Risk Management Framework Today

Formerly DIACAP Dimensions

… and Tomorrow

January 2017
Volume 7, Issue 1

In this issue:

RMF and the Cloud

By P. Devon Schall

Probably the most talked-about concept in information technology today is cloud computing, often simply called "The Cloud."

According to the National Institute of Standards and Technology (NIST), cloud computing is "a model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

For the past few years, departments and agencies across the government have been aggressively pursuing "migration" of systems and applications to the cloud in order to save money and "deliver public value" by increasing operational efficiency.

Moving away from traditional data centers and into the cloud provides a variety of challenges, particularly in the area of information security landscape.

In a survey recently conducted amongst IT professionals, the top three rated cloud issues were security, availability, and performance. These concerns impact the level of trust consumers have with their data existing in a cloud environment.

The top seven cloud security risks and summaries as published by Cloud Security Alliance are listed below:

- Privileged user access. Sensitive data processed outside the enterprise brings with it an inherent level of risk
- Regulatory compliance. Cloud computing providers may be hesitant to undergo external audits and security certifications
- Data location. The customer probably doesn't know exactly where their data is hosted
- Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers creating confidentiality concerns
- Recovery. A cloud provider should be able to tell what will happen to the data and service in case of a disaster
- Investigative support. Investigating inappropriate or illegal activity may be more difficult in the cloud computing environment
- Long-term viability. Data and logging should remain available even after services are discontinued

The federal government has taken steps to mitigate these risks and concerns in order to facilitate cloud migration without compromising security.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services. FedRAMP utilizes a baseline set of agreed-upon standards and includes independent evaluation of cloud service providers by authorized Third Party Assessment Organizations (3PAOs).

Sounds an awful lot like the Risk Management Framework (RMF), doesn't it? In fact, the "baseline set of standards" used by FedRAMP is derived from the very same "security controls catalog" used in RMF.

In the DoD world, the Defense Information Systems Agency (DISA) has established its own cloud authorization

See *RMF and the Cloud*, Page 2

Training Opportunities are Expanding

By Alice Steger

Ever since the "birth" of RMF by NIST in 2010, BAI has been a provider of training to government agencies and their industry partners. As adoption of RMF has spread across the government, and beyond, our training offerings have evolved accordingly. Now, in 2017, another significant expansion of BAI training programs is underway. Here are some of the highlights:

New classroom location—Orlando

In addition to our "traditional" classroom locations in Colorado Springs, Huntsville and National Capital Region (Pentagon/Crystal City area), and our Online Personal Classroom™ training, we will now be offering training in the Orlando, FL area, with *RMF for DoD IT* classes beginning in June, 2017.

Friday Supplemental classes

We will be introducing a series of one-day classes to supplement our four-day *RMF for DoD IT* training program. These classes will initially be offered to organizations planning "on-site" training. Options include:

- eMASS Workshop
- Continuous Monitoring Overview
- Certified Authorization Professional (CAP) exam preparation

Certified Cloud Security Professional (CCSP) Training

Like most of the IT world these days, security professionals are keenly interested in cloud computing. Accordingly, BAI will be launching a five-day training program that will provide guidance in securing systems and applications in the cloud environment, as well as preparing students to take the CCSP certification exam given by ISC2 (www.isc2.org). Training will begin with an online class in April, followed by a class in the National Capital Region (Pentagon/Crystal City area) in June.

Need more information? Call us at 1-800-RMF-1903 or visit www.rmf.org.

"What is the relationship between RMF and the Cloud? It depends on your perspective ..."

***RMF and the Cloud* from Page 1**

program that is essentially an enhanced version of FedRAMP.

Numerous resources exist to support these efforts. The Cloud Computing Security Requirements Guide published by NIST is an invaluable resource in reviewing and ensuring adequate system hardening. DISA Security Technical Implemental Guides (STIGs) are also utilized to verify the risk and threats listed above mitigated.

What is the relationship between RMF and the Cloud? It depends on your perspective.

