RMF TODAY ...AND TOMORROW
OCTOBER 2023
VOLUME 15, ISSUE 4

NEWSLETTER

CYBERSECURITY FRAMEWORK IS GETTING AN UPDATE!

BY KATHRYN DAILY, CISSP, CGRC, RDRP

"The biggest change that we see happening is that the scope has been expanded from focusing on critical infrastructure to all organizations, regardless of type or size. "

Cont. on Page 2

RMF AND TOILET TISSUE

BY LON J. BERMAN, CISSP, RDRP

"...Most IT systems rely on external providers such as web-based services or cloud service providers. In essence, their security issues can easily become our security issues. It's a lot like security control inheritance in that sense."

Cont. on Page 3

10 CONCEPTS FOR A THRIVING RMF PROGRAM

BY AMANDA LOWELL, RDRP

"A lot of folks get wrapped up in the nitty gritty of security controls, but what upper management and your AO are looking for is proper justification of your decisions within the RMF package. "

Cont. on Page 4

BAI NOW ISSUING DIGITAL BADGES UPON COURSE AND EXAM COMPLETION!

On August 3, 2023, BAI launched our digital badging program through Credly!

Since then, hundreds of our students and RDRP members have accepted digital badges in recognition of their continuous learning and subject mastery.

These non-repudiable badges never expire, are real-time verified, and can be easily shared via LinkedIn and in email signatures.

BAI students and RDRP members who took our training or passed the RDRP exam may fill out the form on our landing page to receive a digital badge for their achievements: https://rmf.org/bai-digital-badges/

Upon submission of the form, we will touch base with you to issue a badge in the next 7-10 business days.

Thank you for choosing BAI for your continuing education and professional development!

Risk Management Framework Today... *and Tomorrow*

In This Issue:

BAI Information Security RMF Resource Center

https://rmf.org

CYBERSECURITY FRAMEWORK IS GETTING AN UPDATE!

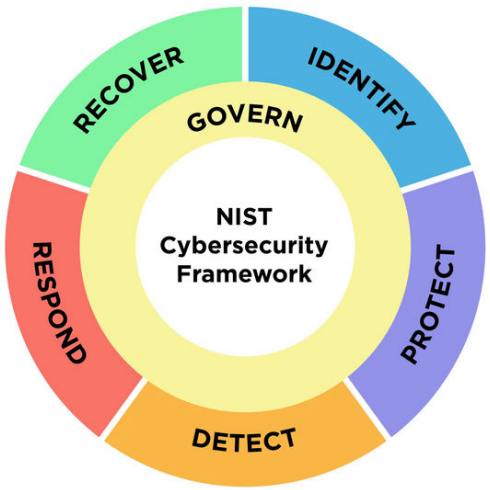
BY KATHRYN DAILY, CISSP, CGRC, RDRP

Over a decade ago NIST published the Cybersecurity Framework as a base set of standards, guidelines, and best practices to manage cybersecurity risks for critical infrastructure. While it is currently voluntary for critical infrastructure, Executive Order 13800, May 11, 2017, required federal agencies to, "Use the Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agencies cybersecurity risk."

Since its inception, the NIST CSF has become an integral resource to help organizations develop security programs even outside of the federal government and critical infrastructure and as such, the publication of CSF 2.0 Initial Public Draft (IPD) in August 2023 has generated a lot of conversation on online forums within the cybersecurity community. NIST has sought considerable amounts of feedback from the commercial sector, government sector, and academia for the development of CSF 2.0.

The biggest change that we see happening is that the scope has been expanded from focusing on critical infrastructure to all organizations, regardless of type or size. In fact, the title of the document has changed from, "Framework for Improving Critical Infrastructure Cybersecurity" to simply, "The Cybersecurity Framework."

NIST also saw fit to introduce the "Govern" pillar to cover organizational context. In terms of governance, risk, and compliance (GRC), govern(ance) is the set of policies, rules, or frameworks that an organization uses to achieve its goals. In CSF, governance will include determination of priorities and risk tolerances of the organization, assessment of cybersecurity risks and impacts, establishment of cybersecurity policies and procedures, and an understanding of the roles and responsibilities. The new Govern function in CSF 2.0 will inform and support the other previously existing functions.



