RMF TODAY ...AND TOMORROW
JULY 2023
VOLUME 15, ISSUE 3

NEWSLETTER

RMF TOMORROW: TRUTH OR FICTION?

BY LON J. BERMAN, CISSP, RDRP

"When it comes to the future of RMF, rumors abound but truth is hard to come by."

Cont. on Page 2

NIST SP 800-53 DELTA FROM REV 4 TO REV 5

BY KATHRYN DAILY, CISSP, CGRC, RDRP

"The main difference is the update and enhancement of the controls framework to address privacy alongside security, rather than tacking it on at the end, as has arguably been done in previous years"

Cont. on Page 3

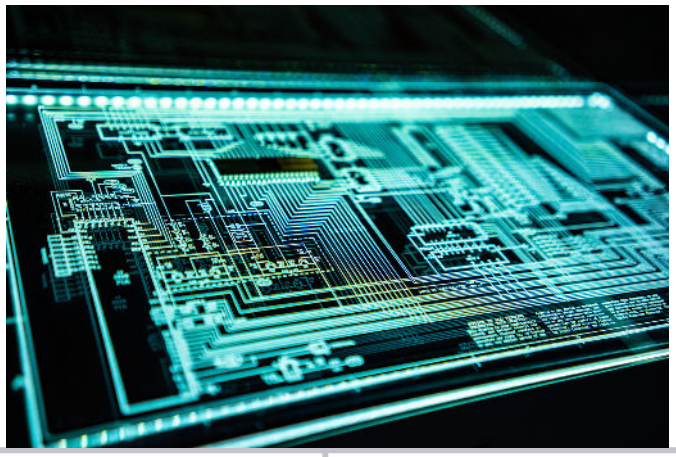
SO, YOU THINK YOU CAN PRACTICE RMF...?

BY PHILIP D. SCHALL, PH.D., CISSP, RDRP

"...when asked how to get into the RMF field, I first warn that RMF does not appear to be the most exciting work to do, but it is in high demand and an interesting skillset once mastered."

Cont. on Page 4

NEW OFFERINGS: RMF AND SUPPLY CHAIN SECURITY AND HUNTSVILLE IN-PERSON CLASSES



BAI Information Security is thrilled to announce that we have developed a brand new, online, instructor-led course to teach you how to secure your organization's supply chain within your existing RMF package.

Learn more about the class: https://rmf.org/rmf-and-supply-chain-security/

Find your training date and register today: https://register.rmf.org!

BAI is back in Huntsville this fall! We love our customers in Alabama, and we are excited to bring in-person RMF training to you. Join us from October 16-20 for our RMF for DoD IT + eMASS bundle and enjoy our training without Teams and Slack notifications to distract you.

Learn more about our Huntsville venue: https://register.rmf.org/venues/huntsville/

Register today at https://register.rmf.org!

Risk Management Framework Today... *and Tomorrow*

In This Issue:

BAI Information Security RMF Resource Center

https://rmf.org

RISK MANAGEMENT FRAMEWORK (RMF) TOMORROW: TRUTH OR FICTION?

BY LON J. BERMAN, CISSP, RDRP

When it comes to the future of RMF, rumors abound but truth is hard to come by. In this article, we'll take a look at some of the speculations and see if there's any truth to them.

Let's start with an oldie. "*DoD will abandon RMF and develop their own information security framework*." This one's been around for quite some time and, quite frankly, there is no truth whatsoever to it. DoD is firmly established within the Joint Task Force and has agreed to move in lock step with the federal civil agencies and the intelligence community. The only way a new information security framework would come into being is if all federal departments and agencies agreed to it – an extremely unlikely occurrence.

"*RMF will be replaced by the NIST Cybersecurity Framework (CSF).*" There has been some recent "buzz" over CSF, with NIST actively working on a new version of this framework. CSF was conceived as a voluntary framework for use by critical infrastructure industries such as transportation and telecommunications. While CSF does have some applicability to government information systems, it was never intended to replace RMF, and that has not changed.

"*RMF will be fully automated*." For those of us struggling to put together RMF packages, this is a lovely thought, but it is just not feasible. RMF encompasses three classes of security controls, to wit: Management, Operational and Technical. Automation may be able to be leveraged to maintain compliance with technical controls (e.g., configuration settings of system software), but automating management and operational controls remains a bridge too far.

"*Artificial Intelligence (AI) will make RMF obsolete*." AI may well be used to assist in various aspects of the RMF process, such as document preparation, but even in the most optimistic scenario, this would fall far short of rendering RMF "obsolete".

