, which has recently been enhanced to include modules dedicated to the RMF transition.

Our FISMA RMF training program is suitable for Federal "civilian" agencies as well as DoD personnel looking for insight into the future of "C&A" within their programs.

Each of our training programs consists of a one-day Fundamentals class, followed by a three-day In Depth class. The cost of training is $650 for the one-day class, $1,500 for the three-day class, or $1,935 for the full four-day program (both classes).

DIACAP Fundamentals (One-day)	DIACAP In-Depth (Three-day)
6 Jun 2011 (H)	7-9 Jun 2011 (H)
13 Jun 2011 (CS)	14-16 Jun 2011 (CS)
27 Jun 2011 (NCR)	28-30 Jun 2011 (NCR)
11 Jul 2011 (SD)	12-14 Jul 2011 (SD)
22 Aug 2011 (A)	23-25 Aug 2011 (A)
29 Aug 2011 (NCR)	30 Aug-1 Sep 2011 (NCR)
12 Sep 2011 (SD)	13-15 Sep 2011 (SD)

FISMA RMF Fundamentals (One-Day)	FISMA RMF In-Depth (Three-Day)
20 Jun 2011 (DC)	21-23 Jun 2011 (DC)
22 Aug 2011 (DC)	23-25 Aug 2011 (DC)
3 Oct 2011 (DC)	4-6 Oct 2011 (DC)

(H) - Huntsville, AL, (CS) - Colorado Springs, CO,
(NCR) - Ashburn, VA, (SD) - San Diego, CA,
(A) - Anaheim, CA, (DC) - Washington DC

On-line registration and payment for all scheduled classes is available at www.diacap.net (for DIACAP classes) or www.fisma1.net (for FISMA RMF classes). Registration can also be done by downloading a registration form and submitting the completed form by FAX or email.

Payment arrangements include credit cards, SF182 forms, or purchase orders.

Please visit www.diacap.net or www.fisma1.net for the latest training schedule, including any new dates or locations.

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 (at least 8-10) and a suitable classroom facility. We offer a substantial discount over the normal "per student" registration cost; the discount grows larger as the class size increases. Our "on-site" training fee includes all instructional services, training materials, and instructor travel expenses. Most importantly, you will avoid the travel expenses associated with sending your people to training away from the office. Please contact us to request an on-site training quotation.

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