NIST has placed an emphasis on protecting the supply chain as supply chain attacks become more prominent. Under the new pillar, Govern, NIST has created a subcategory focused on cybersecurity supply chain and updated content to reflect the latest NIST guidance and Framework practices related to cybersecurity supply chain risk management and secure software development.

Based on a mountain of feedback, NIST provided further guidance on the implementation of CSF. NIST has provided implementation examples to provide hypothetical examples of action-oriented processes to achieve CSF subcategories. Additionally, NIST has increased the informative references to standards, guidelines, regulations, and other resources to help inform how an organization achieves the functions, categories and subcategories.

NIST continues to receive feedback on the CSF 2.0 IPD through November 4, 2023. Early 2024 is the anticipated publication of the Final CSF 2.0 document.

ASK DR. RMF!

"Privacy Potential" asks:

Dear Dr. RMF,
I currently assess a boundary that includes all of our desktops, laptops, network printers, and some local printers. There are a number of devices (i.e. desktop/laptops) that don't store Personally Identifiable Information (PII) *per se*, but will disseminate PII to our records management boundary on a daily basis. So, my interpretation is considering we process PII within this particular boundary we (desktop environment) would require a Privacy Impact Assessment (PIA). Does this sound accurate? Any assistance you may provide would be greatly appreciated.

Dr. RMF responds:

Dear "Privacy Potential",
From your description of this "workflow", Dr. RMF can see that your desktop and laptop users are gathering PII and then sending it across your system boundary into your records management systems. If that is an accurate take on what is happening on a daily basis, then absolutely your "desktop environment" *would* require a PIA.

RMF AND TOILET TISSUE

BY LON J. BERMAN, CISSP, RDRP

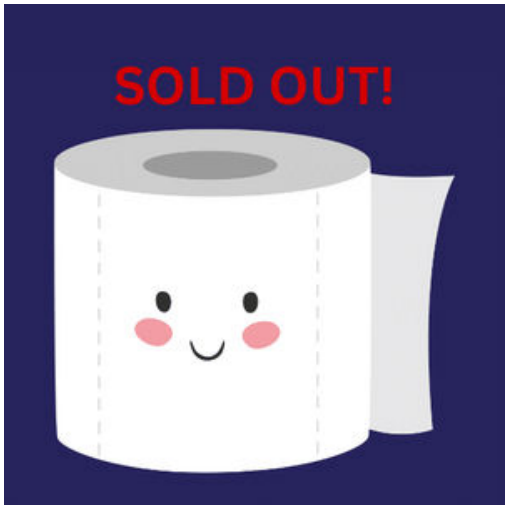
The year 2020 will be remembered for lots of things, not the least of which was the "great toilet tissue shortage." Who can forget running from store to store, only to be confronted with empty shelves? 2020 was also the year the term "supply chain" began to appear in the mainstream press. All sorts of product shortages were blamed on "supply chain issues". So, what exactly is a "supply chain" and what does it have to do with the Risk Management Framework (RMF)?

A supply chain is defined as the network of all the entities involved in the creation and sale of a product, starting with raw materials and ending with a finished product. Supply chain security is management of the supply chain that focuses on risk management of external suppliers, vendors, logistics, and transportation.

It's easy to see how our IT systems can be affected by supply chain security issues. Nearly every IT system is comprised of components acquired from external suppliers. In addition, most IT systems also rely on external providers such as web-based services or cloud service providers. In essence, their security issues can easily become our security issues. It's a lot like security control inheritance in that sense.

None of this is new to new to IT security experts. In fact, in May 2022 the National Institute of Standards and Technology (NIST) published an extensive volume of guidance on supply chain security, NIST Special Publication (SP) 800-161r1, entitled Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. This publication includes templates for key Cybersecurity Supply Chain Risk Management (C-SCRM) activities, including:

- C-SCRM Strategy and Implementation Plan
- C-SCRM Policy
- C-SCRM Plan
- C-SCRM Risk Assessment



NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, published in September 2022, contains an entire security control family dedicated to Supply Chain Management. As you probably already know, this publication is the source of the controls in the Risk Management Framework (RMF) baselines.