"*The number of NIST SP 800-53 security controls will be vastly reduced.*" I've read this one in a few places over the years, but there does not appear to be any factual basis for it. If anything, the number of security controls in NIST SP 800-53 seems to be increasing, e.g., the addition of Privacy and Supply Chain controls in the 800-53 Rev 5.

"*eMASS will be replaced by a new tool.*" There may actually be a grain of truth in this one. DoD spends a lot of money each year maintaining eMASS and they have been desperately looking for a way of reducing this expenditure. One possible way would be to find a commercial tool that could be configured to do what eMASS does today. It seems unlikely such a tool exists, and, even if one was found, it's not at all clear that purchasing/licensing the tool and then configuring or customizing it would end up being any less costly. Nevertheless, this is probably one that bears watching over the coming year.

"*DISA STIGs are going away*." This one may have come about because of the funding issues surrounding the DoD SCAP Compliance Checker (SCC) tool. That's a long story and I won't go into the details here, but suffice it to say it has nothing whatever to do with the STIGs themselves. To the best of anyone's knowledge, STIGs are alive and well and the local economy of Chambersburg, PA is safe for the foreseeable future ☺

If you hear any more "future of RMF" rumors, please contact our BAI subject matter expert team (aka. "Dr. RMF") at drrmf@rmf.org.

ASK DR. RMF!

A reader who calls himself "Dis-appointed?" asks:

Dear Dr. RMF,

Are appointment letters required to obtain an eMASS account for the roles of ISSO, ISSM, and SCA? Also, are appointment letters required for executing the roles of ISSO, ISSM and SCA (outside of obtaining eMASS accounts)?

Dear Dis,

There is no DoD-wide policy regarding eMASS access. Access policies are maintained at the individual DoD component level. Dr. RMF therefore recommends you direct your question to the administrator of the particular eMASS system that your organization uses (e.g., Army eMASS, Air Force eMASS, Navy eMASS, etc.).

Dr. RMF recommends a formal appointment letter be given to each person with a designated "role" in the RMF process. This will ensure that they are aware of their responsibilities.

Also, for what it's worth, please note there is not a "one to one match" between the eMASS account "roles" and the RMF "roles" as defined in DoD Instruction 8510.01.

NIST SP 800-53: WHAT'S THE DELTA FROM REV. 4 TO REV. 5?

BY KATHRYN DAILY, CISSP, CGRC (FORMERLY CAP), RDRP

NIST SP 800-53 (National Institute of Standards and Technology Special Publication 800-53) provides a set of security and privacy controls for information systems and organizations. It was initially developed by NIST thanks to the E-Government Act of 2002, or more specifically, the Federal Information Security Management Act (FISMA) passed on December 17th, 2002. This control set has evolved many times over the years, and in September 2020, NIST released Rev. 5.

The main difference between NIST SP 800-53 Rev 4 and Rev 5 is the update and enhancement of the controls framework to address privacy alongside security, rather than tacking it on at the end, as has arguably been done in previous years. Here are some key differences:

1. 269 new controls and 2 new families: Rev. 5 introduces 65 new base controls and 204 control enhancements. 28 of these controls are assigned to the moderate baseline. Many of those new controls come from the two new families to wit, Supply Chain (SR) and Personally Identifiable Information Processing and Transparency (PT) – More to follow.

2. Consolidating the Control Catalog: Rather than having a separate appendix (J) for privacy controls, Rev. 5 has integrated the privacy controls into its own distinct family (PT – Personally Identifiable Information Processing and Transparency) and the existing PM – Program Management family. Additionally, some privacy controls were also incorporated into current security controls, allowing the controls to serve both security and privacy, and achieving more efficient control implementation. One example of a privacy control having been integrated into a previous security control is the inclusion of privacy training elements in the AT family.

3. Integrating supply chain risk management: Rev. 5 has established a new family of controls focused on supply chain risk management to ensure that security and privacy requirements, threats, and other concerns are addressed throughout the system development lifecycle and throughout the supply chain. Both government (at all levels) and industry now have a much larger focus on supply chain threats and NIST has responded by including the controls required for organizations to effectively manage that risk.

