Risk Management Framework Today

Formerly DIACAP Dimensions

… and Tomorrow

September, 2016
Volume 6, Issue 3

In this issue:

Understanding the Authorization Decision	1
Which RMF Training Delivery Model is Right for Me?	2
Top Ten-RMF Pitfalls Revisited	3
Security Control Spotlight—Contingency Planning	4
Training for Today… and Tomorrow	5

Understanding the Authorization Decision

By Lon J. Berman, CISSP

If you ask most system owners about the desired outcome of their RMF efforts, they will readily tell you "we are expecting the Authorizing Official (AO) to sign an Authorization to Operate (ATO) for our system." But how much do they *really* know about what goes into that decision? Do they understand that ATO is not the only possible outcome of the authorization process? What are the other possible authorization decisions and what do they mean to the system owner?

To truly understand authorization decisions, you need to understand the decision process itself. In Step 5 of the RMF process, the AO is presented with an Authorization Package that contains, at a minimum, a System Security Plan (SSP), a Security Assessment Report (SAR) and a Plan of Action & Milestones (POA&M).

- The SSP includes a comprehensive system description, documentation of roles and responsibilities, system categorization, and complete documentation of the implementation and status of each applicable security control in the system baseline.
- The SAR is provided by the Security Controls Assessor (SCA) and contains the results of the independent assessment of the system; each control is assessed as being Compliant (C), Non-compliant (NC), or Not Applicable (NA).
- The POA&M contains the system owner's "response" to the findings of the independent assessment (planned mitigation/remediation steps, resources and schedule).

Additionally, the AO may be provided with a Risk Assessment Report (RAR) that assigns a Risk Level (Very Low, Low, Moderate, High, Very High) to each finding, along with an overall recommendation from the SCA.

The AO will then analyze the risk posture of the system, as indicated by these documents. Some of the questions the AO will ask him/herself are:

- Is the system capable of operating at an acceptable level of risk *today*?
- Does the system owner, as evidenced by the POA&M, have a credible plan to address risks identified in the independent assessment?

Based on this analysis, the AO needs to decide if the overall system risk is *acceptable*. The very nature of the word "acceptable" indicates this will be a *subjective* decision on the part of the AO.

If the AO feels the overall risk is acceptable and there are no Very High or High risk findings, he/she will issue an ATO. Each ATO includes an Authorization Termination Date (ATD). The overall term of the ATO cannot exceed three years. During the term of the ATO, the system owner is required to maintain and report on the security posture of the system. At a minimum, this entails providing an updated POA&M to the AO on a quarterly basis. A new ATO must be obtained on or before the ATD (see Note below).

If there are Very High or High risk findings, but the AO deems the risk acceptable due to a compelling need to put the system into operation, an ATO with Conditions can be issued. Typically, an ATO with Conditions is given for a time period of six months or less, and highlights the specific high risk items that need the system owner's attention. In order to issue an ATO with Conditions, the AO must obtain approval from the

See *Authorization Decisions*, Page 2

Which RMF Training Delivery Model is Right for Me?

By Annette Leonard

You know your organization needs RMF training, but you're not sure which "delivery model" will best serve your needs. Here we present some of the considerations that can help you decide.

Regularly-scheduled classroom training
RMF training is available monthly, on a rotating basis, in our classrooms in Colorado Springs, Huntsville and National Capital Region (Pentagon/Crystal City area). Classroom training provides a distraction-free learning environment that is optimal for many students. The downside is of course the additional expense of travel if the student doesn't happen to be local to the classroom site.

Regularly-scheduled online training
Online, instructor-led training is also available on a monthly basis. The major advantage is the removal of travel costs from the equation. Many students do learn well in this environment, but for some, it is difficult to balance the learning experience with the usual "in-office" distractions.