In other words, all information system owners are now required to include supply chain security in their comprehensive security plans and procedures. The Supply Chain Risk Management (SR) control family contains 12 security controls covering key supply chain security issues.

ARTICLE CONTINUES ON PAGE 5

ASK DR. RMF!

"Boundless" asks:

Dear Dr. RMF,
We are working on an acquisition for several new medical imaging devices in our hospital. Each of these new devices contains an embedded computer running the Linux operating system. A connection to the hospital's data network is used to send imaging data to the main hospital database. Will these systems need their own RMF ATO, or can they be included in the overall system boundary of the hospital and therefore not require a separate ATO? If the new devices require their own ATO, can we add it to the vendor's scope of work or do we have to do it ourselves?

Dr. RMF responds:

Dear "Boundless",
The question of whether to seek a separate ATO for the new imaging devices depends on the hospital's overall Assessment and Authorization (A&A) strategy. Some facilities will lump everything into a single system boundary, while others will maintain an ATO for the network infrastructure and separate ATOs for systems connecting to the network. The best way to make that determination is to approach the Authorizing Official (AO) or his/her designated representative.

As for adding RMF to the vendor's scope of work, you can certainly do that but keep in mind you'll need to provide more specific guidance than just "do RMF". You'll be far better off with specific tasking to the vendor, such as "evaluate your product against the following STIGs and make appropriate remediations to the system configuration to address non-compliant items".

10 CONCEPTS FOR A THRIVING RMF PROGRAM

BY AMANDA LOWELL, RDRP

My friends and I joke that being in the field of cybersecurity is equivalent to searching for unicorns–achieving cybersecurity is a myth…

Let me explain.

The "cybersecurity" buzzword, as it is thrown around by executives today, is a myth. The concept of security itself means protection from risk. Complete cybersecurity (aka zero residual risk) in any organization is impossible. This is why I am so passionate about unveiling security theater; to me, the ultimate form of corporate deception is lip service about security to customers that do not have the ability or access to verify those claims. What organizations should strive for (and communicate to their stakeholders!!!) is resilience against threats and effective management of risk.

Lucky me! I recently had the privilege of attending BAI's Risk Management Framework (RMF) for DoD IT Full Program + eMASS eSSENTIALS training in Pensacola, FL. Our training was developed to assist DoD personnel and contractors in establishing and maintaining a cybersecurity program in accordance with the National Institute of Standards and Technology (NIST) Risk Management Framework.

Establishing an RMF package within government information systems and achieving an authorization to operate is required to comply with the Federal Information Security Modernization Act of 2014 (FISMA). But, as with many federally required activities (I'm looking at you, taxes), navigating the "how" is more confusing than trying to understand differential calculus when you haven't yet learned to multiply.

So, I wrote this article to help ISSMs, system owners, system admins, and other folks involved in RMF using the concepts taught in our flagship training. I learned all of this from our illustrious lead RMF instructor, Linda Gross (CISM, RDRP), who boasts 40 years serving the Army in cybersecurity from the DITSCAP years, through DIACAP, and into RMF. Some of you may be facing more time/resource/personnel challenges than others, but these key takeaways will help you transition from barely surviving to thriving.

10 CONCEPTS FOR A THRIVING RMF PROGRAM:

1. Step 0: Performed throughout all steps!

RMF 2.0 introduced a new step in the 6-step lifecycle: Prepare! Entitled Step 0, the Prepare step is intended to be performed before each of the steps, not just at the beginning of the RMF Lifecycle. Each step will have a set of deliverables and individuals responsible for the activities, so make sure you have scoped and delegated the work as best as you can for each step before you try to execute.

2. Document, document, document

This may seem self-explanatory, but when folks are under-resourced, documentation is the first to go. However, you are going to need lots of evidence for your RMF package. The evidence needed can go from memorandums of understanding that offload responsibility to your service provider, to aggregations of logs with signatures proving that regular auditing is occurring. Linda put it this way: "Get credit for what you are already doing." If you have already implemented security controls in some measure (99% of you have implemented at least ONE security control), create space for the team to document the entire process, as the artifacts you create may be applicable to multiple controls.

