Risk Management Framework Today...

and Tomorrow

In this issue:

Do I really need four-day live instructor-led RMF Training?
Why Free Online RMF Training Isn't Enough ……………………………………1

RMF Across the Government Landscape ……………………………………..2

Risk. What to Do With It. ……………………………………..3

Ask Dr. RMF ……………………………………..5

Training for Today… and Tomorrow. ……………………………………..6

Find us on LinkedIn

BAI Information Security Consulting & Training

April, 2021 Volume 11, **Issue 2**

Do I really need four-day live instructor-led RMF Training?

Why Free Online RMF Training Isn't Enough

By Philip D. Schall, Ph.D., CISSP, RDRP

At BAI RMF Resource Center, we often have conversations with our students on the topic of taking formal classroom RMF training. In the modern digital landscape, we are able to learn about and complete projects we never thought possible twenty years ago through free online resources. The internet has enabled us to learn so much with a few keystrokes, but as much as I hate to break the news to you, RMF has historically not been a topic that can be learned easily or successfully through self-study via free online resources.

After collecting data over the past three years in my RMF research, the consistent pattern I have seen from respondents are RMF practitioners stressing the importance of receiving formalized RMF classroom training and how much easier it is to complete RMF packages when proper training has been received. This data has been validated with statistical significance in a research study scheduled for publication this summer. Stay tuned!

Some major challenges with self-directed RMF education are:

Thousands of pages of NIST guidance and RMF policy being very overwhelming for those new to the RMF process and interpreting government policy. See https://rmf.org/rmf-publications/ and NIST Special Publications (SP) for examples.

RMF policy and the intricacies of NIST policy can be very confusing. Having someone available to answer your questions and guide you in real-time can save you an enormous amount of time vs. the alternative of Google and Reddit research. Also, the information you may find on online forums may not be the most up to date guidance due to policies being updated and changing regularly.

The most valuable element of BAI's RMF training is the hands-on consulting experience of our instructors. This real-world experience is invaluable. Unfortunately, RMF policy does not always translate well from the policy wonks to real-world policy application. We understand these nuances and can provide you solutions and assistance from our RMF consulting experiences.

I understand we are all very overwhelmed with work priorities, and we are looking for whatever shortcuts we can find to boost efficiency and productivity, but it has been BAI's experience that this increased efficiency and productivity can be achieved from an RMF standpoint by committing to a four-day RMF full course. We often see that students who try to self-teach or take shortcuts end up spending months posing questions to our own Dr. RMF and trying to digest hundreds of pages of NIST documentation alone.

As BAI's training leader, I highly encourage any student who may be questioning if RMF training is truly necessary to consider the value RMF live instructor-led training delivered by a seasoned RMF practitioner. BAI also offers former students access to programs such as TrainPlus™ which provides a support lifeline for when former students may find themselves stuck in an RMF predicament. Please allow BAI RMF Resource Center to educate you and guide you through the RMF journey by attending our flagship four-day RMF full course training program. RMF is who we are!

Risk Management Framework Today…

and Tomorrow

> ***"Almost all departments and agencies have adopted the key RMF publications, such as NIST SP 800-37. They have then adapted this guidance into their own departmental or agency-level policy."***

BAI Information Security Consulting & Training

RMF Across the Government Landscape

By Lon J. Berman, CISSP, RDRP

More than ten years ago, RMF came into existence with the intention of becoming the "unified information security framework for the federal government". With widespread adoption of RMF throughout most federal civil agencies, DoD components and intelligence community agencies, it is safe to say that goal has been met. However, it is important to understand that while RMF is a *unified* information security framework, it is not a 100% *uniform* information security framework. There are differences … some significant and others subtle … in the way RMF has been put into practice in the various departments and agencies.

Almost all departments and agencies have *adopted* the key RMF publications, such as NIST SP 800-37. They have then *adapted* this guidance into their own departmental or agency-level policy. This article will highlight some of the adaptations that we see across the government landscape.