Cloud computing service providers such as Amazon GovCloud typically undergo an RMF-like authorization process such as FedRAMP or the DISA cloud authorization process. This results in formal authorization by the government, very similar to the RMF Authorization to Operate (ATO). Typically this authorization will include a suite of inheritable controls.

Application owners developing new software for deployment to the cloud, or those migrating existing applications from government data centers to cloud service providers, will follow the normal RMF life cycle leading to ATO. The process will be facilitated by inheritance of controls from the cloud service provider. Typically, control families such as Physical and Environmental, Media Protection and Maintenance can be inherited by the application owner.

Top Ten—Documentation Recommendations

By Lon J. Berman, CISSP

Supporting documentation (aka. artifacts) is key to providing evidence of compliance with security controls. Previously in this Newsletter we have spent some time describing the three fundamental classes of RMF documentation, to wit:

- Policy. Policy documents describe what the organization does to provide for confidentiality, integrity and availability of systems information. In short, a policy document says "This is what we do."

- Procedure (SOP). Procedure documents describe how the various security features are implemented, in other words, "This is how we do it."

- Assurance. Assurance documents provide evidence that the SOPs are actually being carried out; in other words, "See? We're actually doing it!"

With that background, here is our Top Ten list of documentation recommendations.

10. Where feasible, make use of a document management system with version control, check-in/out, etc.

9. Do not write SOPs "in a vacuum." Be sure to engage with the people who actually carry out the procedures being documented.

8. Re-use existing documentation to the greatest extent possible. There's no need to write a brand new Incident Response Plan "from scratch" if you've already got one; just make the necessary additions to ensure all the RMF controls are covered.

7. Do not be concerned with *how many* documents you create. So long as the numerous controls/CCIs are covered, it does not matter if you have one document or 100!

6. Obtain management signatures where appropriate. Policy documents should always be signed by organizational management. Key procedural documents (such as Contingency and Incident Response Plans) should likewise be signed as evidence of "management buy-in."

5. Make sure all documentation is carefully reviewed and proofread. Errors in spelling and grammar will reflect poorly on the system owner. No need giving this sort of "negative vibe" to the independent assessors.

4. Make sure only the "latest and greatest" version of each document is provided to the assessor.

3. Include a "Change Log" with each policy and procedure document. This makes it easy to document ongoing document reviews and updates, which should be a key part of your continuous monitoring activities.

2. Make sure documents are properly assessed for information sensitivity (consult the organization's Classification Guide as necessary). Unclassified documents should have appropriate information sensitivity marking (e.g., FOR OFFICIAL USE ONLY) on the cover and on each page's top or bottom margin. For classified documents, be sure to follow marking requirements per DoD Instruction 5200.01.

1. Make sure document content is clearly traceable to the controls/CCIs being covered. This can be done with an index or table within each document or references loaded into eMASS or other support tool. One way or the other, the assessor needs to be able to clearly locate each CCI in a policy, a procedure, and, where applicable, an assurance document.

Security Control Spotlight—Training

By Kathryn M. Daily, CISSP

In this issue we will shine the spotlight on the Awareness and Training (AT) family of security controls. We'll show you how the controls dictate the types and frequencies of training that organizations must provide. You'll also learn about the extent to which existing DoD publications provide system owners with "automatic compliance."

Those familiar with DIACAP may recall there was a single control, PRTN-1 (entitled "Information Assurance Training") in the Personnel area, that covered most aspects of training. Additionally, a control in the Physical and Environmental area, PETN-1, covered training on environmental controls.

With RMF, there are a total of 7 security controls and control enhancements in the AT family, to wit:

- AT-1 Security Awareness and Training Policy and Procedures
- AT-2 Security Awareness Training
- AT-2(2) Security Awareness—Insider Threat
- AT-3 Role-based Security Training
- AT-3(2) Security Training—Physical Security Controls
- AT-3(4) Security Training—Suspicious Communications and Anomalous System Behavior
- AT-4 Security Training Records

"With RMF, there are a total of 7 security controls and controls enhancements in the AT family..."