3. Take care of the "little things"

Going off the previous point, Linda means "little things" to be small areas of non-compliance within your existing workflow that can be easily remediated. For example, if you have implemented role-based access control (RBAC) as a part of control AC-2, and you identify that one employee has not been assigned the appropriate role for his responsibilities, do not wait for the assessor or AO to come and tell you that you are non-compliant. A quick call to the domain administrator can assign the individual the least-privileged roles required to do his/her job, and the issue will be resolved before the problem trickles into later steps. "Little things" add up, and can mean the difference between an ATO, conditional ATO, and a denial of authorization to operate (DATO).

4. Know who's responsible for what–and have it on record

Your information system likely communicates with several other systems, applications, and services. Once you have decided on your system boundary (what systems are covered in your authorization process), you will be relying on the owners of other integrated IT systems and components to provide common controls and collaborate with you on hybrid controls. Make sure all inherited or hybrid controls are specifically outlined in your SLAs, MOUs, and other agreements with third parties, so you have non-repudiable evidence if those systems are found non-compliant.

ARTICLE CONTINUES ON PAGE 5

RMF TOILET TISSUE, CONTINUED FROM PAGE 2

These controls are:

- SR-1 Policy and Procedures
- SR-2 Supply Chain Risk Management Plan
- SR-3 Supply Chain Processes and Procedures
- SR-4 Provenance
- SR-5 Acquisition Strategies, Tools and Methods
- SR-6 Supplier Assessments and Reviews
- SR-7 Supply Chain Operations Security
- SR-8 Notification Agreements
- SR-9 Temper Resistance and Detection
- SR-10 Inspection of Systems or Components
- SR-11 Component Authenticity
- SR-12 Component Disposal

Wellllllllll … I admit it, I lied … a little bit! NIST SP 800-53 Rev 5 is the official policy of most federal civil agencies (e.g., Dept. of State, Treasury, Homeland Security, Health and Human Services, etc.), however it has still not been officially adopted by the Department of Defense (DoD). Official DoD policy is still based on NIST SP 800-53 Rev 4. DoD is expected to adopt Rev 5 "shortly".

10 CONCEPTS, CONTINUED FROM PAGE 3

5. All risks lead back to the ISSM

The Authorizing Official is the individual who accepts the risk for the organization, but ultimately, all risks lead to the ISSM. If you are the ISSM, responsibility for due diligence and mitigation of risk is traced back to you. Don't fall into the trap of thinking, "I assigned that responsibility to the system administrator," or "Our platform service provider handles those controls!" It is your job to ensure activities are being performed and to report to upper management when they are not. CYA!

6. Get to know key individuals

RMF is both a complex and subjective process. Every AO will have different risk tolerance levels, and different biases and preferences when it comes to your RMF package. So, Linda says to make sure you get to know your security controls assessor, system owner, authorizing official (and AODRs), third party POCs, and anyone else is involved in the process. You may not need to host their baby showers or have weekly brunch, but a basic introduction and having their contact information on hand will go a long way.

7. Use your resources: RMF Knowledge Service

We plug this all the time, but did you know there is a repository of resources for your RMF package provided by the Office of the Secretary of Defense (OSD)? The RMF Knowledge Service (RMFKS) is packed with templates in component workspaces and supplemental documents that will help you navigate each step of the RMF Lifecycle. The website has been down for a few weeks as of writing (September 28, 2023 edit: it's back up!), but the RMF Knowledge Service can be found at https://rmfks.osd.mil/ and is accessible to anyone with a Common Access Card (CAC) or External Certification Authorities (ECA) certificate (with sponsor).

8. Keep your eye on the why: Justification

A lot of folks get wrapped up in the nitty gritty of security controls, but what upper management and your AO are looking for is proper justification of your decisions within the RMF package.

This is the reason that implementation statements are critical for your security controls, so use the 5 W's method to summarize:

- Who is implementing the control,
- What actions/automation are being performed,
- When/at what intervals,
- Where (on which systems/environments)
- How are the controls implemented and the results verified?

Justification is even more important when you are trying to get more resources. Keep a record of conversations with SMEs, management, and admins on what resources are needed and how the resource would enable them to better meet requirements.

