Risk Management Framework Today

… and Tomorrow

In this issue:

Find us on LinkedIn

BAI Information Security Consulting & Training

Powerful but not well understood: Reciprocity, Type Authorization, and Assess Only

By Lon J. Berman CISSP, RDRP

All of us who have spent time working with RMF have come to understand just what a time-consuming and resource-intensive process it can be. As bad as that may be, it is made even worse when the same application or system ends up going through the RMF process multiple times in order to be approved for operation in a distributed environment (i.e., multiple locations). It turns out RMF supports three approaches that can potentially reduce the occurrence of redundant compliance analysis, testing, documentation and approval. These are: Reciprocity, Type Authorization, and Assess Only. This article will introduce each of them and provide some guidance on their appropriate use … and potential abuse!

Reciprocity

According to the RMF Knowledge Service, Cybersecurity Reciprocity is designed to "reduce redundant testing, assessing and documentation, and the associated costs in time and resources." The idea is that an information system with an ATO from one organization can be readily accepted into another organization's enclave or site without the need for a new ATO. For this to occur, the receiving organization must:

- Review the complete security authorization package (typically in eMASS)
- Determine the security impact of installing the deployed system within the receiving enclave or site
- Determine the risk of hosting the deployed system within the enclave or site
- If the risk is acceptable, execute a documented agreement (MOU, MOA or SLA) with the deploying organization for maintenance and monitoring of the system
- Update the receiving enclave or site authorization documentation to include the deployed system

It should be noted the receiving organization must already have an ATO for the enclave or site into which the deployed system will be installed.

Reciprocity can be applied not only to DoD, but also to deploying or receiving organizations in other federal departments or agencies.

Type Authorization

Type Authorization is a specific variant of reciprocity in which an originating organization develops an information system with the explicit purpose of deploying said system to a variety of organizations and locations. Per DoD 8510.01, Type Authorization "allows a single security authorization package to be developed for an archetype (common) version of a system, and the issuance of a single authorization decision (ATO) that is applicable to multiple deployed instances of the system." Type authorization is used to deploy identical copies of the system in specified environments. Type authorized systems typically include a set of installation and configuration requirements for the receiving site.

The receiving organization Authorizing Official (AO) can accept the originating organization's ATO package as authorized. This permits the receiving organization to incorporate the type-authorized system into its existing enclave or site ATO. A type-authorized system cannot be deployed into a site or enclave that does not have its own ATO. The receiving site is required to revise its ATO documentation (e.g., system diagram, hardware/software list, etc.) to include the type-authorized system.

Note that if revisions are required to make the type-authorized system acceptable to the receiving organization, they must pursue a separate authorization.

RMF Assess Only

IT products (hardware, software), IT services and PIT are not authorized for operation through the full RMF process. However, they must be securely configured in accordance with applicable DoD policies and security controls, and undergo special assessment of their functional and security-related capabilities and deficiencies. This is referred to as "RMF Assess Only".

The Information Systems Security Manager (ISSM) is responsible for ensuring all products, services and PIT have completed the required evaluation and configuration processes (including configuration in accordance with applicable DoD STIGs and SRGs) prior to incorporation into or connection to an information system.

See *Powerful but not well understood…* Page 2

Risk Management Framework Today

… and Tomorrow

"… BAI has long taught that "Prepare is Step 0" in its RMF fundamentals and In-Depth courses..." owners will need to address any of this..."

Find us on LinkedIn

BAI Information Security Consulting & Training

NIST 800-37 Rev 2: It's Official!

By Kathryn Daily, CISSP, RDRP

NIST has officially released NIST 800-37 Rev 2 and dubbed it as "RMF 2.0." The framework has been updated to include both cybersecurity and privacy to be key for an authorization decision.

"RMF 2.0 gives federal agencies a very powerful tool to manage both security and privacy risks from a single, unified framework," said Ron Ross, a fellow at NIST. "It ensures the term compliance means real cybersecurity and privacy risk management–not just satisfying a static set of controls in a checklist."

