Risk Management Framework Today

Formerly DIACAP Dimensions

... And Tomorrow

Find us on Facebook

Linked in

New Risk Management Framework Website

By Kathryn Farrish

With all the changes going on in the world of C&A, BAI is following closely along. We have created a new Risk Management Framework website (www.rmf.org) that will eventually replace both the DIACAP and FISMA websites. Within this website you can find information relating to the Risk Management Framework as it pertains to your needs, whether you are a federal agency, a DoD organization, or a commercial company with products and services to provide to government agencies. We are still in the process of adding content, but the end result will be a 'one-stop shop' for all your Risk Management, Security Authorization needs. As the transformation is not complete, we will still maintain separate training programs for the DoD and Federal worlds, and registration for those classes will remain on their respective websites, although you can find training information on the new RMF website. We will also post past newsletters, consulting services, and

much of the same information as we have. In addition, we have a frequently asked questions page to help you out with making the transition to the RMF process as well as necessary documents that make up the RMF process. As the transition continues, if you have questions that are not answered on our website, feel free to use the 'Contact Us' link, and we will do our absolute best to answer those questions for you, as well as add them to our FAQ to help others in your situation.

We've Gone Social!

By Kathryn Farrish

The DIACAP Resource center can now be found on Facebook and Linked In! Like our facebook page to receive updates on the C&A Transformation, and other interesting tid bits, or join a discussion with fellow IA practitioners. Have an IA related question that you just can't find the answer to? Our discussion groups are a great way to get that solution! Also, feel free to share your own experiences within information assurance to others.

You can search within Facebook for, "The DIACAP Resource Center" or go to our webpage (www.rmf.org) and click on the Facebook link!
If Linked In is more your style, we are there too! Linked In is the number one professional networking site. Our Linked In page will keep you updated on our training classes, news regarding the C&A Transformation, and provide you with a space to discuss all information assurance related questions, comments or concerns.

In this issue:

New Cloud Computing Security Authorizations!

By Kathryn Farrish

The federal government, in an effort to increase efficiency and decrease cost to agencies has established a standard approach to Assessing and Authorizing (A&A) cloud computing services and products. The process, Federal Risk Authorization Management Program (FedRAMP) operates under the "Approve Once, Use Often" motto. This will allow an independent commercial company, who is sponsored by one federal agency, to be used by other federal agencies once they have completed the process, and therefore not requiring each government agency who wishes to use their services pay for an accreditation.

Assessments will be done by third party assessment organizations (3PAOs) that have undergone an evaluation based on a formal process for acceptance. 3PAOs will perform initial and periodic assessment of Cloud Service Provider (CSP) systems, provide evidence of compliance, and play an on-going role in ensuring that CSPs meet FEDRAMP requirements. The initial list of approved 3PAOs is expected to be released on or around 1 November 2011, although the likelihood of that date being accurate is low. The process, while it is moving, has not been meeting the previous pre-defined deadlines.

Assessment of risk will be accomplished using the NIST SP 800-53A, however, there are several modifications that have been made to the low and moderate impact levels. Many of the controls have additional enhancements than are required for the standard 800-53 assessment. Additionally, FedRAMP has specified the parameters for all organization-defined controls and also provided additional requirements and guidance. While the proposed FedRAMP security requirements document is still in draft form, many are speculating that little or nothing will be changed before the final version is released.

The FedRAMP Assessment and Authorization (A&A) process is as follows:

1. CSP and agency sponsor begin authorization process with FedRAMP office

2. CSP, agency sponsor and FedRAMP office review security requirements and any alternative implementations

3. FedRAMP office coordinates with CSP for creation of System Security Plan (SSP)

4. CSP has independent assessment of security controls and develops appropriate reports for submission to FedRAMP office

5. FedRAMP office reviews and assembles the final authorization package for the Joint Approval Board (JAB)

6. JAB reviews final certification package and authorizes CSP to operate

7. FedRAMP office adds CSP to authorized system inventory to be reviewed and leveraged by all Federal agencies

8. FedRAMP provides continuous monitoring of CSP.

"Approve once, use often"

Top Ten—Documentation Artifacts

By Lon J. Berman

Supporting documentation, or artifacts, are a key element of the Security Authorization (C&A) process. Artifacts provide written evidence of compliance with requirements (aka. Security Controls or IA Controls). There are no hard and fast rules in RMF regarding the number and content of specific artifacts, but there are a number of "essentials" that will most likely be in every System Owner's documentation set. NOTE: Many of these documents can be developed and maintained at an organizational or command level (rather than for each specific system) and apply to all systems owned by that organization.