RMF Roles and Responsibilities. One of the key areas of adaptation is the appointment of the Authorizing Official (AO). Many agencies appoint a single AO to be responsible for issuing and monitoring the Authorization to Operate (ATO) for all systems within the agency. Smaller agencies that don't have a large number of systems are the most frequent ones to have a single AO, but there are large organizations, such as the US Navy, that have also embraced this approach. In the case of a large agency with a single AO, the AO will typically have a large staff to handle most of the mechanics of the authorization process. Many large organizations have multiple AOs to cover the various mission areas and programs.

System Registration. Most government organizations handle RMF system registration under the larger umbrella of IT Portfolio Management. Each department or agency has its own database for this purpose, and its own process for creating and updating records in that database.

System Categorization. NIST SP 800-37 specifies each system will be categorized as having a security impact level of High, Moderate or Low, using the categorization process delineated in Federal Information Processing Standard (FIPS) 199. However, systems designated as National Security Systems (NSS) are categorized in a different fashion, following the process delineated in Committee on National Security Systems Instruction (CNSSI) 1253. NSS are categorized as High, Moderate or Low for *each* of the three principal security objectives: Confidentiality, Integrity and Availability. That's how it plays out in most departments/agencies, however DoD is a notable exception – *all* systems, both NSS and non-NSS, are categorized in accordance with CNSSI 1253.

Security Controls and Overlays. Each department and/or agency may have its own unique set of overlays. Most overlays add security controls to the baseline to deal with specific types of systems (e.g., industrial control systems) or specific information content (e.g., classified information, privacy information).

Assessment. Each department and/or agency will have its own approach regarding independent assessment (RMF Step 4). Some will maintain a dedicated staff of assessors to perform system assessments, while others rely on system owners to conduct self-assessments which are then reviewed by a staff assessor.

Automation Support. Many departments and/or agencies have standardized on an automated tool that is used by system owners to document their compliance with baseline controls,

See Gov Landscape, Page 4 for more.

Risk. What to Do With It.

By Kathryn Daily, CISSP, CAP, RDRP

Recently our regional grocery store chain notified their employees and customers that they had a data breach involving some HR data and pharmacy records. The breach was caused by a vulnerability in the Accellion file-sharing system which the grocery chain immediately stopped using. As I was perusing the comments on the news article about the breach many were placing the breach solely at the foot of the grocery chain and completely ignoring the vendor that *actually caused* the breach in the first place. What they failed to understand is that you cannot eliminate all risk.

There is not an IT system out there that does not have some type of risk that comes with it. As RMF practitioners, we are tasked with identifying, and managing the risk to our systems. The NIST Special Publication 800-39 outlines how federal agencies should manage risk to federal IT systems with a 4-step process: i) Framing Risk; ii) Assessing Risk; iii) Responding to Risk; and iv) Monitoring Risk. Today we are going to focus on step 3 and discuss ways to respond to the risk identified in the risk analysis.

> ***"There is not an IT system out there that does not have some type of risk that comes with it. As RMF practitioners, we are tasked with identifying, and managing the risk to our systems."***

Keep in mind that one should be doing a risk analysis on external vendors as well as their own systems so you should be able to quantify the entire risk picture for your system assuming you understand the security mechanisms in place for those vendors. It is entirely possible that the vendor considers their security mechanisms as confidential information and will not share them. That should be noted as a risk to your own system when choosing to use that vendor.

So, we have identified our risk. Now what? As outlined in the NIST SP 800-39 we have five choices for risk response, to wit: i) Risk acceptance; ii) risk avoidance; iii) risk mitigation; iv) risk sharing; and v) risk transfer.

