Risk Management Framework Today

… and Tomorrow

In this issue:

Find us on LinkedIn

BAI Information Security Consulting & Training

*April, 2019 Volume 9, **Issue 2***

Security Control Inheritance

By Lon J. Berman CISSP, RDRP

CNSSI 4009 defines Security Control Inheritance as "a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application".

The typical example of inheritance is that of a web application or other information system hosted within a government data center. The data center has established physical, environmental and network security protections such as door locks, guards, power controls, temperature controls, network boundary security, etc. These types of controls will typically inure to the benefit of all the information systems hosted within that data center. Establishing a formal "inheritance relationship" for these controls enables the data center's compliance to be leveraged by the hosted systems, thus simplifying the RMF effort for each hosted system.

Another example of inheritance is that of an organization's "front office" that has put in place various policies intended for use by subordinate entities within the organization. Each of the information systems owned by the subordinate entities can inherit compliance with specific security controls based on the existence of those organizational-level policies.

In many of the NIST publications dealing with RMF, inheritable controls are also referred to as "common controls" and an organization offering up common controls for inheritance is referred to as a "common control provider".

In order for a specific system (we'll call it "System A") to inherit controls from a common control provider, all of the following must be true:

1. The controls must be developed and implemented by an organization other than the system owner of "System A"

2. The controls must be implemented outside the authorization boundary of "System A"

3. There must be a formal agreement, such as a Memorandum of Agreement (MOA) or Service Level Agreement (SLA), in place between the system owner of "System A" and the provider

4. The provider must be have been assessed and authorized in accordance with their department/agency's RMF process; in other words, the common control provider needs to have Authorization to Operate (ATO)

Given requirement number 4, above, you might be wondering if commercial Cloud Service Providers, such as Amazon, are able to function as common control providers. The answer is Yes, and it is because they *do* have government ATOs through federal programs such as FedRAMP (for federal civil agencies) and the "DISA provisional authorization" that essentially extends the concept of FedRAMP into DoD.

Security controls most often offered up for inheritance by common control providers are in the Physical and Environmental (PE), Media Protection (MP) and Maintenance (MA) families. Depending on the specific common control provider, additional controls in other families may also be available for inheritance. Early in the process of establishing a hosting relationship with a data center or cloud service provider, system owners should request the list of security controls available for inheritance.

It is important to understand that inherited controls are not considered "automatically compliant". What "System A" will actually inherit is the compliance status (i.e., compliant or non-compliant) of each inherited control. Inherited controls that are considered non-compliant by the provider will also be considered as non-compliant for "System A" and must therefore be documented on the "System A" Plan of Action and Milestones (POA&M). In that case, it could be said that "System A" inherits the *risk* from the common control provider.

Implementation of some security controls is best accomplished by a combined effort between the common control provider and the hosted system owner. For example, many data centers (common control providers) offer data backup services to their hosted customers. The data center's role includes deployment of enterprise backup hardware/software, logistical arrangements for transportation of off-site backup media, etc. The hosted system owner's role includes installation and configuration of backup agent software, etc. To accommodate this scenario, common control providers can offer up hybrid controls for inheritance, in which both the common control provider and the hosted system owner have a role.

Risk Management Framework Today

… and Tomorrow

"…concepts like RMF Sprint and RMF Bridge Program are just "kicking the can down the road" regarding RMF compliance and creating misconceptions about the rigor required to successfully work through the entire RMF process and gain an ATO..."

Find us on LinkedIn

BAI Information Security Consulting & Training

RMF Conference Observations

By P. Devon Schall, PhD, CISSP, RDRP

Over the past 12 months, I have attended a handful of DoD cybersecurity conferences with the goal of convincing the DoD community that RMF training is a key solution in combatting the perceived RMF crisis. These conferences include the Air Force Information Technology & Cyberpower Conference (AFITC), the Armed Forces Communications & Electronic Association West conference (AFCEA West) as well as the Armed Forces Communications & Electronic Association conference at Fort Belvoir (AFCEA Belvoir). A few common themes are surfacing at these shows which include the idea that RMF is failing and that RMF needs to be completed faster. The goal of this article will be to discuss some of these common themes. I recognize the RMF Improvement Suggestions listed below are very controversial, so I will attempt to provide objective observations for each suggestion based on my personal experiences.

RMF Improvement Suggestions:

1. If we can make RMF like TurboTax, it will be easier and faster! So east in fact, we won't even need RMF training.

   I know some of you will be upset to hear this, but RMF requires critical thinking and manual risk evaluations. As one of my RMF mentors always told me, "tools are not the answer". Although I love the idea of creating a software tool that presents RMF like Turbo Tax, I feel like the money DoD would spend on paying contractors to create this kind of RMF software tool is unnecessary. Although RMF is a complicated process, it is manageable if proper training is delivered. The biggest issue we are seeing regarding the RMF crisis is a lack of funding. It is my observation, that the funding that would be put towards an RMF software tool would be better spent in paying RMF practitioners and increasing the cybersecurity workforce for DoD.