10. Information Security Policy. A comprehensive policy document should be prepared for the system or the owning organization, clearly stating the key policies that will be implemented and maintained. This document should be signed by the organizational director or commander.

9. Acceptable Use Policy. This document specifies the "rules of behavior" for system users, and should be signed by each user prior to being granted system access. The AUP should also specify consequences of failure to comply. Many organizations maintain separate AUP's for ordinary users and privileged users.

8. Incident Response Plan. This document delineates the processes to be followed for various types of security incidents, such as loss or damage to equipment, unauthorized access to information, classified information "spillage", etc.

7. Contingency Plan. This document (or set of documents) specifies the steps to be taken in the event normal operation of the system is hampered due to natural or man-made disaster.

6. Vulnerability Management Procedures. This document provides the process for vulnerability and patch management of software, to include operating systems, databases, applications, etc.

5. Account Management Procedures. This document provides the process for establishing user accounts, confirming "need to know", setting privileges and removing accounts, as well as periodic account reviews.

4. Audit Procedures. This document specifies the process for periodic review of audit logs from operating systems, databases and applications, archiving and retention of audit records, etc.

3. System Backup Procedures. This document specifies the procedures for periodic backup of systems and data, including offsite transportation, backup retention, restoration processes, etc.

2. Configuration and Change Management Procedures. This document (or set of documents) provides the processes for configuration, change and release management, and will typically include a Configuration Control Board (CCB) charter as well as guidance for change request and approval, configuration documentation, configuration audit, etc.

1. "As Built" Documentation. These documents provide an accurate picture of the current state of the system, and normally include complete hardware and software inventories, documented configuration settings for installed software, system and network diagrams data flow and accreditation boundary. These are living documents that should be meticulously maintained in accordance with the organizations' configuration management process.

IA Control Spotlight—Rules of Behavior

By Kathryn Farrish

Sensitive and classified information stored on servers, workstations, media and documentation are at risk of access, monitoring, copying, destruction, and illegal distribution if rules are not in place to prevent such actions. Access to sensitive and classified facility access points is a risk from unauthorized personnel. Personnel performance in the work place is at risk of being non-productive due to unethical and irresponsible behavior if consequences for those actions are not defined and acknowledged by employees.

The Rules of Behavior (PRRB-1 and PL-4) are a set of rules that describe the IA operations of the information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. In order to be compliant, it must be required that the rules contain a signature page for each user to acknowledge receipt, indicating that they have read and understand, and agree to abide by the rules of behavior. Electronic signatures are acceptable for acknowledgement. Rules of behavior must be signed as a condition of access to the information system(s).

"Rules of behavior are a set of rules that describe the IA operations of the information system and clearly delineate IA responsibilities and expected behavior."

Agencies and organizations have flexibility in the detail and contents however topics in the Rules of behavior should include (but are not limited to the following):

- **Work at home**

- **Dial-in Access**

- **Connections to the internet**

- **Use of copyrighted work**

- **Unofficial use of government equipment**

- **Assignment and limitations of system privileges and individual accountability**

- **Password Usage**

- **Searching databases and divulging information**

- **Other topics, as appropriate**

When developing a rules of behavior, keep in mind that the intent is to make all users accountable for their actions by acknowledging that they have read, understand, and agree to abide by the rules of behavior. The rules should not be a complete copy of the security policy or procedures guide, but rather cover, at a high level the topics listed above.

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).
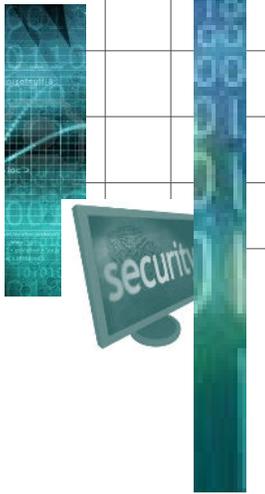
DIACAP Fundamentals (One-day)	DIACAP In-Depth (Three-day)
26 Sep 2011 (CS)	27-29 Sep 2011 (CS)
17 Oct 2011 (H)	18-20 Oct 2011 (H)
24 Oct 2011 (NCR)	25-27 Oct 2011 (NCR)
31 Oct 2011 (SD)	1-3 Nov 2011 (SD)
7 Nov 2011 (ANA)	8-10 Nov 2011 (ANA)
5 Dec 2011 (NCR)	6-8 Dec 2011 (NCR)

FISMA RMF Fundamentals (One-Day)	FISMA RMF In-Depth (Three-Day)
3 Oct 2011 (DC)	4-6 Oct 2011 (DC)
14 Nov 2011 (DC)	15-17 Nov 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.