According to the framework, "The unified and collaborative approach to bring security and privacy evidence together in a single authorization package will support authorizing officials with critical information from security and privacy professionals to help inform the authorization decision,"

BAI has long taught that "Prepare is Step 0" in its RMF fundamentals and In-Depth courses. RMF 2.0 makes preparation the official first step of the RMF process "to achieve more effective, efficient, and cost-effective security and privacy risk management processes."

The update also calls for maximum use of automation in executing the RMF, calling the technology "particularly useful in the assessment and continuous monitoring of controls, the preparation of authorization packages for timely decision-making, and the implementation of ongoing authorization approaches."

The risk management framework lists seven objectives for the update:

- To provide closer linkage and communication between the risk management processes and activities at the C-suite or governance level of the organization and the individuals, processes, and activities at the system and operational level of the organization;
- To institutionalize critical risk management preparatory activities at all risk management levels to facilitate a more effective, efficient, and cost-effective execution of the RMF;
- To demonstrate how the NIST Cybersecurity Framework can be aligned with the RMF and implemented using established NIST risk management processes;
- To integrate privacy risk management processes into the RMF to better support the privacy protection needs for which privacy programs are responsible;
- To promote the development of trustworthy secure software and systems by aligning life cycle-based systems engineering processes… with the relevant tasks in the RMF;
- To integrate security-related, supply chain risk management (SCRM) concepts into the RMF to address untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout the SDLC; and
- To allow for an organization-generated control selection approach to complement the traditional baseline control selection approach and support the use of the consolidated control catalog in NIST Special Publication 800-53, Revision 5

***Powerful but not well understood*... from Page 1**

Thus, the Assess Only process facilitates incorporation of new capabilities into existing approved environments, while minimizing the need for additional ATOs. Additionally, in many DoD Components, the RMF Asses Only process has replaced the legacy Certificate of Networthiness (CoN) process.

It is important to understand that RMF Assess Only is not a *de facto* Approved Products List.

Risk Management Framework Today

… and Tomorrow

"… Based on the results of this study, a significant, positive relationship exists between the receipt of formalized RMF training and perceptions of RMF effectiveness..."

Find us on LinkedIn

BAI Information Security Consulting & Training

The Results Are In!

A Quantitative Study on the Receipt of Formalized RMF Training and Perceptions of RMF Effectiveness, Sustainability, and Commitment in RMF Practitioners.

By P. Devon Schall, Ph.D., CISSP, RDRP

Over the past year, I have conducted research on the relationship between the receipt of formalized RMF training and perceptions of RMF effectiveness, sustainability, and commitment in RMF practitioners. I am very pleased to announce, I have completed the study and have some interesting results to report. This article will provide an overview of my research methods and research study findings.

Research Methods

Quantitative data on the perceived confidence, compliance commitment, and sustainability ratings for RMF were collected and used in this research. Survey research was implemented, and data were collected through a questionnaire. The intended participants in the study were those who work in the U.S. Government or serve as U.S. Government contractors with requirements of cybersecurity compliance in their job roles. The survey questionnaire was provided to the members of the LinkedIn group titled Risk Management Framework (RMF) Resource Center via a survey link posted in the group as well as a private message sent to each member of the group with an explanatory invitation. This group consists of 1779 members and was established to provide its members with the opportunity to connect in understanding RMF. The survey was presented to all group members without any prior research or bias regarding their previous RMF training received or years of experience. The data were analyzed utilizing statistical methods of descriptive statistics, analysis of variance (ANOVA) and Pearson's
Correlations.

Findings

Based on the data collected , a significant, positive relationship exists between the receipt of formalized RMF training and perceptions of RMF effectiveness. Statistical significance can be seen in ANOVA tests where there was a significant difference in the mean effective Perceived Competency Scales (PCS) Scores among those with varied levels of formal RMF training (MS = 5.388), (F [2,78] = 3.645, p < .05). Pearson's Correlation also indicated that there was a significant positive association with the Effective PCS Score and the Amount of Training Received Category, (r = .253, n = 81, p = .023).