2. Automating RMF will make the whole process faster, easier, and more effective!

   Initially, I thought RMF automation was a great idea until I had a conversation with our lead RMF engineer about it. After relating RMF automation to STIG automation, BAI's engineer indicated that too often, automating components of RMF can end up breaking systems where they no longer function, and we don't know what steps to roll them back to a functional state. RMF was created to be a risk management process that requires organic thinking and risk-based decisions vs. one-click solutions.

3. If we can create a minimized streamlined set of controls to grant folks ATO's with conditions, we can clear up the congestion in the RMF pipeline and get things moving.

I worry concepts like RMF Sprint and RMF Bridge Program are just "kicking the can down the road" regarding RMF compliance and creating misconceptions about the rigor required to successfully work through the entire RMF process and gain an ATO. Recently, in BAI's RMF classes, we have had students tell us that they are getting ATO's with conditions by only working a small amount of controls, and the RMF process as prescribed by NIST isn't reflecting what is happening in the field. Although, the RMF process may be abridged for some, this is not necessarily a good thing. Skipping steps and rushing through RMF isn't helping with the cybersecurity posture of our systems, and it is not in line with the spirit of RMF. I understand RMF is robust and challenging, but it should never be treated as a check-the-box process to be rushed through with the sole goal of meeting requirements. At the end of the day, lazy or improperly completed RMF packages threaten national security.

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,

Government IT Security staff work with systems owners to make sure that all systems in the agency have implemented the proper Risk Management Framework (RMF) controls. Organizations have deployed technologies like eMASS, XACTA, and RSA to manage the workflow and documentation for the RMF for their systems. Yet, there is confusion about how to implement RMF when the systems move to the cloud. Should government organizations contractually mandate audits? Should the IT Security Department request the RMF packages from the cloud vendor for review? Should the vendor be required to update the RMF compliance software tools and be treated like all other systems that are part of the RMF process?

In an RMF Dilemma

Dear Dilemma,

First of all, Dr. RMF wants to reassure you that you are not alone. Numerous organizations are being "encouraged" (or "compelled") by their management to start moving systems and applications to the cloud. Most are feeling uneasy about the information security implications of the move. High on the list of their concerns is, of course, RMF.

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. Think about it. Commercial CSPs use virtualization technology to provision resources (e.g., servers) for their hosted customers. Modern government data centers are doing the same. Government data centers provide numerous RMF controls for inheritance by hosted systems. Ditto for commercial CSPs. Just like you would for a hosting data center, you'll need to ask a potential CSP for a list of the controls they are authorized to offer as inherited or shared. Government data centers have Authorization to Operate (ATO) in accordance with RMF, which provides assurance to hosted customers that they are being configured and operated in a secure fashion. CSPs are subject to a very similar process, variously called FedRAMP in the civil agency sector and DISA Provisional Authorization in the DoD world. Again, you'll need to ask potential CSPs for a copy of their FedRAMP or DISA ATO.

Government agencies are implementing solutions to facilitate the "interface" between government networks and the cloud. For example, DoD offers a Cloud Access Point (CAP) to control and monitor network traffic between government and cloud. Also, DoD Cyber Security Service Providers (CSSPs), also known as Computer Network Defense Service Providers (CNDSPs), are available to systems hosted in the cloud.

Any tools you are using to support your RMF efforts in your current environment should be applicable to the cloud environment as well. CSPs are making efforts to facilitate the use of tools, e.g., by "publishing" their suite of inheritable/sharable controls in DoD eMASS.

You will undoubtedly face numerous challenges in migrating your systems to the cloud environment, but Dr. RMF is confident the RMF challenge will be a manageable one.

Dear Dr. RMF,

First of all, just stumbled across this blog few days ago....awesome! There is piles of documentation but not enough community sourced help for the RMF process. I tried starting an RMF sub-reddit but it never took off!

I have so many questions! But one in particular that is hard to get answers: what are the pros and cons of providing inheritance?

I support a system that will automate access control processes for a number of other systems, which will interface with us through API. We handle the 2875 process, spit them a set of outputs, and their system provisions an account based on what we send. There is a number of other recertification features designed to remediate audit findings, but don't need to get into the details.

The goal is for us to provide a handful of AC controls to inherit to these connected systems. What types of considerations and risks should we keep in mind when deciding what controls to provide for inheritance?

Thank you so much!

Inheritance-r-Us

See *ASK Dr. RMF…* Page 4

Risk Management Framework Today

… and Tomorrow

"...The new framework is still in development, but we know a little about what will be included. It will be risk-based, outcome based, voluntary and non-prescriptive..."

Find us on LinkedIn

BAI Information Security Consulting & Training

NIST Privacy Framework: An Update

By Kathryn Daily, CISSP, CAP, RDRP

Back in September 2018, NIST announced their plans to develop a data privacy framework based off their cybersecurity framework that has been extremely successful in both government and private sector. NIST has worked with industry through webinars and workshops and incorporated both public and private sector feedback for the data privacy framework.

