Risk Management Framework Today…

and Tomorrow

In this issue:

Find us on LinkedIn

BAI Information Security Consulting & Training

Cybersecurity Framework – Is it relevant to Federal/DoD organizations?

By Lon J. Berman, CISSP, RDRP

Just when folks were beginning to get somewhat comfortable … or, at least, familiar … with the Risk Management Framework (RMF), along come our friends at the National Institute of Standards and Technology (NIST) throwing another framework our way! The Cybersecurity Framework (CSF) has actually been in development since 2013 and was originally intended as a voluntary set of guidelines for managing information security in Critical Infrastructure (CI) industries such as energy, transportation and health care. In recent years, CSF has begun cropping up in a variety of places beyond the CI industries, including, perhaps surprisingly, Federal and DoD agencies.

Now you may be wondering what exactly is going on. Is CSF considered relevant to Federal/DoD organizations at all? Is CSF intended to eventually replace RMF?

First of all, CSF is absolutely relevant to Federal/DoD organizations as well as private industry. CSF is a methodology for managing organizational IT risk, which is applicable to all organizations, large or small. For example, a recent DoD CIO memo on the topic of "DoD Cyber Hygiene Scorecard" states that "…a rollout of new and updated metrics will occur over the coming weeks and months in order to move the Department into additional functional elements of the Cybersecurity Framework. The focus has been mainly on the Identify function, and will now move toward the Protect, Detect, Respond and Recover functions". Evidently DoD is at the early stages of CSF implementation as a tool in their development of cybersecurity capabilities at the departmental level.

Secondly, CSF is definitely not viewed as a replacement for RMF in DoD/Federal agencies … probably a good thing, given the time and energy your organization has probably invested in RMF already and plans to invest in the near future. CSF and RMF differ fundamentally in their approaches to the cybersecurity risk management effort. CSF tends to operate at an organizational level, while RMF operates primarily at the information system level. That said, however, it is expected that CSF and RMF will be complementary within DoD/Federal organizations.

How exactly can CSF and RMF "play together"? NIST Interagency Report (NISTIR) 8170, currently in DRAFT form, attempts to answer that question by providing eight scenarios ("use cases") to illustrate some of the ways that CSF can be leveraged in the DoD/Federal space and support RMF efforts within the organization, to wit:

1. Integrating enterprise and cybersecurity risk management
2. Managing cybersecurity requirements
3. Integrating and aligning cybersecurity and acquisition processes
4. Evaluating organizational cybersecurity
5. Managing the cybersecurity program
6. Maintaining a comprehensive understanding of cybersecurity risk
7. Reporting cybersecurity risks
8. Informing the tailoring process

For example, this is NIST's take on item 5, above, "Managing Cybersecurity Risk":

Manage Cybersecurity Requirements

Benefit(s): • Determine where cybersecurity requirements overlap and/or conflict in order to ensure compliance and improve efficiency and effectiveness. • Prioritize Subcategory outcomes based on the reconciliation of requirements, as well as mission priorities and the operational environment/threat information. • Operationalize cybersecurity activities based on the Cybersecurity Framework Profile.	**Primary SP 800-39 Level:** 2 – Mission/Business Processes **Primary Cybersecurity Framework Components:** Core, Profile(s)
Summary: Federal agencies can use the Cybersecurity Framework Core Subcategories to align and deconflict cybersecurity requirements applicable to their organizations. This reconciliation of requirements helps to ensure compliance and provides input in prioritizing requirements across the organization using the subcategory outcomes. This becomes a means of operationalizing cybersecurity activities and a tool for iterative, dynamic, and prioritized risk management for the agency.	
Typical Participants: Risk Executive, Chief Information Officer, Senior Information Security Officer/Chief Information Security Officer (CISO)	
Primary NIST Documents: NIST Special Publication 800-39, Cybersecurity Framework	

NISTIR 8170, The Cybersecurity Framework: Implementation Guidance for Federal Agencies, is available online at the following URL: https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/

Risk Management Framework Today…

and Tomorrow

"…CMMC is required for every organization doing business with the DoD. If you make a nut that is used on a ship, you've got to be compliant and no one knows what the required level is for the vendor making that nut as that is up to the individual contracting office..."

Find us on LinkedIn

BAI Information Security Consulting & Training

CMMC Is Here!

By Kathryn Daily, CISSP, CAP, RDRP

So, in the last edition of the newsletter I wrote about the need for verification of NIST 171 compliance from DoD contractors, suppliers and vendors who process controlled unclassified information (CUI). Well, the DoD sure delivered on that request. A mere days after the last article was published, DoD came out with the Cybersecurity Maturity Model Certification (CMMC).

Essentially there are five levels that an organization can achieve with CMMC ranging from Level 1, basic cyber hygiene through level 5, state of the art cybersecurity practices. Each level has a different subset of requirements that builds upon the previous level(s) with level 5 having the most requirements. Each organization will be required to have an assessment done by a third party (to be determined later) and verify that they are compliant at the level they claim.