It is interesting to note that all 7 of these controls are applicable to all system categorization levels.

The two most commonly-used overlays (Classified Information Overlay and Privacy Overlay) retain the same 7 controls/enhancements, however they also add some extensions and statutory references to these controls. For example, the Classified overlay extends the training requirement to include specific training on classified information handling and consequences of unauthorized disclosure.

These 7 security controls and control enhancements break down into a total of 29 Assessment Procedures (CCIs). And … big surprise! … 19 out of the 29 CCIs are considered "Automatically Compliant" by DoD, by virtue of the existence of DoD Directive 8570.01 (or it's replacement, DoD Directive 8140).

That leaves the system owner with just these 10 CCIs to implement and document:

- Refresher role-based training (CCIs 000109 and 000110)
- Physical security controls training (CCIs 002051, 001566, 001567)
- Malicious code training (CCIs 002054, 002054)
- Training records (CCI 000113)
- Monitoring individuals' training (CCI 000114)
- Retention of training records (CCI 001336)

The independent assessor is expected to carefully review the organization's training records to ensure the procedures in the DoD publication (8570/8140) are being properly implemented.

Training for Today … and Tomorrow

Our training programs:

- **RMF for DoD IT** – recommended for DoD employees and contractors that require detailed RMF knowledge and skill training; covers the new RMF life cycle 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 (non-DoD) employees and contractors; 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)** – open to all, however prior knowledge of RMF is recommended. This is a three day "In Depth" program.
- **Certified Cloud Security Professional (CCSP)** – recommended for government employees and contractors working (or planning to work) in the cloud environment, this four-day training program will prepare students for the CCSP certification examination given by ISC2

Our training delivery methods:

- **Traditional classroom** – regularly-scheduled training programs are offered at various locations nationwide, including Colorado Springs, Huntsville, National Capital Region (Pentagon/Crystal City area), and Orlando
- **Online Personal Classroom™** – regularly-scheduled training programs are also offered in an online, instructor-led format that enables you to actively participate from the comfort of your home or office
- **On-site training** – our instructors are available to deliver any of our training programs to a group of students from *your* organization at *your* site; please contact BAI at 1-800-RMF-1903 to discuss your requirements

Regularly-scheduled classes through June, 2017:

RMF for DoD IT—4 day program (Fundamentals and In Depth)

- **23-27 JAN 2017 (National Capital Region and Online Personal Classroom™)**
- **27 FEB-2 MAR 2017 (Huntsville and Online Personal Classroom™)**
- **20-23 MAR 2017 (Colorado Springs)**
- **27-30 MAR 2017 (Online Personal Classroom™)**
- **10-13 APR 2017 (National Capital Region)**
- **17-20 APR 2017 (Online Personal Classroom™)**
- **8-11 MAY 2017 (Huntsville)**
- **15-18 MAY 2017 (Online Personal Classroom™)**
- **12-15 JUN 2017 (Colorado Springs)**
- **19-22 JUN 2017 (Online Personal Classroom™)**
- **26-29 JUN 2017 (Orlando)**

RMF for Federal Agencies—4 day program (Fundamentals and In Depth)

- **22-25 MAY 2017 (Online Personal Classroom™)**

Information Security Continuous Monitoring—3 day program (In Depth class only)

- **11-13 APR 2017 (Online Personal Classroom™)**

Certified Cloud Security Professional (CCSP)—5 day program

- **3-7 APR 2017 (Online Personal Classroom™)**
- **26-30 JUN 2017 (National Capital Region)**

Registration for all classes is available at https://register.rmf.org

Payment arrangements include credit cards, SF182 forms, and Purchase Orders.

Contact Us!

RMF Today … and Tomorrow is a publication of BAI Information Security, Fairlawn, Virginia.

Phone: 1-800-RMF-1903
Fax: 540-808-1051
Email: rmf@rmf.org