On-site (or online) "private class"
Our instructors are available to travel to your site and provide RMF training. The main advantage is a lower "per student" cost. The disadvantage is having to put all your personnel in training at the same time. Optionally, customization of the course curriculum (at additional cost) is available to optimize the training for your organization.

Please contact BAI at 1-800-RMF-1903. We can help you find the optimal training solution for your organization.

Authorization Decisions **from Page 1**

DoD Component CIO. Note that the ATO with Conditions is similar in some respects to the Interim Authorization to Operate (IATO) that was given under DIACAP.

If the AO feels the system risk is unacceptable for *any* reason, a Denial of Authorization to Operate is issued. DATO will prevent a new system from going into operation. For an existing system, DATO requires operation to be halted.

In the special case where a system requires certain testing to be done in an operational environment, an Interim Authorization to Test (IATT) can be sought. IATTs are typically given for a short period of time to permit functional testing in a "live" environment. Most DoD components have some sort of expedited process for obtaining IATT. Such a process will include, at a minimum, a comprehensive test plan provided by the System Owner, along with evidence of testing to ensure other systems or networks will not be at undue risk during the "live" testing period.

The AO is expected to "publish" the authorization decision in the form of a signed document or e-mail message. If an enterprise tool such as eMASS is being used, the authorization decision document will be uploaded to the system's artifacts repository and the authorization status updated accordingly.

NOTE: In the future, DoD is expected to support the concept of *Ongoing Authorization*, in which the AO is given the flexibility to "extend" a system's ATO based on the success of the System Owner's Continuous Monitoring program. DoD is expected to publish a Continuous Monitoring Policy and SOP in the near future that will lay out the guidelines for this approach. Needless to say, many System Owners are anxiously awaiting the publication of this policy, with the hope that it can reduce or eliminate the cost and disruption of re-authorization activities. Stay tuned……..

"In the future, DoD is expected to support the concept of Ongoing Authorization ..."

Top Ten—RMF Pitfalls Revisited

By Lon J. Berman, CISSP

Like any complex process, RMF is not without its share of potential pitfalls. In previous issues of *RMF Today … and Tomorrow* we highlighted some of those "gotchas" and suggested ways of avoiding them.

Now that we have the benefit of some more RMF projects under our belt, we thought it was time for a "revisited edition" of the RMF Top Ten Pitfalls.

10. Assuming system boundaries have remained the same. While transition from DIACAP to RMF will not in itself cause system boundaries to change, it is critical to *confirm* the system boundary before beginning the RMF process.

9. Assuming roles and responsibilities have remained the same. RMF transition certainly changes the *names* of some key roles (e.g., DAA is now AO), but, beyond that, it's important to confirm the individuals' names. Many organizations are using the RMF transition as a opportunity to also assign new people to many roles.

8. Assuming system categorization will be easy. System categorization is a *major task*, involving information owners and system owners, as well as cybersecurity personnel. Be sure to allow sufficient time to get it right!

7. Assuming security control inheritance will be straightforward. Inheritance from common control providers such as DoD data centers involves close coordination and attention to detail. Inheritance from commercial cloud providers can be even more challenging.

6. Failing to consider security control overlays. Failure to properly account for security control overlays can cause critical security controls to be missed. The Privacy Overlay requires particularly close attention because it entails an additional "categorization" step.

5. Underestimating the lead time required for independent assessment. RMF assessor teams are busier than ever. Be sure to make contact early to ensure timely service and avoid overall project delays.

4. Expecting too much out of existing documentation artifacts. RMF controls are much more detailed about what needs to be present in the various documentation artifacts (e.g., Incident Response Plan). Do not assume all the controls are covered just because you already have an artifact by that name.

3. Underestimating the training required. It takes specialized knowledge and skill to successfully navigate the RMF process, understand the controls, etc. Training can get your staff "up to speed" quickly.

2. Underestimating the time required. It is critical to be realistic about the time required to get through the RMF process. It is absolutely appropriate to get started *one year* prior to the required date, even for an already accredited system.