9. You can't eliminate every risk

As I mentioned in the intro to this article, it is impossible to eliminate every risk. Don't sweat the controls that are not applicable to your system. More importantly, if you request resources to implement an important control, and you can't get the funding approved, keep a record of those communications and the justification from higher-ups. Following your Risk Assessment Report (RAR), do your best to get rid of the critical risks through implementing industry-standard best practices, and account for all the "low-hanging fruit" in your Security Plan, or risks that are high impact and low in resource cost to mitigate.

10. It's dangerous to go alone!

If I've made anything clear, it's that you cannot manage the entire authorization package alone. Anyone in charge of RMF at their organization needs a team of folks trained in RMF, information security best practices, and technical aspects of security controls in order to be successful. Ultimately, it's up to you to advocate for yourself and your team to get the help you need. Don't try to do it alone–I'm rooting for you!

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 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?

"Extremely in depth classes conducted by professionals with decades in the field. Outstanding addition to my knowledge base."

- Jerry, NNL

"The instructors were not only knowledgeable but also incredibly engaging, providing real-world examples that enriched the learning process. One of the standout aspects of the course was its hands-on approach. It's evident that the BAI team is committed to delivering high-quality education that equips students with practical skills for success in the field. I wholeheartedly recommend the BAI RMF and eMASS course to anyone seeking to deepen their understanding of cybersecurity, compliance, and risk management."

- Demeko, Pueblo Chemical Depot

"Ms. Kathryn Daily was an outstanding instructor and the class was very informative! Thank you."

- Stephen, DCSA

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 MARCH, 2024:

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

- Online Personal Classroom™ ▪ 2-5 OCT ▪ 30 OCT-2 NOV ▪ 27-30 NOV ▪ 4-7 DEC ▪ 8-11 JAN ▪ 22-25 JAN ▪ 12-15 FEB ▪ 11-14 MAR ▪ 25-28 MAR
- Colorado Springs, CO ▪ 13-16 NOV ▪ 26-29 FEB
- San Diego, CA ▪ 11-14 DEC ▪ 25-28 MAR
- Pensacola, FL ▪ 5-8 FEB

eMASS eSSENTIALS—1 day program

- Online Personal Classroom™ ▪ 6 OCT ▪ 3 NOV ▪ 1 DEC ▪ 8 DEC ▪ 12 JAN ▪ 26 JAN ▪ 16 FEB ▪ 15 MAR ▪ 29 MAR
- Colorado Springs, CO ▪ 17 NOV ▪ 1 MAR
- San Diego, CA ▪ 15 DEC ▪ 29 MAR
- Pensacola, FL ▪ 9 FEB

Security Controls Implementation & Assessment Workshop—4 day program

- Online Personal Classroom™ ▪ 23-26 OCT ▪ 13-16 NOV ▪ 4-7 DEC ▪ 29 JAN-1 FEB ▪ 12-15 FEB ▪ 4-7 MAR

STIG 101—1 day program

- Online Personal Classroom™ ▪ 20 OCT ▪ 9 NOV ▪ 18 DEC ▪ 18 JAN ▪ 2 FEB ▪ 23 FEB ▪ 8 MAR ▪ 20 MAR

Information Security Continuous Monitoring—1 day program

- Online Personal Classroom™ ▪ 8 NOV ▪ 20 DEC ▪ 17 JAN ▪ 20 DEC ▪ 21 FEB ▪ 21 MAR

RMF in the Cloud—1 day program

- Online Personal Classroom™ ▪ 19 OCT ▪ 6 NOV ▪ 19 JAN ▪ 20 FEB ▪ 22 MAR

RMF Project Management Advantage (PMA)—1 day program

- Online Personal Classroom™ ▪ 27 OCT ▪ 17 NOV ▪ 8 DEC ▪ 16 FEB ▪ 18 MAR

RMF and Supply Chain Security—1 day program

- Online Personal Classroom™ ▪ 18 OCT ▪ 7 NOV ▪ 19 DEC ▪ 16 JAN ▪ 22 FEB ▪ 19 MAR

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

BAI Information Security Consulting & Training