Risk Management Framework Today...

and Tomorrow

October, 2022 Volume 14, **Issue 4**

The Authorizing Official (AO) Problem & The Army Risk Management Council (ARMC)

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

About four or five years ago, I had a meeting with an Army organization on the topic of providing RMF training targeted specifically at Authorizing Officials (AO's). My memory is a bit hazy, but as I recall, after two or three meetings we had outlined what would be necessary in providing a half day of RMF training targeting AO's as the primary audience. At the time, I was very enthused at the opportunity to fix what I call "The AO Problem". Unfortunately, the discussions I had did not come to any meaningful result and an RMF eLearning course was published shortly thereafter internal to Army. Upon hearing this, I was a bit upset, but I hoped that the meetings and suggestions I made could hopefully help Army in the future.

Flashing forward to today, I recently attended TechNet Augusta. During this conference, I kept hearing chatter of Army shifting to a single AO. Although I do not know the full details of this, I can confirm that one of the single biggest problems I hear from RMF students and practitioners is AO's not fully understanding the RMF process. We also see this as RMF consultants where different AO's take entirely alternative approaches to evaluating a package and granting an ATO. Although my major concern with a single AO would be inability to have a full understanding of all systems being authorized, I certainly would prefer to have a handful of AO's with a strong RMF knowledge base than the alternative.

A relatively new development to Army in parallel with RMF 2.0 is called the Army Risk Management Council (ARMC). For those who are unfamiliar with RMF 2.0 (not to be confused with the NIST, Ron Ross RMF 2.0 initiative), RMF 2.0 is an Army initiative with goals of increasing control inheritance and making the RMF process more agile and compact. I first heard about ARMC from Nancy Kreidler, former Director of Cybersecurity at CIO/G6 and Lt. Gen John Morrison, the Army's deputy chief of staff, G-6 during a keynote at AFCEA TechNet Cyber. During this keynote ARMC was proposed to have goals of deconflicting positions between AO's and taking pressure off AO's who are often making these high-risk decisions alone in a vacuum. The last I heard ARMC was chaired by Army G-3 and was supposed to be fully staffed in May 2022. The goal of ARMC is create a network of AO's and more communication regarding systems and how they interact on the network.

Overall, as you can tell by the topics referenced above, Army recognizes they have an AO problem, and I applaud all involved who are continuously working towards making the RMF process more efficient and effective. At BAI, we fully embrace and support RMF efficiency if proposed RMF initiatives are not suggesting shortcuts that result in weakening and watering down the RMF process. I look forward to updating our readers as I get more information on ARMC and this ongoing AO conundrum.

--

For additional information on RMF training, or to register for an upcoming class, please call BAI at 1-800-RMF-1903 (763-1903) or visit https://rmf.org/rmf-project-management-advantage/

In this issue:

Confessions of a Junior RMF Consultant

By Grace Brammer, RDRP

The very first time I heard about a so-called ‘RMF process,’ I was in my freshman year of college. To anyone familiar with the industry, it may come as a shock to hear that my initial exposure to RMF left me with a mixture of emotions—mostly confused, slightly intimidated…yet still intrigued by this aspect of security I had not heard of before. All the publications, controls, rules, and unfamiliar acronyms left me dazed at first—*especially* the acronyms. I could not fathom how anyone could remember such similarly spelled words! I found myself wondering, “What’s the difference between an ISSO and ISSM?” and “Why do so many control families start with the letter ‘*A*’?” I had no idea at the time that a little less than a year later, I would find myself working a job supporting an organization that teaches all things RMF—a concept I previously never even knew existed.

What Do You Do for Work?

Surprisingly, one of the most complicated parts of RMF for me thus far has been trying to explain to other people what it is that I do, exactly. For the people I can tell who do not *really* want to know all about the NIST 800-53r5, or STIGs, or the latest excel spreadsheet I have seen, I give them the short answer: “*Cybersecurity*!” Being a Junior Consultant however, when it comes to talking with people who are *not* like my college self and have heard of RMF before, I sometimes can feel unqualified to speak confidently about my work. Luckily, I know now that RMF is such a big process, and there’s no way to realistically memorize everything at once. I may still be learning, Continuing Education is important for a reason, after all.

What’s New?

My latest undertaking has involved working with control families Awareness Training (AT) and Risk Assessment (RA) on a private system. My first real consulting project has made me realize it is far better to ask questions as they come up, rather than assume you are correct the first time. I made a mistake documenting my very first set of controls when I assumed the system I was working was a DoD-compliant one. A large number of the controls I was reading through came with a note saying, *“The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.”* I worked the entire control family under the impression these were automatically compliant, when I should have stopped to ask for more information about the system from the beginning. In actuality, the system was a cleared-contractor being authorized by DCSA, not the DoD, disqualifying it from the ‘automatically compliant’ status I had assumed would apply to it. All this to say—when doing RMF, don’t do it alone!