<ins>Risk Acceptance:</ins> With risk acceptance you have essentially accepted that the risk exists and through risk analysis determined that it is not worth the resources to remediate. This might be a financial decision, or it might be based on impact, or even a combination of the two. If your identified risk is building damage from a hurricane, but you're located in Wyoming, you can probably categorize that as a low risk, and it does not make much sense from a cost/benefit standpoint to build the building to withstand a hurricane. If you are on the coast of Florida, that changes the entire perspective on this particular risk. In our grocery store example with the data including pharmacy and HR (likely PII) information risk acceptance is not a likely choice here.

<ins>Risk Avoidance:</ins> With risk avoidance you are in effect saying the identified risk exceeds your organizational risk tolerance. The grocery chain could have determined in their risk management process that the risk of storing PHI and PII with an external vendor was too high and they could have created a proprietary file sharing capability that they could use to control the security internally, assuming they have the personnel who are competent security practitioners.

<ins>Risk Mitigation:</ins> With risk mitigation you are reducing the risk to an acceptable level through the implementation of security controls. With federal information systems we mitigate risk with the 800-53 catalog of security and privacy controls. For private industry, they can also use the 800-53 control set, or they can use another framework to secure their IT systems. The grocery chain could mitigate the risk of the external service provider by selecting a vendor that has an ISO 27001 certification indicating that they have been vetted by an independent auditor to have a risk mitigation plan in place.

See Risk, Page 4 for more.

BAI Information Security Consulting & Training

Gov Landscape, from Page 2

store and index documentation artifacts, record test results, etc. For most DoD agencies and a few outside DoD, the government-owned Enterprise Mission Assurance Support Service (eMASS) is the tool of choice. Commercial RMF tools such as Telos Corporation's Xacta are employed in various departments and agencies across the government landscape. Still other organizations have built their own tool or database to collect RMF information.

The lesson learned here is that while RMF is largely the same across the government, there are numerous unique features in each department/agency's implementation. If you are responsible for creating or maintaining an RMF package, be sure you engage with the owning organization's Information System Security Manager (ISSM) to obtain the RMF policies and guidance relevant to that organization.

Risk, from Page 3

Risk Sharing: With risk sharing you are distributing the liability to multiple organizations. The grocery store chain may decide to give the HR data to one service provider and the pharmacy information to another service provider. In this risk sharing model, the liability is limited because a breach with one provider would only effect half of the data.

Risk Transfer: In the risk transfer methodology you are putting all the risk on another entity. Insurance is a common means of risk transfer for financial risk considerations. If the grocery store chain purchased cyber liability insurance, they could essentially protect themselves from the financial repercussions of the data breach. It does not do much for the individuals who's PII and PHI have been compromised but it does protect the organization from a financial perspective and may cover things such as lawsuits or the cost of credit monitoring for effected individuals.

As you can see, there are several options for addressing the risk you have identified in your risk analysis. While the NIST SP 800-39 gives you a process for managing that risk, it is up to your team of security practitioners to look at each risk and analyze the impact and the likelihood of occurrence to determine what risk response methodology best fits each identified risk.

For more information on managing risk in DoD and Federal organizations, check out our 4-day Risk Management Framework course options.

> ***"While the NIST SP 800-39 gives you a process for managing that risk, it is up to your team of security practitioners to look at each risk and analyze the impact and the likelihood of occurrence to determine what risk response methodology best fits each identified risk."***

Possible Risks
1422. Alien Invasion
1423. City destroyed by angry Monkey God
1424. Building eaten by giant pig.
SMC

"Well he certainly does a very thorough risk analysis."

Figure 1: The risks identified in the cartoon can safely be categorized as low.

Risk Management Framework Today…

and Tomorrow

"...the Army is preparing to update their RMF policies and procedures to include something called a "Continuous ATO". This is part of a larger effort they are calling "RMF Sentinel" or "RMF 2.0". They will now be allowing Authorizing Officials (AOs) to "extend" ATOs based on the success of the system owner's continuous monitoring activities."