Many are questioning why a second framework is necessary. Bob Siegel, of Privacy Ref, Inc, provides a fantastic simile for the relationship between security and privacy. "Just as the drapes on a window may be considered a security safeguard that also protects privacy, an information security program provides the controls to protect personal information. Security controls limit access to personal information and protect against its unauthorized use and acquisition. It is impossible to implement a successful privacy program without the support of a security program. Just as the bars on a window help prevent intruders from entering into your home while allowing people to look inside, a security program can implement controls without regard for privacy."

As with CSF, the privacy framework will be voluntary and intended to be leveraged in addition to the CSF. Also like the CSF, the privacy framework will be developed without granular controls and focused on outcomes rather than getting organizations stuck in the definition of terms.

The new framework is still in development, but we know a little about what will be included. It will be risk-based, outcome based, voluntary and non-prescriptive. It will be adaptable to many different organizations, technologies, lifecycle phases, sectors and uses. It will provide a common and accessible language.

The development is ongoing and we'll update you with more in future editions. Keep in touch.

ASK Doctor RMF... from Page 3

Dear Inheritance-r-Us,

In spite of the fact that your sub-reddit effort was not successful, Dr. RMF commends you for trying to increase the level of communication within the RMF community.

Offering up controls for inheritance is clearly an advantage to the connected systems that interface to you. Inheritance allows them to leverage your compliance and avoid having to deploy their own technical solutions or develop their own documentation in those specific areas.

The challenge is to select controls for which you are able to provide 100% of the implementation. With the obvious exception of physical and environmental controls, there are probably only a few controls that your connected systems can fully implement solely by leveraging your implementation. For many other controls, it is far more likely that your connected systems' implementation would be a combination of your efforts and theirs. Dr. RMF recommends you consider offering them up as hybrid inherited controls.

The biggest issue that can arise from security control inheritance is that receiving systems tend to "blindly" accept everything a common control provider offers. What they should be doing is carefully reviewing each control that is offered up as inheritable and selecting for inheritance only those that they can truly comply with by virtue of the provider's implementation.

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, 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, security controls, and transition from DIACAP to RMF.
- **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.
- **Continuous Monitoring Overview** – designed as an add-on to RMF for DoD IT. This is a one day "fundamentals" program.
- **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 on the implementation of DISA Security Technical Implementation Guides (STIGs) utilizing a virtual online lab environment.

Our training delivery methods:

- **Traditional classroom**
- **Online Personal Classroom™**
- **On-site training**

Regularly-scheduled classes through September, 2019:

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

- NEW ♦ **Aberdeen, MD ▪ 12 –15 AUG**
- NEW ♦ **Dayton, OH ▪ 22-25 JUL**
- ♦ **National Capital Region ▪ 8-11 APR ▪ 15-18 JUL**
- ♦ **Huntsville ▪ 10-13 JUN ▪ 9 –12 SSEP**
- ♦ **Pensacola ▪ 6-9 MAY ▪ 5-8 AUG**
- ♦ **Colorado Springs ▪ 24-27 JUN ▪ 23-26 SEP**
- ♦ **San Diego ▪ 29 APR-2 MAY ▪ 29 JUL-1 AUG**
- ♦ **Dallas ▪ 13-16 MAY ▪ 19-22 AUG**
- ♦ **Online Personal Classroom™ ▪ 15-18 APR ▪ 20-23 MAY ▪ 17-20 JUNE ▪ 8-11 JUL ▪ 12-15 AUG ▪ 16-19 SEP**

eMASS eSSENTIALS—1 day program

- NEW ♦ **Aberdeen, MD ▪ 16 AUG**
- NEW ♦ **Dayton, OH ▪ 26 JUL**
- ♦ **National Capital Region ▪ 12 APR ▪ 19 JUL**
- ♦ **Huntsville ▪ 14 JUN ▪ 13 SEP**
- ♦ **Pensacola ▪ 10 MAY ▪ 9 AUG**
- ♦ **Colorado Springs ▪ 28 JUN ▪ 27 SEP**
- ♦ **San Diego ▪ 3 MAY ▪ 2 AUG**
- ♦ **Dallas ▪ 17 MAY ▪ 23 AUG**
- ♦ **Online Personal Classroom™ ▪ 23 APR ▪ 29 MAY ▪ 18 JUN ▪ JUL 23 ▪ 20 AUG ▪ 20 SEP**

STIG 101—1 day program

- ♦ **Online Personal Classroom™ ▪ 19 APR ▪ 24 APR ▪ 24 MAY ▪ 30 MAY ▪ 21 JUN ▪ 26 JUN ▪ 12 JUL ▪ 16 AUG ▪ 20 SEP**

Continuous Monitoring Overview—1 day program

- ♦ **Online Personal Classroom™ ▪ 20 JUN ▪ 4 SEP**

RMF in the Cloud—1 day program

- ♦ **Online Personal Classroom™ ▪ 19 JUN ▪ 5 SEP**

SCA Workshop—2 day program

- ♦ **Online Personal Classroom™ ▪ 21-22 MAY ▪ 24-25 JUL ▪ 10-11 SEP**