> ***“A large number of the controls I was reading through came with a note saying, “The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level...”***

--

For additional information on RMF training, or to register for an upcoming class, please call BAI at 1-800-RMF-1903 (763-1903) or visit https://rmf.org/rmf-project-management-advantage/

NIST Updates the AI RMF

By Kathryn Daily, CISSP, CAP, RDRP

Artificial intelligence (AI) is the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. One example of AI is the use of virtual filters on our face when taking pictures with various cell phone applications. Another example is autocorrect, where algorithms use machine learning (ML) and natural language processing to identify incorrect usage of language and suggest corrections.

In response to the RFI, NIST received more than 130 responses from industry, non-profit, individuals, government, and academia.

Once NIST received the responses they were grouped into themes based on commonalities. A total of 7 themes were identified; with Machine learning still in the initial stage of development, so many attack vectors are not clear, so cyber defense strategies are also in their early stages. In order to aid with the development of AI/ML, NIST has developed the AI Risk Management Framework to address risks in the design, development, use and evaluation of AI products, services and systems. The intent with this voluntary framework is to continuously update it to keep it up to date with AI trends as the development continues.

"In order to aid with the development of AI/ML, NIST has developed the AI Risk Management Framework to address risks in the design, development, use and evaluation of AI products, services and systems."

NIST released the initial draft AI RMF in March of 2022 and is now updating it to reflect the feedback that has been received since the creation of the initial publication and the end of the recent comment period ending on 29 September 2022. The fact that NIST is updating this framework in the same year as the initial draft, demonstrates its commitment to staying up to date with the development of the emerging AI technology and incorporating the feedback from stakeholders in a timely manner. The second draft is anticipated to be published in January 2023. While the comment period has officially ended at the time this article was published, NIST will be conducting a third AI RMF workshop on 18-19 October 2022 and will be receiving feedback at that event.

Specifically with this comment period, NIST was seeking guidance on how industry or sector may utilize the Framework, how smaller organizations can use it, how it can be used for procurement and acquisition, how the Framework can help address security concerns, including guarding against adversarial attacks on AI systems, among other topics. Once received and organized, NIST will release the comments publicly for all to see.

Keep an eye out for that updated publication in January, and keep an eye out here for our review of the updated framework!

--

For additional information on RMF training, or to register for an upcoming class, please call BAI at 1-800-RMF-1903 (763-1903) or visit https://rmf.org/rmf-project-management-advantage/

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/.

"Secret Admirer" writes:

I'm finally ready to admit it publicly … I'm a huge admirer of Dr. RMF … Oh, how I love a man in a white coat!

Beyond that, I do have an RMF-related question. I'm an application developer in my company and I just found out our system engineers are handling STIG compliance in a very "odd" way. What they do is they scan the server with SCC and for any items that come up non-compliant they just write "Necessary for system functionality" in the STIG Viewer. They don't even try to remediate the finding. When I pointed out how wrong this is, they told me the government ISSM had approved what they are doing. I tried appealing to my boss but he told me "that's engineering's problem" and I should stay out of it. Please, Dr. RMF, tell me what I can do to fix this.

Dr. RMF Responds:

I agree you're in a difficult position, but the good news is this is a problem that may very well fix itself, so to speak. The system your company is developing will undoubtedly need to go through independent assessment before an ATO is approved. If the assessors are at all on the ball, they will quickly pick up on this "creative" approach to STIG compliance, and may very well write this up as a high risk finding. The government ISSM will then find himself in the position of having to ask your company to revisit the STIG compliance effort and actually do it *right*.

"The system your company is developing will undoubtedly need to go through independent assessment before an ATO is approved."

By the way, for what it's worth, if Dr. RMF was in charge of things, that ISSM would find himself out of a job.

Oh, and one more thing. Dr. RMF thanks you for being a not-so-secret admirer. But please, let's just leave it at that. After all, I am a married man and I wouldn't want Mrs. RMF getting upset with me. I'm sure you understand.

"AO A-Okay" writes:

I have worked on a number of different DoD contracts over the years and I've noticed that some of the DoD Components (e.g., Army) have different Authorizing Officials (AOs) for each of their various major commands or programs, while other DoD Components (e.g., Navy) have a single AO for the entire organization. Are both of these approaches in accordance with "official" DoD policy? From a practical standpoint, is one approach "better" than the other? Recently I heard a rumor that Army may be attempting to go to a "single AO". If that is the case, what effect do you think it will have on present and future Army RMF efforts?