Sounds great, right? Well not exactly. NIST 171 was only required for organizations that possessed CUI. CMMC is required for every organization doing business with the Department of Defense If you make a nut that is used on a ship, you've got to be compliant and no one knows what the required level is for the vendor making that nut as that is up to the individual contracting office. We are supposed to be compliant by Fall of 2020 when the CMMC levels are added to new contracts (what happens with existing contracts is a whole different story that is still TBD), without knowing what the levels on the RFP will require. It's entirely possible that an organization will be assessed to a certain CMMC level only to find out that all of the contracts they would have bid on require a higher level CMMC. Another issue is cost. Cybersecurity compliance is never cheap, even when implemented at a low to moderate level.

Katie Arrington of DoD is in the process of a nationwide listening tour and has stated that cost should not be an issue to small business because this won't be terribly expensive. I'm saying she must not have worked for small business. This will absolutely be costly for small businesses and could be a barrier for small business and startups to get into the DoD space. Small businesses that are in the DoD space could be forced out, even when they don't process any CUI.

I like where the DoD was headed with the verification process for NIST 171, but I feel like they may have missed the mark on the compliance and certification process. Of course, the CMMC document is still a DRAFT and may very well change before the projected January, 2020 publication date.

Risk Management Framework Today…

and Tomorrow

"...A healthy dose of concern is a good thing, but there is no reason to panic. The truth is a government-owned system hosted by a commercial Cloud Service Provider (CSP) is not that much different than a system hosted in a government data center..."

Find us on LinkedIn

BAI Information Security Consulting & Training

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 is a Ph.D. researcher with a primary research focus of RMF.

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

Dear Dr. RMF,

I work in an Army program and I feel like I am getting the hang of RMF, but when the heck do I schedule an independent assessment (SCA-V)?

Show Me the SCA-V

Dear Show Me the SCA-V,

When determining when to schedule a SCA-V assessment you'll want to take several things into consideration. First you need to know when your current ATO expires. Next you'll need to know a ballpark timeframe when your team will be ready for the assessment, but you'll have to know this early enough in advance to get on the schedule. The SCA-V teams stay busy so expect to schedule several months prior to when you want the assessment done. Last but not least, make sure you have a budget in place for the SCA-V assessment!

Dear Dr. RMF,

I am a new doctoral student that is having a hard time nailing down a research topic. I work as an Information Systems Security Officer (ISSO) within the DoD, and I have experience with the RMF. I'm currently pursuing the Doctor of Information Technology degree with a specialization in Information Assurance and Cybersecurity. I have tried to find a research topic that focuses on RMF, but I have not been successful. Could you recommend a research topic within RMF? Any help would be greatly appreciated.

Elusive Research Topic

Dear Elusive Research Topic,

I feel your pain on this one as I was in your shoes not long ago. First off, you've probably already observed that not very much peer-reviewed research has been done on RMF. The lack of research makes literature reviews challenging, but it also provides evidence of a significant gap in research. When I was trying to figure out my own dissertation topic, I even went as far as asking Dr. Ron Ross if he knew of any peer-reviewed RMF research. Dr. Ross emailed me back relatively quickly and indicated that he was not familiar with any peer reviewed research on the implementation of RMF.

Taking this all into consideration, I suggest thinking about the aspects of RMF that intrigue you or even frustrate you.

Once you're zeroed in on a broad topic, start thinking about whether you are interested in qualitative or quantitative methods (don't be scared of statistics), and establish your variables. Once that groundwork is done, you should have the general direction of your research topic.

Overall, you're going to be spending a lot time analyzing the variables you select, so I suggest they are something that you are really passionate about. Also, don't be shy about data collection. One of my biggest regrets of my dissertation research was not collecting enough varied data. If I had collected more data, I think I could publish more than a few articles from my data collection.

Good luck! Keep your eyes on the prize.

Risk Management Framework Today…

and Tomorrow

"...I ask that you help me in gaining clarification on CMMC expectations and projections so that I can share it with Arrington and DoD..."

Find us on LinkedIn

BAI Information Security Consulting & Training

Will CMMC be the death of small contractors?

By Philip D. Schall CISSP, RDRP

Dear DoD Contractors:

As you likely know from reading Kathryn Daily's article earlier in this newsletter, the DoD is preparing to roll out cybersecurity contractor requirements via CMMC that are very time and cost intensive. Many concerns have come up regarding CMMC which question the DoD's aggressive timelines and the ability for small contractors to shoulder the cost of implementation. Some business leaders have gone as far to suggest that CMMC will be the death of small business.