Breaking It All Down

I conducted a quantitative (based on math and statistics) research study which delivered a survey through a LinkedIn Group titled Risk Management Framework Resource Center. The survey presented Likert-type scales which asked respondents on a 0-7 scale how strongly they identified as being effective in implementing RMF, felt committed to RMF, and felt RMF was a sustainable framework for the U.S. Government. The participants were also asked how many hours of formalized RMF training they had received.

For those who are not experts in statistical analysis, I will try to explain simply how the data were analyzed. After collecting the results of the survey, I split the data into three groups. Those groups were low (0-32 hours of formalized RMF training received), medium (32-40 hours of formalized RMF training received), and high (40+ hours of formalized RMF training received).

To establish if any statistically significant data existed, I utilized a statistical method called an Analysis of Variance (ANOVA). The ANOVA tests relates to groups (for this study my three RMF formalized training hours categories) and it indicated if a significant difference existed in any of the groups as they related to the participants answers to the 0 – 7 Likert-type scales.

In this scenario, the ANOVA test indicated that one of the three groups were significantly different from the other two.

I then used another statistical method called Duncan's Multiple Range Test to dig deeper into the data and learn that the biggest difference was between the medium group (32-40 hours of formalized RMF training received) and the high group (40+ hours of formalized RMF training received).
The conclusion from the ANOVA paired with Duncan's Multiple Range Test was that RMF practitioners who receive 40+ hours of formalized RMF training showed a statistically significant increase in their confidence in being proficient and effective

See *The Results are In!...* Page 5

Risk Management Framework Today

… and Tomorrow

"...Being overwhelmed at the start of the RMF process is VERY common. You are not alone, in my opinion, the majority of RMF issues are rooted in folks being overwhelmed with the sheer volume of RMF information..."

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 Doctor RMF,

We just received our report from Alex, our independent assessor team lead, and there were a surprising number of findings that were listed as "conflicted controls." Betty, our ISSM, said it has something to do with STIG compliance, but I'm not sure how that relates to the various controls that are being reported as conflicted. She said we can address these issues by putting them on our POA&M, but I don't want to do that without understanding exactly what is conflicted and why. I looked through DoDI 8510.01, CNSSI 1253 and NIST SP 800-53, and I don't see any reference to "conflicted controls". I thought we did a pretty good job preparing the RMF package and I am surprised at these results. The whole thing is giving me a headache and I need some "medical" advice. Please, Doctor, can you enlighten us on what is going on here?

Frustrated in Fayetteville

Dear Frustrated,

I absolutely understand your confusion regarding STIG compliance. When I began learning RMF, I had similar RMF headaches. The remedy to your headaches are understanding that these conflicts are coming from the files you have imported from STIG Viewer. These Continuous Monitoring and Risk Scoring (CMRS) files include STIG compliance results from Security Content Automation Protocol (SCAP) scans as well as "manually entered" STIG results. Each individual STIG item is associated with a control (or, more accurately, with a CCI). In your case, one or more non-compliant STIG settings are associated with controls that you previously marked as compliant in eMASS. You should visit each of the findings in asset manager and determine if they can be made compliant (which will require a new CMRS import and possibly a new SCAP scan). If the "conflicting" STIG items cannot be made compliant, you'll need to change the status of a control/assessment procedure to Not Compliant in eMASS and create a POA&M item for that finding. Once eMASS matches the findings from your imported CMRS file you will no longer have these "conflicted controls".