Dr. RMF Responds:

DoD policy requires each system to have an assigned Authorizing Official (AO), but does not specify a single AO or multiple AOs per DoD Component. Therefore both approaches are considered to be in accordance with DoD policy. As for the question of which approach is "better", Dr. RMF most definitely prefers the multiple AO approach. The reason is that the AO's role is to make an authorization decision for each system based on risk

Find us on LinkedIn

Want to see more of Dr. RMF? Watch our Dr. RMF video collection at https://www.youtube.com/c/BAIInformationSecurity.

Dr. RMF, from Page 4:

and mission need. A single AO at the very top of a DoD component would be so far removed from the individual programs that it would be nearly impossible for him or her to have good insight into mission need. In practice, the single AO will likely turn out to be little more than a "rubber stamp" for the recommendation of the Security Control Assessor (SCA). So you've probably figured out by now that Dr. RMF does not favor the Army's apparent move to "consolidate" the AO role. In addition to the weakness described above, the "single AO" approach will also create yet another bottleneck in the Army's already overly lengthy ATO process. Alas...

> ***"In practice, the single AO will likely turn out to be little more than a "rubber stamp" for the recommendation of the Security Control Assessor (SCA)."***

"Controls Freak" asks:
I'm still fairly new at the profession, but since being assigned to an RMF project by my company, I have become rather obsessed with the RMF security controls. My ambition is to memorize all the controls and control enhancements in NIST 800-53 so that if someone says "MA-3", for example, I will be able to quote the control text verbatim. Is this a reasonable ambition, Dr. RMF, and do you think it will lead to future promotions?

Dr. RMF Responds:
First of all, true confession. Back in his younger days, Dr. RMF did exactly what you're talking about, but with the DIACAP controls. There were only about 100 of those, so it wasn't quite the same. Now you realize there are well over a thousand controls and control enhancements in the NIST SP 800-53 Rev 5. Dr. RMF believes it would definitely be a major undertaking to memorize them all, but I'm sure it can be done. After all, medical students memorize the name and function of every bone, muscle, nerve and blood vessel in the body. Yeah, they're pretty smart folks, but so are a lot of us cybersecurity professionals. Just sayin'… However, just because it's a "monumental achievement" to memorize all the RMF controls doesn't mean it's something you should spend your time doing. It's kind of like climbing Mount Everest, but without the risk of death … unless you're foolish enough to walk across a city street with your head buried in the 800-53 document! Sure, memorizing the RMF controls might get you some "geek cred" in cybersecurity circles, but it is unlikely to get you a promotion on the job. There are much better ways to spend your time furthering your cybersecurity knowledge and skills. Get some more training (from BAI, of course), pick up a new certification, you get the drill. Those kind of things are far more likely to advance your career than becoming the uber-geek of RMF controls!

Want to see more of Dr. RMF? Watch our Dr. RMF video collection at https://www.youtube.com/c/BAIInformationSecurity.

Risk Management Framework Today...

and Tomorrow

Classroom RMF and eMASS Training is Back!

BAI RMF Resource Center is pleased to announce the return of RMF and eMASS training classrooms with the addition of our new locations in Colorado Springs, Pensacola, San Diego, and Crystal City!

RMF for DoD IT and Federal Agencies & eMASS eSSENTIALS ™

Pensacola, FL — October 24th – 28th

Colorado Springs, CO — November 7th – 11th and February 27th – March 3rd

San Diego, CA — December 5th – 9th and March 27th – 31st

Crystal City, VA — January 30th – February 3rd

Enjoy the scenery after class in Colorado Springs (top left), Pensacola (bottom left), Crystal City (top right), or San Diego (bottom right)!

New Course Announcement: RMF for DoD IT +
*****RMF Project Management Advantage*****

RMF Project Management Advantage is a one-day course designed for RMF practitioners and/or managers at all levels with goals of utilizing project management best practices and strategies from Project Management Institute (PMI) as well other global industry proven project management standards. The course was authored and is taught by a senior RMF practitioner and Project Management Professional (PMP) who is passionate about leveraging real-world RMF and project management experience to reduce RMF project costs and streamline the RMF process. If you are interested in decreasing RMF implementation time and cost, this course is for you! Seats currently available for 1-day PMA and 5-day RMF + PMA Bundle—sign up now!

To register, contact alice@rmf.org or go to register.rmf.org.