In an article written by Lauren C. Williams in Federal Computer Week titled "Will DoD's new cyber rules crush small business?" Williams expressed concerns that small businesses could be dramatically impacted due to resource constraints. She also states that Katie Arrington, DoD's HQE Cyber for ASD (A) (Highly Qualified Expert in Cybersecurity for the Assistant Secretary of Defense for Acquisition), told reporters that CMMC should only cost a few thousand dollars. It is obvious by looking at CMMC draft guidance that this is a gross inaccuracy.

Another aspect of CMMC that is worth discussion is DoD indicating that CMMC will be an allowable cost reimbursement for contractors. This statement raises the questions of how contractor reimbursement will be handled for subcontractors. The only reasonable action for subcontractors to recoup their CMMC expenses are to raise their consulting rates which could have serious consequences in already highly competitive acquisitions.

At a recent listening session, Arrington indicated that CMMC requirements need to be in place by Fall of 2020. With no clear path forward regarding third party assessment, or the way in which subcontractors will meet these aggressive requirements, I am focusing my Fall 2020 research efforts on contractor perceptions of CMMC. I have chosen Likert scales as a research instrument to evaluate contractor perceptions of CMMC cost and CMMC timelines. In this survey research, I am also collecting open-ended responses on contractor feelings of CMMC.

I ask that you help me in gaining clarification on CMMC expectations and projections so that I can share it with Arrington and DoD. As a government contractor, these topics are very important to me, and I am sure you have similar concerns. A link to the CMMC data collection instrument can be found below. Thank you in advance for your participation in this study, and I look forward to sharing results with you early in 2020.

CMMC Perceived Competence Scales (PCS) Survey:

www.drrmf.org

V/R,

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

Risk Management Framework Today…

and Tomorrow

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

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.
- **Cybersecurity Framework (CSF) Full Program** – provides a CSF fundamentals overview and then expands on the central tenet of the Framework, which is effective risk management.
- **Security Controls Assessment (SCA) Workshop** – provides a current and well-developed approach to evaluation and testing of security controls to prove they are functioning correctly in today's IT systems.
- **eMASS eSSENTIALS** – provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS (in a simulated environment) is utilized.
- **Continuous Monitoring Overview** – 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.
- **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.
- **Certified Authorization Professional (CAP) Preparation** – led by one of the top IT certification trainers in industry, this course provides preparation for the Certified Authorization Professional (CAP) certification administered through (ISC)2.

Our training delivery methods:

- **Traditional classroom**
- **Online Personal Classroom™ (online instructor-led)**
- **Group class for your organization (on-site or online instructor-led)**

Regularly-scheduled classes through March, 2020:

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

- **Aberdeen ▪ 4 –7 NOV**
- **Dayton, ▪ 21-24 OCT**
- **National Capital Region ▪ 7-10 OCT ▪ 27 JAN -30 JAN**
- **Huntsville ▪ 9 –12 DEC ▪ 30 MAR – 2 APR**
- **Pensacola ▪ 4-7 NOV ▪ 24-27 FEB**
- **Colorado Springs ▪ 9-12 DEC ▪ 16-19 MAR**
- **San Diego ▪ 28-31 OCT ▪ 3-6 FEB**
- **San Antonio ▪ 2-5 MAR**
- **Virginia Beach ▪ 23-26 MAR**
- **Online Personal Classroom™ ▪ 7-10 OCT ▪ 18-21 NOV ▪ 16-19 DEC ▪ 13-16 JAN ▪ 10-13 FEB ▪ 9-12 MAR**

CSF Full Program—4 day program (Fundamentals and In Depth)

- **Online Personal Classroom™ ▪ 4-7 NOV**

eMASS eSSENTIALS—1 day program

- **Aberdeen ▪ 8 NOV**
- **Dayton ▪ 25 OCT**
- **National Capital Region ▪ 11 OCT ▪ 31 JAN**
- **Huntsville ▪ 13 DEC ▪ 3 APR**
- **Pensacola ▪ 8 NOV ▪ 28 FEB**
- **Colorado Springs ▪ 13 DEC ▪ 20 MAR**
- **San Diego ▪ 1 NOV ▪ 7 FEB**
- **San Antonio ▪ 6 MAR**
- **Virginia Beach ▪ 27 MAR**
- **Online Personal Classroom™ ▪ 14 NOV ▪ 23 JAN ▪ 20 FEB**

STIG 101—1 day program

- **Online Personal Classroom™ ▪ 22 NOV ▪ 20 DEC ▪ 17 JAN ▪ 14 FEB ▪ 19 FEB ▪ 13 MAR**

Continuous Monitoring Overview—1 day program

- **Online Personal Classroom™ ▪ 12 NOV ▪ 18 FEB**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 22 JAN**

CAP Prep—1 day program

- **Online Personal Classroom™ ▪ 21 FEB**

SCA Workshop—2 day program

- **Online Personal Classroom™ ▪ 13-14 NOV ▪ 26-27 FEB**