Risk Management Framework Today

… and Tomorrow

In this issue:

Find us on LinkedIn

BAI Information Security Consulting & Training

*July, 2019 Volume 9, **Issue 3***

The NIST Cybersecurity Framework

By Marilyn Fritz, CISSP

Cybersecurity is notoriously challenging, with every new day bringing more media stories about losses from endless breaches. Beleaguered cybersecurity professionals are left coping with the onslaught and, more often than not, pleading for resources. Leaders in both private and public sectors all around the globe are hammered with conflicting requests for resources. Cybersecurity outcomes can be nebulous, at best. So how to decide which wins? How are the priorities established? What works?

This is where any cybersecurity framework comes in… And where "*The*" (NIST) Cybersecurity Framework shines. So what is "It" (*the NIST Cybersecurity Framework, or "CSF"*)? Before going down that path, know that there are a number of cybersecurity frameworks – each with varying degrees of global deployment. Leading examples include ISO 27001, COBIT, and NIST's other (mega) NIST Risk Management Framework (RMF), which leverages NIST SP 800-53 controls. A security framework is intended to guide the management and implementation of security programs and associated controls. Basically, all frameworks consist of a set of processes and information security control sets (think *anti-virus, back-ups, awareness and training*) that align strategy with implementation in an effort to define priorities for resource allocation that mitigate risk. However, the challenge often lies in how to understand the security posture of organizations that have implemented different frameworks. This is one place that the CSF does a pretty good job. That is, the CSF can be used as an overlay, or translator, for other, disparate cybersecurity frameworks. Or, it can serve independently.

Originally intended for critical infrastructure ("basic survival systems" such as healthcare, financial, energy, communications, among others), the CSF flexibility, common language and potential rigor have been a boon to its adoption. It can be implemented with relative ease irrespective of the environment, and executives appreciate the value of a framework that they can understand. This has speeded the path for global adoption - and the CSF is breaking records on that score.

The CSF was developed by the National Institute for Standards in Technology (NIST), an agency of the U.S. Department of Commerce. The NIST mission is to promote innovation and industrial competitiveness. It is the same agency that created the rigorous Risk Management Framework, or "RMF", mandated by the President for use by the U.S. Department of Defense (DoD) and Federal government information systems. So NIST has credibility. Furthermore, the CSF leverage the same NIST SP 800-53 information security control set used by the RMF. It gets better, because the CSF was created with ongoing, extensive collaboration among multiple representatives in the private and public sector. It is also current, with regular updates to address evolving threats such as supply chain risk management (SCRM), and Internet of Things (IoT) and artificial intelligence (AI) - to name a few.

As with any such framework, the CSF lays out an iterative process for identifying and mitigating cybersecurity risk. The CSF does present its own language, but is readily recognized to match with terminology in other, more established frameworks, and is relatively easy for those who hold the purse strings to understand, even the occasional luddite. The CSF consists of an iterative 7-step model for "Establishing or Improving a Cybersecurity Program." These are: 1. *Prioritize and Scope*; 2.*Orient*; 3. *Create a Current Profile*; 4.*Conduct a Risk Assessment*; 5. *Create a Target Profile*; 6. Determine, Analyze and Prioritize Gaps; 7. *Implement Action Plan*. The following are key components integral to these steps:

The Framework Core, which defines five functions (*Identify, Detect, Protect, Respond, Recover*), each containing **Categories and Sub-categories** of tasks and sub-tasks. For example, the *Identify* Function includes the Category, *Supply Chain Risk Management (SCRM),* which consists of multiple **Sub-categories.** For the Identify SCRM Category, one Sub-category task is: "*Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process*."

See *The NIST Cybersecurity Framework…* Page 2

Risk Management Framework Today

… and Tomorrow

"…Contractors are required to submit a self-attestation, or a documented "pinky swear", that they are compliant with the controls in the NIST SP 800-171. ..."

Find us on LinkedIn

BAI Information Security Consulting & Training

Third Party Cybersecurity Assessments for Contractors

By Kathryn Daily, CISSP, CAP, RDRP

That's an eye-catching headline, right? Unfortunately, it's not actually a thing, at least not yet, but will be in the future, if I get my way. Currently, all federal information systems are required to go through an Assessment and Authorization (A&A) process to be in compliance with the Federal Information Security Modernization Act (FISMA) in order to store, process or transmit government information. Vendors who possess that same information are held to a much lower standard and thus hold a greater amount of risk.

In December of 2015 the U.S. Department of Defense published a three-page interim rule to the Defense Federal Acquisition Supplement (DFARS) that gave government contractors a deadline of 31 December 2017 to implement the requirements of the NIST Special Publication (SP) 800-171. These requirements protect the confidentiality of Controlled Unclassified Information (CUI) in non-federal systems and organizations. As of now, there is very little, or no oversight into how or if contractors are complying with these requirements. Contractors are required to submit a self-attestation, or a documented pinky swear, that they are compliant with the controls in the NIST SP 800-171.

In my opinion, that's not enough. There needs to be independent validation that contractors are in fact compliant with these requirements. The DoD doesn't have the bandwidth to do these verifications for all contractors but they could authorize companies to perform third-party assessments to provide the much needed assurance. Some may argue that the expense of a third-party assessment would be a barrier for small and medium sized companies, and while they may be correct, you have to understand that cybersecurity isn't, and shouldn't be, cheap. Cutting corners and not meeting requirements leaves government information susceptible to a breach and I think we can all agree that no one wants that.

The NIST Cybersecurity Framework...

Each Sub-category in turn refers to multiple "**Information References**" consisting of detailed "how to" tasks that provide detailed information on how to meet this requirement. The CSF points to Information References for several other frameworks. This serves as a cross-mapping, which enables the overlay, or translation, capability. The granularity in the Information References provide flexibility and varying degrees of rigor so that it can be effective for most private and public sector organizations, despite differences in existing framework, the organization's size, complexity or required rigor for the intended security posture.

Implementation Tiers: The CSF proposes four levels of implementation similar to the notion of a maturity model. The highest level indicates the strongest implementation. An organization assigns Tiers to determine **Current** and **Target Profiles**. The gap between the two serves to define a roadmap that aligns to the organization's strategy and goals – stuff purse string holders really appreciate. This allows them to review and reflect on things like the legal/regulatory requirements and industry best practices… And to make informed resource allocation decisions for prioritizing risk management efforts – the gold that the CSF offers within a reasonable grasp.

Risk Management Framework Today

… and Tomorrow

"...As RMF and eMASS subject matter experts, we are intimately familiar with RMF tools and processes, and in our experience many of our students think they have a good idea of how RMF and eMASS function when in actuality they do not! ..."

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 was wondering if you could guide me to the official "source" for all SOP's required for RMF. I have copies of SOP's I have done for another group but these were built off templates we were given from our ISSM at the time. I have combed over the RMF site as well as the NIST site. I feel like I am missing a key source for these types of materials. Any help would be greatly appreciated.

SOP Templates

Dear SOP Templates,

As much as I hate to break the news to you, no official source for RMF templates exists. Our best recommendations are to review your previous SOP's and create new documentation for the system you are working on. There is no required format for RMF artifacts. As long as you can document how controls are being implemented you should be in good shape!

You can also check your components workspace on RMF Knowledge Services to see if their component has posted any guidance. We know some of them have templates. If you are still stuck, you could also try and contact your AODR for your organization and see if they have any templates you can use.

Good luck!

Dear Dr. RMF,

I can tell you I am definitely new to eMass. However, I have registered several packages and brought over artifacts. I have blindly (using the job aid) assigned controls, exported the spreadsheet and reimported. Haven't been able to produce the RAR or POAM. With that being said, do you still feel that this training would be beneficial?

New to eMASS

Dear New to eMASS,

We do think it would be beneficial for you to take the eMASS training. As RMF and eMASS subject matter experts, we are intimately familiar with RMF tools and processes, and in our experience many of our students think they have a good idea of how RMF and eMASS function when in actuality they do not! Your phrase of "blindly using the job aid" jumped out at me. We often find new RMF and eMASS practitioners save considerable time and effort when they have received formalized training and are confident in the implementation choices they are making.

Dear Dr. RMF,

RMF IA 4 Identification Management control is not easy. It has so many rabbit holes. I am not sure how to tackle this control. Could you please simplify this control for me. Let's say for IA 4 Identifier Management, the information system is a web application / web server. For the web application or web site, the user's digital certificate is used to log on. In this case, how would a IS prevent reuse of identifiers? Each identifier is unique. This identifier is issued and managed by DOD. Does this mean IA 4.4 (the organization manages IS identifiers by assigning identifier) be Not Applicable because the users identifier is their digital certificate Since the IA 4.4, talks about not only individuals but also devices, should we take this from the perspective of a device only? Is this control asking how we manage Active Directory name for devices? Lastly, could this control be even inheritable? The last assessor stated it should be inheritable but did not say from whom? I can't see who I could even inherit this from. Maybe a Datacenter?

Rabbit Holes

Dear Rabbit Holes,

It sounds like you're in quite the RMF tizzy. First we need to look at what the control is requiring. IA-4 pertains to individuals, groups, roles, and devices. It sounds like your individual identifier management is handled via DoD CAC. Ideally you would be able to inherit compliance for that from the agency that issues CACs but unfortunately, that's not set up for inheritance. I would suggest you consider that portion of the control compliant. The agency that issues the CAC has measures in place to ensure that they are unique, not reused, etc. Next you need to look at your system and determine if your system utilizes groups. If so, how do you manage the groups? Do the same for roles and devices. IA-4 is a complex control, but it is manageable if you take it apart and look at it piece by piece. Hope this helps!

Risk Management Framework Today

… and Tomorrow

"...The history of eMASS can be traced back to a project called Digital DITSCAP at the Defense Logistics Agency (DLA) in the early 2000's. ..."

Find us on LinkedIn

BAI Information Security Consulting & Training

The Expanding Role of eMASS

By Lon J Berman, CISSP, RDRP

The Enterprise Mission Assurance Support Service (eMASS) is a DoD system that serves as an information repository and workflow manager for the Risk Management Framework (RMF) process. The history of eMASS can be traced back to a project called Digital DITSCAP at the Defense Logistics Agency (DLA) in the early 2000's. From those humble beginnings, eMASS has grown to become the *de facto* standard for RMF support across DoD. While not *every* DoD agency uses eMASS, it is by far the most prevalent support tool for DoD RMF. The functionality of eMASS has grown as well, as numerous new subsystems and features have been added to better support DoD organizations and system owners. Through a combination of formal training and on-the-job experience, the eMASS user community is becoming more adept at working with this tool and fully utilizing its broad range of functionality. Here are some ways in which the role of eMASS is continuing to expand:

Asset Manager. This eMASS subsystem enables system owners to record asset information on servers, workstations, network devices, etc., and upload applicable scans and Security Technical Implementation Guide (STIG) checklists. eMASS automatically applies a "mapping" of STIG items to security controls such that any STIG item that is not implemented will result in a corresponding security control being labeled as non-compliant. Use of Asset Manager has been on the increase for some time. Many DoD organizations now require at least a "sample" of each system's assets to be recorded in Asset Manager, with scans and STIG checklists applied as appropriate.

Assess-Only. DoD Instruction 8510.01 identifies two distinct RMF processes. "Assess and Authorize" is the traditional RMF process, leading to ATO, and is applicable to systems such as enclaves, major applications and PIT systems. "Assess Only" is a simplified process that applies to IT "below the system level", such as hardware and software products. Several DoD components have begun using the Assess Only process as a successor to their legacy Certificate of Networthiness or Approved Products List programs.