Dear Doctor RMF,

My organization is developing a new system and we were told by our command that we need to pursue an ATO in accordance with RMF. Unfortunately, none of us has a shred of cybersecurity experience. Our manager, Carl, who is not even an IT person, instructed us to look on the RMF Knowledge Service website for guidance on what to do. Mary, one of our technical support people, suggested the DISA website. Both of these look like good sources, but frankly we were overwhelmed by the sheer volume of information out there. We couldn't even figure out where to begin. We have 12+ months to get this done, which we hope is enough time if we can get off to a good start. Dr. RMF, can you give us some concise guidance on how best to get our efforts going in the right direction?

Lost in RMF-land

Dear Lost,

Being overwhelmed at the start of the RMF process is VERY common. You are not alone, in my opinion, the majority of RMF issues are rooted in folks being overwhelmed with the sheer volume of RMF information. With the publishing of NIST 800-37 Rev 2, the first step of the RMF process is Step 0 – Prepare. I firmly believe the best way to operationalize step 0 in in the RMF process is to attend an RMF training program that is chock-full of practical guidance. Whether you choose to attend training through BAI or another organization, I strongly suggest you make sure the program which you enroll in is being taught by RMF practitioners with real-world RMF experience. Unfortunately, training classes can crop up being led by someone with minimal RMF experience teaching from a PowerPoint that was given to them by organizational leaders trying to "make a quick buck" off of the need for RMF training.

Enrolling in an RMF training program is critical to the success of RMF initiatives. As Dr. RMF, I am currently conducting peer-reviewed research to support this hypothesis. For additional information on the relationship between the receipt of formalized RMF training and perceptions of RMF effectiveness my doctoral dissertation can be found at www.rmf.org/rmfdissertation.

Risk Management Framework Today

… and Tomorrow

"...As an RMF practitioner, I am committed to improving the real-world application of RMF with the goal of mitigating the idea that RMF is failing..."

Find us on LinkedIn

BAI Information Security Consulting & Training

Ask Dr. RMF (Continued)

Dear Doctor RMF,

We recently went through RMF assessment and we were told that numerous CCIs were non-compliant because we had not provided "compelling evidence". To the best of our knowledge, we had artifacts showing policy and procedure (SOP) covering each control/CCI in our baseline. Dr. RMF, please help us understand what more we can provide in the way of evidence that will make these items compliant?

Compelled to Write

Dear Compelled,

Unfortunately, RMF can be a very subjective process! My recommendations would be to review your non-compliant CCI's and make sure you have provided evidence that sufficiently examines, interviews, and tests the controls. Although not all of these topics can be shown with physical evidence the examples below may help.

EXAMINE Review, observe, analyze assessment objects (i.e., specifications, mechanisms, or activities) to facilitate assessor understanding, clarification, or obtain evidence.

INTERVIEW Conduct discussions with individuals or groups to facilitate understanding, clarification, or obtain evidence.

TEST Run assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior. Examples: automated test tools output, system configuration screen shots.

The full body of compelling evidence for each Control/CCI should include the following:

- Policy – a statement that the organization does do what the Control/CCI mandates
- Procedure – documentation that shows how the organization does what the Control/CCI mandates
- Evidence – documentation that demonstrates that the organization is actively utilizing the documented procedure

The Results Are In!... from Page 3

To support the ANOVA results, correlation analyses were conducted and showed a significant positive relationship existed on a linear basis between the receipt of formalized RMF training and RMF practitioners' perceptions of being effective in the application of RMF. A weak trend was observed in the relationship between the receipt of formalized RMF training and perceptions of RMF commitment and no significant relationships were observed between the receipt of formalized RMF training and perceptions of RMF sustainability.

Future Research

I plan to conduct future research studies which explore the relationships between the receipt of formalized RMF training and increased RMF project efficiency and cost savings. I am confident that by showing conclusive data that formalized RMF training reduces overall project costs the RMF community can get away from the idea that anyone can learn RMF by reading NIST policy documents in their free time. As an RMF practitioner, I am committed to improving the real-world application of RMF with the goal of mitigating the idea that RMF is failing.

The entirety of my research study can be found below:

www.rmf.org/rmfdissertation

I hope I didn't you lose you in this article! