Risk Management Framework Today

… and Tomorrow

October, 2018
Volume 8, Issue 4

Find us on LinkedIn

In this issue:

Is RMF Broken?
Can it be fixed or is it beyond repair?

By Lon J. Berman CISSP, RDRP

Thanks to the work of the Joint Task Force, RMF is now the official information security life cycle process across all three "segments" of the Executive Branch, i.e., DoD, federal civil agencies, and the intelligence community. It's now been 4 ½ years since DoD officially "adopted" RMF (DoDI 8510.01, published in March of 2014) … and much longer for many of the other federal departments/agencies.

There is a growing sentiment that somehow RMF is "broken." What exactly are the issues that have led people to come to this conclusion? The consensus seems to be that RMF is just "too time consuming and labor intensive." Some even go so far as to claim that, even if conscientiously applied, RMF does little to actually make information systems more secure.

Let's analyze these claims. There is no doubt RMF is a time-consuming process. Even for systems categorized in the Low and Moderate range, a considerable amount of time must be spent to address the vast number of security controls (and even "vaster" number of individual assessment objectives or CCIs) in the baseline. In addition to providing implementation statements for each control/CCI in the System Security Plan, the system owner will more than likely be faced with the prospect of either revising existing system documentation (such as Standard Operating Procedures) to cover the gamut of controls, or having to develop whole new documentation artifacts for various subject areas. On top of all that, the system owner will need to provide documented "evidence of compliance" (such as screen shots, copies of e-mails, etc.) for many of the controls. Overall, a daunting task for many system owners, especially in light of the fact that existing cybersecurity staff may be the only available resources with the knowledge to be able to do the work.

As if that's not enough, many organizations (agencies, commands, DoD components) compound the problem by creating review processes that further "bottleneck" the process. Even after the independent assessment is done and a POA&M has been developed, the organization's multi-layered "package approval chain" is likely to add weeks, if not months, to the overall timeframe to ATO.

To many system owners and their staff, RMF seems like nothing but a "mountain of paperwork." How can that possibly make systems more secure? After all, wouldn't it be more effective to redirect the RMF effort to something more "productive," like detecting and mitigating technical vulnerabilities that can expose systems to external attack? We certainly need to be vigilant about technical security, but history has shown that non-technical security measures (e.g., policies, procedures, training, etc.) are equally important. For example, denial of service caused by external attack and denial of service caused by a poorly trained system administrator's error are indistinguishable to the end user. Unauthorized system access due to hacker activity and unauthorized system access due to failure of the administrative process for account approval can both result in compromise of sensitive information. To be truly secure, our information security practices must be "holistic" in nature – including management and operational considerations as well as the technical. Holistic security is what RMF is all about – it's not just a meaningless paperwork exercise.

All that said, it is absolutely a daunting challenge to conscientiously apply RMF to our information systems.

See *Is RMF Broken*, Page 2

The Newest NIST Framework: The NIST Privacy Framework

By Kathryn Daily, CISSP, CAP, RDRP

NIST has announced the development of a Privacy Framework. The framework is needed to ensure the ability to design, operate, or use technologies in ways that are observant of various privacy needs in a progressively connected and complicated environment. It is expected to help manage risk by protecting people's information. Privacy risks can also arise from how organizations collect, store, use, and share this information to meet their mission or business objective, as well as how individuals interact with products and services.

NIST believes that organizations that design, operate, or use these products and services would be better able to address the full scope of privacy risk with more tools to support better implantation of privacy protections. The privacy framework will be a voluntary framework that can be used by government and industry alike. NIST will work with industry, civil society groups, academic institutions, federal agencies, state, local, territorial, tribal, and foreign governments through a series of workshops and requests for public comments over the next year in order to shape and develop the Privacy Framework. As this is a voluntary tool, there is no executive order, or other authoritative driver for NIST to develop this framework.

Resources:

NIST Privacy Framework Development Schedule
https://www.nist.gov/privacy-framework/development-schedule

***Is RMF Broken*, from Page 1**

System owners can do several key things to help meet that challenge. First of all, we need to make sure everyone involved in the process receives appropriate *training*. A soldier would not be expected to operate a communication device or a weapons system without thorough training on its proper operation. The same thing should be true for our information security "soldiers" working "in the RMF trenches." Secondly, we should be prepared to begin RMF activities early in the system life cycle, thereby minimizing the "time crunch" to get things done.

Once ATO is achieved, we should implement a continuous monitoring program that will ensure our security posture remains at a high level and minimizes the level of effort for the RMF re-authorization effort that awaits us down the road.

Agencies and organizations should also be doing their part to help system owners meet the challenge. A good start is developing and documenting policies and procedures that can be *inherited* by individual system owners. Organizations should also be working to streamline the review and approval process for RMF packages submitted by system owners. Lastly, organizations at the highest level

***… are you listening, Department of Defense?* …**

should develop and publish policies, procedures and support tools for Continuous Monitoring that can be leveraged by all.

"… are you listening, Department of Defense?..."

RMF 30-Day Sprint

By P. Devon Schall, M.S., MA.Ed. CISSP, RDRP

Over the past few months, I have heard rumblings of something called "RMF 30-Day Sprint". It came up initially during an RMF for DoD IT training I taught in Virginia Beach, and it was pitched as a new program to grant conditional one year ATO's with the only requirement being to be compliant with 36 controls. I quickly socialized "RMF 30-Day Sprint" with my team, and they countered with the question of who would choose the 36 controls and why they would be chosen. This was a valid point that I had no answer to. I brushed "RMF 30-Day Sprint" off as an idea that was discussed over a water cooler and not a reality. Well, it appears that I was wrong. After recently attending the Air Force Information Technology & Cyberpower Conference (AFITC) in Montgomery, RMF 30-Day Sprint was confirmed during an informational session I attended. This short article will provide a discussion of the driving forces of "RMF 30-Day Sprint".

"... grant conditional one year ATO's with the only requirement being to be compliant with 36 controls..."

Who?

"RMF 30-Day Sprint" is currently an Air Force initiative. At this point, I have not figured out what committee chose the 36 controls being addressed in the program.

When?

"RMF 30-Day Sprint" hasn't formally gained approval, but it was presented to me like it was already being implemented. A senior ranking Air Force official said, "RMF 30-Day Sprint has not been formally approved, but we are all preparing for it to be signed". This same person indicated that "RMF 30-Day Sprint" would span across all of DoD. I doubt this, but I also doubted this whole program, so who knows!

Why?

Authorizing Officials (AO's) and assessment teams are buried in backlogged RMF packages. "RMF 30-Day Sprint" is an attempt for teams to get caught up and work through system review in an efficient capacity. It has been expressed to me that many systems are "running in the red" and operating without an ATO.

Future Implications.

At this point, it is hard to tell if "RMF 30-Day Sprint" will catch on or if this is a one-off Air Force initiative. Although I cannot predict the success of this initiative, I can confirm that RMF practitioners are incredibly frustrated and the RMF pipeline is clogged with the process currently working very inefficiently. Early data from my RMF research is showing RMF practitioners are committed to RMF as a long-term sustainable cybersecurity framework for the US Government. I imagine the solution is going to come down to RMF practitioners figuring out a way to make RMF operate efficiently and not be a cumbersome, check the box, compliance process that is plagued with weak financial and administrative support.

RMF 30-Day Sprint Controls:

SA-4, SA-4(1), SA-4(6), SA-4(7), CM-2, CM-8, CP-9, CP-9(3), CA-3, AC- 17, AC-17 (2), AC-17(3), IA-2, IA-2(2), AC-5, AC-6, AC-6(2), AC-2, AC-2(7), CM-6, IA-4, IA-4 (2), IA-5, IA-5(1), IA-5(3), IA-5(5), IA-5(6), IA-5(7), IA-5(2), SC-12, CM-7, CM-7(3), CM-1, CM-3, CM-9, CM-10(1)

BAI Announces Security Control Assessment (SCA) Workshop

By Alice Steger, Director of Sales & Marketing

"...Security Controls Assessment Workshop provides a current and well-developed approach to evaluation and testing of security controls …"

Training Overview

Security Controls Assessment 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. This course shows you how to evaluate, examine, and test installed security controls in the world of threats and potential breach actions surrounding all industries and systems. If a system is subject to external or internal threats and vulnerabilities - which most are - then this course will provide a useful guide for how to evaluate the effectiveness of the security controls that are in place.

The **Security Control Assessment (SCA)** is a process for assessing and improving information security. It is a systematic procedure for evaluating, describing, testing and examining information system security prior to or after a system is in operation. The SCA process is used extensively in the U.S. Federal Government under the RMF Authorization process. Security assessments are conducted to support security authorization events for agencies and organizations. These assessments provide data in a tiered risk management approach to evaluate both strategic and tactical risk across the enterprise.

This security control assessment process identifies vulnerabilities and countermeasures and determines residual risks; then the residual risks are evaluated and deemed either acceptable or unacceptable. More controls must be implemented to reduce unacceptable risk and then re-evaluated. The system may be deployed only when the residual risks are acceptable to the enterprise.

Who Should Attend

The SCA Workshop is recommended for all system owners, developers and staff, and will enable them to better prepare for independent assessment by DoD or federal agencies. SCA Workshop is also recommended for those currently performing independent assessment or those who aspire to do this work.

Training Goals

The goal of the SCA activity is to *assess* the security controls using appropriate assessment procedures to determine the extent to which the controls are:

- Implemented correctly,
- Operating as intended, and
- Producing the desired outcome with respect to meeting the security requirements for the system.

Course Prerequisites

A prerequisite to this course is a strong understanding of RMF, and it is highly recommended students complete the 4-day RMF training program prior to registration.

Delivery Methods

Security Control Assessment (SCA) will initially be offered as an online, instructor-led class, using our Online Personal Classroom™ technology.

Learn More

For additional information on Security Control Assessment (SCA) training, including initial dates for *Security Control Assessment (SCA)*, please call BAI at 1-800-RMF-1903 or visit https://register.rmf.org.

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, security controls, and transition from DIACAP to RMF.
- **RMF for Federal Agencies** - recommended for Federal "civil" agency (non-DoD) employees and contractors that require detailed RMF knowledge and skill training; covers the RMF life cycle, documentation, and security controls.
- **Security Controls Assessment (SCA) Workshop** – Security Controls Assessment 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** – designed as an add-on to RMF for DoD IT. This training program provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS (in a simulated environment) is utilized.
- **RMF in the Cloud** – designed as an add-on to RMF for DoD IT. This one-day training program will provide students the knowledge needed to begin shifting their RMF efforts to a cloud environment.
- **Certified Authorization Professional (CAP) Preparation** – designed as a one-day add-on to RMF for DoD IT. CAP Prep provides preparation for the Certified Authorization Professional (CAP) certification administered through $(ISC)^2$.
- **STIG 101** – is designed to answer core questions and provide guidance and hands-on experience with the implementation of DISA Security Technical Implementation Guides (STIGs).

Our training delivery methods:

- **Traditional classroom** – regularly-scheduled training programs are offered at various locations nationwide, including Colorado Springs, Huntsville, National Capital Region (Pentagon/Crystal City area), Dallas, Pensacola, and San Diego.
- **Online Personal Classroom™** – regularly-scheduled training programs are also offered in an online, instructor-led format that enables you to actively participate from the comfort of your home or office
- **On-site training** – our instructors are available to deliver any of our training programs to a group of students from *your* organization at *your* site; please contact BAI at 1-800-RMF-1903 to discuss your requirements

Regularly-scheduled classes through March, 2019:

RMF for DoD IT—4 day program

- **Colorado Springs ▪ 3-6 DEC ▪ 18-21 MAR**
- **Dallas ▪ 29 OCT - 1 NOV ▪ 25 - 28 FEB**
- **Huntsville ▪ 10 - 13 DEC ▪ 11 - 14 MAR**
- **National Capital Region ▪ 28-31 JAN**
- **Pensacola ▪ 5-8 NOV ▪ 11-14 FEB**
- **San Diego ▪ 28-31 JAN**
- **Online Personal Classroom™**
  ▪ 22 - 25 OCT ▪ 26 - 29 NOV ▪ 10 - 13 DEC
  ▪ 14– 17 JAN ▪ 25- 28 FEB ▪ 25- 28 MAR

RMF for Federal Agencies—4 day program

- **Online Personal Classroom™ ▪ 11-14 MAR**

SCA Workshop —2 day program

- **Online Personal Classroom™ ▪ 10 - 11 DEC ▪ 20 - 21 FEB**

eMASS eSSENTIALS—1 day program

- **Colorado Springs ▪ 7 DEC ▪ 22 MAR**
- **Dallas ▪ 2 NOV ▪ 1 MAR**
- **Huntsville ▪ 14 DEC ▪ 15 MAR**
- **National Capital Region ▪ 1 FEB**
- **Pensacola ▪ 9 NOV ▪ 15 FEB**
- **San Diego ▪ 1 FEB**
- **Online Personal Classroom™**
  ▪ 13 NOV ▪ 24 JAN ▪ 21 FEB ▪ 6 MAR

STIG 101—1 day program

- **Online Personal Classroom™**
  ▪ 26 OCT ▪ 14 NOV ▪ 30 NOV ▪ 14 DEC ▪ 18 JAN
  ▪ 20 FEB ▪ 1 MAR ▪ 7 MAR ▪ 29 MAR

Continuous Monitoring Overview —1 day program

- **Online Personal Classroom™ ▪ 5 MAR**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 15 NOV ▪ 8 MAR**

CAP Prep—1 day program

- **Online Personal Classroom™ ▪ 29 OCT**

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.

BAI