Ask Dr. RMF

Do you have an RMF dilemma that you could use advice on how to handle? If so, Ask Dr. RMF! BAI's Dr. RMF consists of BAI's senior RMF consultants who have decades of RMF experience as well as peer-reviewed published RMF research

Dr. RMF submissions can be made at https://rmf.org/dr-rmf/.

Troy with DoD writes:

We have a boundary that we are assessing and within the boundary we have multiple controls that speak to "Alternate site". It was deemed that we could not have an alternate site, due to lack of funding and the way our architecture is configured it would not be cost effective. So my question is should these controls be marked Non-compliant and risk accepted, or Not Applicable?

Dr. RMF responds:

You raise an interesting question here, Troy. One of the cornerstones of RMF is the ability to tailor the security control baseline to best fit the needs of the organization and the system. Since your organization has made a design decision to not deploy an alternate processing site, you could potentially make a case for declaring any alternate site-related controls as Not Applicable. That said, Dr. RMF recommends against taking this approach. In our experience, your assessor is likely to frown upon tailoring out the alternate site controls, especially if your system is categorized as Moderate or High for Availability.

Dr. RMF recommends leaving the alternate site controls in your baseline and marking them as Non-compliant. They will then need to be put in your POA&M and annotated as Risk Accepted. Further, Dr. RMF recommends you obtain a signed letter from your Authorizing Official confirming his/her decision not to deploy an alternate site. If possible, the letter should also include mitigating factors that lessen the risk, such as redundancy built into the primary site or potential workarounds if the primary site becomes unavailable.

Jack with US Army writes:

I've been hearing rumors that DoD may be moving away from requiring systems to get a new ATO every three years. Is there any truth to that? If so, how do we get our systems approved for a longer-term ATO?

Dr. RMF responds:

Jack, thank you for submitting this very pertinent question. The concept of "Continuous Authorization" has been around for quite a while. NIST Special Publication 800-37 Rev 2 describes it in detail, but it has found little or no traction within DoD until very recently.

Case in point: the Army is preparing to update their RMF policies and procedures to include something called a "Continuous ATO". This is part of a larger effort they are calling "RMF Sentinel" or "RMF 2.0". They will now be allowing Authorizing Officials (AOs) to "extend" ATOs based on the success of the system owner's continuous monitoring activities. For example, they are requiring STIG Checklists and ACAS Scans to be periodically uploaded into the eMASS record as evidence of continuous monitoring. Also, RMF Sentinel will include a Common Control Provider that will offer numerous additional controls for inheritance. RMF Sentinel is very much a "work in progress", so Dr. RMF recommends you contact your AO or Program ISSM for further information.

Dr. RMF expects to see similar activities coming from other DoD components in the near future.

Risk Management Framework Today…

and Tomorrow

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 RMF life cycle, documentation, and security controls.
- **RMF Supplement for DCSA Cleared Contractors** – covers the specifics of RMF as it applies to cleared contractor companies under the purview of the Defense Counterintelligence and Security Agency (DCSA). Companies holding a Facility Clearance who also maintain "on premise" information technology (such as standalone computers and small networks) will benefit from this training.
- **DFARS Compliance with CMMC/NIST SP 800-171 Readiness Workshop**—provides detailed practical application based DFARS training that will help DoD contractors work through DFARS requirements towards certification in the most efficient means possible.
- **eMASS eSSENTIALS** – provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS is exemplified in our eMASS eXPERIENCE™ simulation environment.
- **STIG 101** – is designed to answer core questions and provide guidance on the implementation of DISA Security Technical Implementation Guides (STIGs) utilizing a virtual online lab environment.
- **Security Controls Implementation Workshop** – provides an in-depth look into Step 3 of the Risk Management Framework process Implement Security Controls. Upon completion of the course the student can confidently return to their respective organizations and ensure the highest level of success for the most difficult part of the RMF process.
- **Security Controls Assessment Workshop** – provides a current approach to evaluation and testing of security controls to prove they are functioning correctly in today's IT systems.
- **Information Security Continuous Monitoring** – equips learners with knowledge of theory and policy background underlying continuous monitoring and practical knowledge needed for implementation.
- **RMF in the Cloud** – provides students the knowledge needed to begin shifting their RMF efforts to a cloud environment.

Our training delivery methods:

- **Traditional classroom**
- **Online Personal Classroom™ (interactive, live, instructor-led)**
- **Private group classes for your organization (on-site or online instructor-led)**

Regularly-scheduled classes through September, 2021:

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

- ♦ **Online Personal Classroom™ ▪ 26 - 29 APR ▪ 10 - 13 MAY ▪ 17 - 20 MAY ▪ 24 - 27 MAY ▪ 7 - 10 JUN ▪ 14 - 17 JUN ▪ 28 JUN - 1 JUL ▪ 12 - 15 JUL ▪ 19 - 22 JUL ▪ 26 - 29 JUL ▪ 9 - 12 AUG ▪ 16 - 19 AUG ▪ 30 AUG - 2 SEP ▪ 13 - 16 SEP ▪ 27 - 30 SEP**
- ♦ **San Diego ▪ 28 JUN - 1 JUL**
- ♦ **Colorado Springs ▪ 14 - 17 JUN**

RMF Supplement for DCSA Cleared Contractors—1 day program

- ♦ **Online Personal Classroom™ ▪ 19 APR ▪ 20 MAY ▪ 24 JUN ▪ 8 JUL ▪ 5 AUG ▪ 9 SEP**

DFARS Compliance with CMMC/NIST SP 800-171 Readiness Workshop —3 day program

- ♦ **Online Personal Classroom™ ▪ 19 - 21 APR ▪ 1 - 3 JUN ▪ 21 - 23 JUN ▪ 6 - 8 JUL ▪ 2 - 4 AUG ▪ 7 - 9 SEP**

eMASS eSSENTIALS—1 day program

- ♦ **Online Personal Classroom™ ▪ 30 APR ▪ 21 MAY ▪ 28 MAY ▪ 11 JUN ▪ 18 JUN ▪ 16 JUL ▪ 23 JUL ▪ 30 JUL ▪ 13 AUG ▪ 20 AUG ▪ 3 SEP ▪ 17 SEP ▪ 1 OCT**
- ♦ **San Diego ▪ 2 JUL**
- ♦ **Colorado Springs ▪ 18 JUN**

STIG 101—1 day program

- ♦ **Online Personal Classroom™ ▪ 16 APR ▪ 14 MAY ▪ 21 JUN ▪ 2 JUL ▪ 30 JUL ▪ 27 AUG ▪ 24 SEP**

Information Security Continuous Monitoring—1 day program

- ♦ **Online Personal Classroom™ ▪ 23 APR ▪ 3 JUN ▪ 9 JUL ▪ 30 JUL ▪ 10 SEP**

RMF in the Cloud—1 day program

- ♦ **Online Personal Classroom™ ▪ 23 APR ▪ 1 JUN ▪ 23 JUN ▪ 8 JUL ▪ 4 AUG ▪ 8 SEP**

Security Controls Implementation & Assessment Workshop—4 day program

- ♦ **Online Personal Classroom™ ▪ 19 - 22 APR ▪ 1 - 4 JUN ▪ 21 - 24 JUN ▪ 26 - 29 JUL ▪ 23 - 26 AUG ▪ 20 - 23 SEP**

Please note that all classes are currently being delivered in an online, instructor-led format, but traditional classrooms will be reinstated as government travel restrictions are relaxed.

Contact Us!

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

Phone: 1-800-RMF-1903
Fax: 540-518-9089
Email: rmf@rmf.org

Registration for all classes is available at

https://register.rmf.org

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

Find us on LinkedIn

BAI Information Security Consulting & Training