Defense Security Service (DSS). DSS has embraced eMASS as its standard support tool for RMF within the National Industrial Security Program (NISP). eMASS has been customized to support the classified contractor community, including specific security control baselines and overlays for various IT configurations, including Single-user Standalone (SUSA), Multi-user Standalone (MUSA), etc. Classified contractors are now required to use NISP eMASS to document their compliance, build their RMF packages and submit to DSS for approval (ATO).

FISMA. System owners are required to record certain FISMA items, such as ATO expiration dates, contingency plan test dates, etc. eMASS has always provided "place holders" for this type of information, but traditionally, each DoD component's IT Program Registry or Portfolio Management System has been the authoritative repository. Of late, however, DoD organizations are beginning to rely on eMASS as the authoritative source for the information from which their FISMA metrics are derived.

Expansion beyond DoD. Probably the most interesting … and surprising … expansion of eMASS has been its adoption by the Department of Veterans Affairs (VA). This represents the first significant use of eMASS outside of DoD. It will be interesting to see if this is the start of a trend. Could widespread adoption of eMASS among civil agencies or the intelligence community be in our future? Only time will tell.

eMASS eSSENTIALS

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 upcoming 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, security controls, and transition to RMF.
- **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.
- **CSF Fundamentals** – provides a high-level view of CSF. Discussion is centered on identifying the primary drivers (policy and guidance), differentiating amongst the Cybersecurity Framework Core (including functions, categories, subcategories and information references).
- **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.

Regularly-scheduled classes through December, 2019:

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

- **Aberdeen ▪ 12 –15 AUG ▪ 4 –7 NOV**
- **Dayton, ▪ 22-25 JUL ▪ 21-24 OCT**
- **National Capital Region ▪ 15-18 JUL ▪ 7-10 OCT**
- **Huntsville ▪ 9 –12 SEP ▪ 9 –12 DEC**
- **Pensacola ▪ 5-8 AUG ▪ 4-7 NOV**
- **Colorado Springs ▪ 23-26 SEP ▪ 9-12 DEC**
- **San Diego ▪ 29 JUL-1 AUG ▪ 28-31 OCT**
- **San Antonio ▪ 19-22 AUG**
- **Southern Maryland ▪ 23-26 SEP**
- **Virginia Beach ▪ 9-12 SEP**
- **Online Personal Classroom™ ▪ 8-11 JUL ▪ 12-15 AUG ▪ 16-19 SEP ▪ 7-10 OCT ▪ 18-21 NOV ▪ 16-19 DEC**

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

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

CSF Fundamentals —1day program

- **Online Personal Classroom™ ▪ 7 AUG ▪ 2 OCT ▪ 4 NOV**

eMASS eSSENTIALS—1 day program

- **Aberdeen ▪ 16 AUG ▪ 8 NOV**
- **Dayton ▪ 26 JUL ▪ 25 OCT**
- **National Capital Region ▪ 19 JUL ▪ 11 OCT**
- **Huntsville ▪ 13 SEP ▪ 13 DEC**
- **Pensacola ▪ 9 AUG ▪ 8 NOV**
- **Colorado Springs ▪ 27 SEP ▪ 13 DEC**
- **San Diego ▪ 2 AUG ▪ 1 NOV**
- **San Antonio ▪ 23 AUG**
- **Southern Maryland ▪ 27 SEP**
- **Virginia Beach ▪ 13 SEP**
- **Online Personal Classroom™ ▪ 23 JUL ▪ 20 AUG ▪ 20 SEP ▪ 14 NOV**

STIG 101—1 day program

- **Online Personal Classroom™ ▪ 12 JUL ▪ 16 AUG ▪ 20 SEP ▪ 11 OCT ▪ 22 NOV ▪ 20 DEC**

Continuous Monitoring Overview—1 day program

- **Online Personal Classroom™ ▪ 4 SEP ▪ 12 NOV**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 5 SEP ▪ 13 NOV**

SCA Workshop—2 day program

- **Online Personal Classroom™ ▪ 23-24 JUL ▪ 10-11 SEP ▪ 13-14 NOV**