Find us on LinkedIn

BAI Information Security Consulting & Training

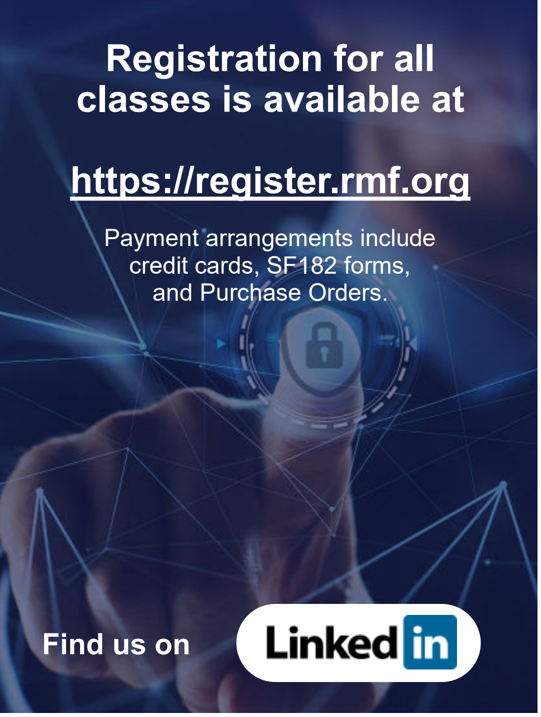
Risk Management Framework Today…

and Tomorrow

Contact Us!

RMF Today … and Tomorrow is a publication of BAI Information Security, Radford, 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

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 for Federal Agencies** – recommended for Federal Agency employees and contractors that require detailed RMF knowledge and skill training; covers the RMF life cycle, documentation, and security controls with an additional emphasis on Federal application.
- **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).
- **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.
- **RMF Project Management Advantage** – provides "how to" guidance for the most commonly-used RMF strategies in project management.

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 December, 2022:

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

- ♦ Online Personal Classroom™ ▪ 24 - 27 OCT ▪ 7 - 10 NOV ▪ 14 - 17 NOV ▪ 28 NOV - 1 DEC ▪ 12 - 15 DEC ▪ 9 - 12 JAN ▪ 23 - 26 JAN ▪ 13 - 16 FEB ▪ 13 - 16 MAR ▪ 27 - 30 MAR
- ♦ Colorado Springs, CO ▪ 7 - 10 NOV ▪ 27 FEB - 2 MAR
- ♦ San Diego, CA ▪ 5 - 8 DEC ▪ 27 - 30 MAR
- ♦ Crystal City, VA ▪ 30 JAN - 2 FEB

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

- ♦ Online Personal Classroom™ ▪ 6-9 FEB

CAP Bootcamp—1 day program

- ♦ Online Personal Classroom™ ▪ 31 OCT ▪ 17 JAN ▪ 10 FEB

eMASS eSSENTIALS—1 day program

- ♦ Online Personal Classroom™ ▪ 21 OCT ▪ 28 OCT ▪ 11 NOV ▪ 18 NOV ▪ 2 DEC ▪ 16 DEC ▪ 19 DEC ▪ 13 JAN ▪ 27 JAN ▪ 2 DEC ▪ 16 DEC ▪ 19 DEC ▪ 13 JAN ▪ 27 JAN ▪ 17 FEB ▪ 17 MAR ▪ 31 MAR
- ♦ Colorado Springs, CO ▪ 11 NOV ▪ 3 MAR
- ♦ San Diego, CA ▪ 9 DEC ▪ 31 MAR
- ♦ Crystal City, VA ▪ 3 FEB

Security Controls Implementation & Assessment Workshop—4 day program

- ♦ Online Personal Classroom™ ▪ 5 - 8 DEC ▪ 6 - 9 FEB ▪ 6 - 9 MAR

STIG 101—1 day program

- ♦ Online Personal Classroom™ ▪ 1 NOV ▪ 22 NOV ▪ 9 DEC ▪ 21 DEC ▪ 19 JAN ▪ 24 FEB ▪ 22 MAR

Information Security Continuous Monitoring—1 day program

- ♦ Online Personal Classroom™ ▪ 4 NOV ▪ 21 NOV ▪ 18 JAN ▪ 22 FEB ▪ 23 MAR

RMF in the Cloud—1 day program

- ♦ Online Personal Classroom™ ▪ 2 NOV ▪ 23 NOV ▪ 13 DEC ▪ 20 JAN ▪ 23 FEB ▪ 24 MAR

Certified Authorization Professional (CAP) Supplement—1 day program

- ♦ Online Personal Classroom™ ▪ 31 OCT ▪ 17 JAN ▪ 10 FEB

RMF Project Management Advantage (PMA)—1 day program

- ♦ Online Personal Classroom™ ▪ 3 NOV ▪ 20 DEC ▪ 10 FEB ▪ 10 MAR

RMF Supplement for DCSA Cleared Contractors (DCSA)—1 day program

- ♦ Online Personal Classroom™ ▪ 21 FEB