4. Adding new state-of-the-practice controls: 800-53 was last updated in 2015. A lot has changed since then. Granted, Rev. 5 came out in 2020 and a lot has changed since THEN, but I digress. Many new controls have been added to reflect evolving cyber threats and new safeguards and countermeasures that have become available. One such control is IA-12, Identity Proofing. Historically, online identity has been managed with usernames, email addresses and passwords. Today, the concept of a user identity is far more complex. Identities now encompass layers of information and verification including physical identification documents, knowledge-based security questions, biometrics, etc. Identity proofing allows organizations to better secure users and their data by verifying the identity of individuals with a much higher level of accuracy.

ARTICLE CONTINUES ON PAGE 5

ASK DR. RMF!

A reader who calls herself "Thirsting for Knowledge" asks:

Dear Dr. RMF,

Recently I've seen a few RMF-related articles online that referred to something called the "knowledge service". Can you tell me what exactly this service is and if you think it would help me develop my RMF skills. Is there a cost associated with this service and do you think my employer would pay for it? I am a contractor, not a DoD employee.

Dear Thirsting,

The RMF Knowledge Service is a website operated by DoD that contains a veritable treasure trove of RMF information … everything from security controls to RMF process steps to documentation artifacts, and more! Dr. RMF absolutely believes it would be helpful to you and highly recommends you become familiar with it at your earliest convenience. The URL is https://rmfks.osd.mil. For active military and DoD employees, all that is needed is a Common Access Card (CAC) and you're in!

However, since you're a contractor, there are a couple of additional steps you'll need to complete. First, you'll need a digital certificate from a vendor authorized by DoD. This is also called an External Certificate Authority (ECA) certificate. Your company may already provide this, but if you need to purchase one on your own, there is typically a fee of about $100 per year (it varies among vendors, so shop around). Second, you'll need a DoD employee to "sponsor" you for access to the Knowledge Service. This requires only that the DoD employee be willing to verify that you have a legitimate "need to know". If you are a contractor, the easiest way to get a "sponsor" is to ask one your DoD customers. Once your account is approved by your "sponsor", you will be able to access the Knowledge Service – there is no additional cost.

SO, YOU THINK YOU CAN PRACTICE RMF: BREAKING INTO CYBER AS AN RMF PRACTITIONER

BY PHILIP D. SCHALL, PH.D., CISSP, RDRP

As a college professor and Director of Training at BAI RMF Resource Center, I often am approached by students of all ages asking how they can break into cybersecurity and the RMF field. What generally follows is a dialogue regarding if they need a college degree or certifications etc. For the past few years, I have usually directed students to www.cyberseek.org/ where they see a glaring employment gap and the promise of hefty salaries, and with some blend of a college degree and certifications, they get their first jobs. Unfortunately, during the last year, I have seen a shift and students having a tough time securing employment.

This article is not centered on the current tech economy, but instead a commentary on what I have experienced as the most ideal blend of education and certification to break into the field. I have read a few articles recently on LinkedIn which have indicated that a college degree is no longer useful and hopeful job candidates should secure certifications and up their technical skills. I am a bit biased as a college professor, but I believe in the value of an approachable and affordable college education. As someone who sees students work through four years of undergraduate coursework and grow into young professionals, I have witnessed first-hand the growth that occurs throughout the college experience. With that said, not all colleges are built equally, and I am a strong proponent of affordable state schools or community colleges if a student cannot secure a large scholarship or does not come from a background of strong means. Essentially, unlike many, I still believe in the value of a traditional college degree, but I recognize that not all programs are built to the same quality.

Next on my list are cybersecurity and IT certifications. My stance on these is straightforward, I firmly believe that a traditional college degree (bachelors or associates) is greatly enhanced when a graduating senior or career switcher can show a hiring director that they have the ambition to obtain a certification like Security+ or CISSP early in their career. I recognize that these first certifications can be daunting, but to me it shows that a job candidate has the tenacity to attempt a challenging certification exam with little experience. It is worth mentioning that BAI RMF Resource Center offers something akin to a certification called RDRP. RDRP stands for Registered DoD RMF Practitioner. This essentially serves as a registry for folks who have received RMF training and have passed BAI's proprietary RMF exam. Information about RDRP can be found at the following link https://rmf.org/what-is-rdrp/.

The final and often most difficult element for a graduating college student is experience.

I suggest that the student do everything they can to secure an internship and if this is not possible, they should gain experience on a university cyber team or through creating a small business that performs IT or cybersecurity support to local businesses.

Overall, I firmly believe in having a blend of a college degree, certifications, and some real-world experience. As the job market gets tighter and the cybersecurity career gap shrinks, the job market will continue to be highly competitive, and we are still encountering entry level jobs written with mid-level skill requirements. The number one piece of advice I can give new graduates trying to break into the field is to have tenacity and a drive to succeed. I had a student a few years ago with no experience besides working at a gas station, and after following the advice above and submitting 130 job applications he got his first job. The student in reference is now a mid-level cybersecurity engineer for a major cybersecurity firm.

Beyond these basic cybersecurity entry suggestions, when asked how to get into the RMF field, I first warn that RMF does not appear to be the most exciting work to do, but it is in high demand and an interesting skillset once mastered. I then suggest that students take an entry-level RMF class like RMF for DoD IT offered by BAI or at the minimum watch the videos series BAI and CompTIA partnered with called RMF Micro Edition. Once some basic RMF education has been completed, I advise students to search entry level roles and make sure they have baseline cybersecurity certifications required for these roles. I find baseline cybersecurity certifications like Security+ paired with RDRP and a college degree can position students strongly to be interviewed for entry-level RMF positions. From there, it becomes an exercise in gaining experience and climbing the ladder to mid and senior level in a short suspense.

"Genius is 1% talent and 99% percent hard work..."
— Albert Einstein

REV. 4 TO REV. 5 DELTA CONTINUED FROM PAGE 3

5. Making controls outcome based: Rev. 5 has removed the entity responsible for satisfying the control (i.e., information system, organization, etc.). This puts the focus on the protection outcome to be achieved by the application of the control. For example, changes to IA-4 Identifier Management:

- Rev 4 states, "the organization manages information system identifiers by:"
- Rev 5 removes "the organization" and simply states, "manage system identifiers by:"

6. Clarifying and defining relationships: Revision 5 clarifies the relationship between requirements and controls as well as the relationship between security and privacy controls in Chapter 2.

7. Separating the control selection processes from the controls: The control selection process was moved from the 800-53, to the 800-53B. The intent with this change was to develop the control catalog as a stand-alone document to enable use by different communities of interest. The control set is technology-neutral, and the guidelines can be adopted by any organization operating an information system with sensitive or regulated data. Many frameworks use the 800-53 control set including the obvious Risk Management Framework used by federal agencies and the Department of Defense. Additionally, DFARS 7012/NIST SP 800-171 which is used by all companies in the defense industrial base that use controlled unclassified information use the 800-53 Control Catalog. The controls also map to other frameworks such as CSF, PCI DSS, and HIPAA. Even organizations that aren't using a specific framework can create their own baseline based on their internal risk assessment to address the identified residual risk.

8. Transferring control baselines and tailoring guidance to NIST SP 800-53B: The High, Moderate, and Low baselines were also moved to the 800-53B to allow the 800-53 control catalog to be used by different communities of interest as the baselines are applicable to federal agencies and reflect specific requirements under FISMA and OMB A-130.

9. Removed "Federal" from the title of the document: In Rev. 5, the word "Federal" was removed from the title. This change was made to reinforce the efforts of widespread adoption by the public and private sector. While only federal systems require the NIST framework, many voluntary frameworks either exclusively use the control set, or have mappings to the 800-53 control set. It's very likely that in future revisions, many of the frameworks not currently based on the 800-53, will be altered to align with it.

Comparing Control AU-2 in Rev. 4 and Rev. 5

Rev. 4	Rev. 5
AU-2: AUDIT EVENTS Control: The Organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why auditable events are deemed to be adequate to support after-the-fact investigation of security incidents; and d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or other situation requiring) auditing for each identified event].	**AU-2: EVENT LOGGING** [1] Control: a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging] [2]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2 a) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event type selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency] [3].

1. Changed the title from Audit Events to Event Logging
2. Changes the parameter regarding the specific types of events the system is capable of logging.
3. Requires a review and update of the event types selected for logging at a specific frequency (From withdrawn control AU-2(3)

BAI SUPPLEMENTAL RESOURCES

WHAT IS REGISTERED DOD RMF PRACTITIONER (RDRP)?

The Registered DoD RMF Practitioner (RDRP) program was created in response to BAI RMF Resource Center recognizing the need for a credential which shows competency and proficiency in the understanding and application of RMF for DoD. RDRP is comprised of a network of information security professionals specializing in supporting Risk Management Framework (RMF) in the Department of Defense (DoD) programs. The requirements to join RDRP are very straightforward:

Step 1: Attend 4 days or more of RMF for DoD IT training.
Step 2: Remit the initial credentialing fee.
Step 3: Complete the 50 questions "RMF for DoD IT Competency Test" with a passing score of 70%.

Being part of the RDRP registry not only adds credentialing value, but it also shows employers and government officials that registrants have a comprehensive understanding of RMF as it is implemented within DoD. Registrants are also joining a community that fosters RMF inquiry as well as networking opportunities amongst colleagues.

The only cost associated with becoming an RDRP is a one-time $100 administration fee that covers program administration. Once an RDRP candidate passes the RDRP exam and remits their $100 registration fee, they will become a lifetime RDRP member.

BAI's students who have completed 4-days or more of RMF DoD IT training may go to rmf.org/rdrp to begin the registration process.

Do you have burning RMF questions that just can't wait? Submit your questions to our Dr. RMF form and receive personalized advice from our panel of RMF experts. In addition, your question may be featured in our newsletter column (with all sensitive and identifying information removed)!

With over 30 years of experience in topics from security controls implementation to risk assessment, we can help you navigate the complex world of RMF.

Want to see more of Dr. RMF? Watch our Dr. RMF video collection on YouTube!

What are People are Saying About Us?

One of the best classes in 40 years
"Ms. Linda Gross did an excellent job. One of the best online classes I attended over the last 40 years. Great Couse! She took my knowledge of RMF to a whole new level. Not sure what you are paying Linda, but it's not enough."

- Eddie, FCOE CIO/G6, Fort Sill

Great Instructors
"Great Instructors!! Ernest and Kathryn are great!!"

- Susan, US Army

Advise all Technical Roles to Attend
"I am very experienced with STIGs...but this opened a few more doors I hadn't considered and provided a larger scale picture of what is to come. I would advise all SAs, NAs, DevSecOps personnel, ISSOs, ISSMs, SCARs and SCAs to attend."

- John, Technica

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.
- **RMF and Supply Chain Security -** equips personnel to develop a tailored C-SCRM program that is cost effective and addresses the necessary supply chain requirements.

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, 2023:

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

- Online Personal Classroom™ ▪ 17-20 JUL ▪ 31 JUL-3 AUG ▪ 7-10 AUG ▪ 28-31 AUG ▪ 11-14 SEP ▪ 25-28 SEP ▪ 2-5 OCT ▪ 30 OCT-2 NOV ▪ 27-30 NOV ▪ 4-7 DEC
- Colorado Springs, CO ▪ 14-17 AUG ▪ 13-16 NOV
- San Diego, CA ▪ 25-28 SEP ▪ 11-14 DEC
- Pensacola, FL ▪ 10-13 JUL
- ***NEW*** Huntsville, AL ▪ 16-19 OCT

eMASS eSSENTIALS—1 day program

- Online Personal Classroom™ ▪ 21 JUL ▪ 4 AUG ▪ 11 AUG ▪ 1 SEP ▪ 15 SEP ▪ 29 SEP ▪ 6 OCT ▪ 3 NOV ▪ 1 DEC ▪ 8 DEC
- Colorado Springs, CO ▪ 18 AUG ▪ 17 NOV
- San Diego, CA ▪ 29 SEP ▪ 15 DEC
- Pensacola, FL ▪ 14 JUL
- ***NEW*** Huntsville, AL ▪ 20 OCT

Security Controls Implementation & Assessment Workshop—4 day program

- Online Personal Classroom™ ▪ 24-27 JUL ▪ 18-21 SEP ▪ 23-26 OCT ▪ 13-16 NOV ▪ 4-7 DEC

STIG 101—1 day program

- Online Personal Classroom™ ▪ 6 JUL ▪ 5 SEP ▪ 20 OCT ▪ 9 NOV ▪ 18 DEC

Information Security Continuous Monitoring—1 day program

- Online Personal Classroom™ ▪ 28 JUL ▪ 7 SEP ▪ 8 NOV ▪ 20 DEC

RMF in the Cloud—1 day program

- Online Personal Classroom™ ▪ 5 JUL ▪ 6 SEP ▪ 19 OCT ▪ 6 NOV

RMF Project Management Advantage (PMA)—1 day program

- Online Personal Classroom™ ▪ 22 SEP ▪ 27 OCT ▪ 17 NOV ▪ 8 DEC

RMF and Supply Chain Security—1 day program

- Online Personal Classroom™ ▪ 8 SEP ▪ 18 OCT ▪ 7 NOV ▪ 19 DEC

TO REGISTER FOR ANY OF THE CLASSES ABOVE, VISIST:
REGISTER.RMF.ORG

BAI Information Security Consulting & Training