1. Underestimating the resources required. The biggest single pitfall is underestimating the resources required to successfully execute the RMF process. The required resources span a variety of skill sets, to wit:

- Security analysts (to understand the controls and assessment objectives)
- System engineers (to plan for implementation of technical controls)
- Technical writers (to develop and/or revise system documentation artifacts)
- Data entry personnel (to enter information into an RMF support tool such as eMass)

… and more!

Security Control Spotlight—Contingency Planning

By Kathryn M. Daily, CISSP

In this issue we will shine the spotlight on the Contingency Planning (CP) family of security controls. First, we'll show you how the controls dictate the subject areas that need to be addressed in the organization/system's disaster recovery and business continuity plans. Second, you'll learn how the contingency planning requirements become more stringent as the system categorization level increases.

Those familiar with DIACAP probably recall the contingency planning requirements were included in a subject area known as Continuity (control names beginning with CO). There were only a small number of controls in the CO group, and most of them were fairly high-level.

With RMF, the contingency planning controls are numerous and quite explicit. For example, CP-2 contains the basic requirements for the organization's contingency plan, to wit:

"With RMF, the contingency planning requirements are numerous and quite explicit..."

The organization:

a. Develops a contingency plan for the information system that:

1. Identifies essential missions and business functions and associated contingency requirements;

2. Provides recovery objectives, restoration priorities, and metrics;

3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];

b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];

e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and

g. Protects the contingency plan from unauthorized disclosure and modification.

In addition to the baseline CP-2 control, there are numerous control enhancements that provide even more prescriptive requirements for the organization's contingency planning.

Control CP-7 contains the Recovery Time Objective (RTO) for the system. In the NIST SP 800-53, this is an "organization-defined value," however DoD has specified minimum acceptable values, based on the system categorization:

- For systems categorized as Availability Moderate, the RTO must be 12 hours or less
- For system categorized as Availability High, the RTO must be 1 hour or less

It should be noted that DoD does not specify a maximum RTO for systems categorized as Availability Low. For such systems, it is up to the system owner to determine an appropriate RTO through its Business Impact Analysis.

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

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 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 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)** – open to all, however prior knowledge of RMF is recommended. This is a three day "In Depth" program.

Regularly-scheduled classes through December, 2016 are as follows:

RMF for DoD IT (Fundamentals and In Depth)

- **19-22 SEP 2016 (Online Personal Classroom™)**
- **3-6 OCT 2016 (National Capital Region)**
- **17-20 OCT 2016 (Online Personal Classroom™)**
- **14-17 NOV 2016 (Huntsville)**
- **14-17 NOV 2016 (Online Personal Classroom™)**
- **5-8 DEC 2016 (Colorado Springs)**
- **12-15 DEC 2016 (Online Personal Classroom™)**

RMF for Federal Agencies (Fundamentals and In Depth)

- **PLEASE CALL**

Information Security Continuous Monitoring (In Depth class only)

- **PLEASE CALL**

2017 training dates coming soon! See register.rmf.org for details.

Online registration and payment is available at **http://register.rmf.org**. Payment arrangements include credit cards, SF182 forms, or purchase orders. For the most up-to-date training schedule, pricing information, and any newly-added class dates or locations, please visit **http://register.rmf.org**.

Classroom training. We offer regularly-scheduled classroom training at our training centers in Colorado Springs, Huntsville, National Capital Region* (Washington, DC area) and Virginia Beach. **Note our new National Capital Region location in the Pentagon/Crystal City area.*

Online Personal Classroom™ training. This method enables you to actively participate in our regularly-scheduled instructor-led classes 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 and a suitable classroom or conference room. Cost is dependent upon class size, so please contact us at 1-800-RMF-1903 (763-1903) to request an on-site training quotation.
Note: we can also provide Online Personal Classroom™ training to a "private" group of students from *your* organization.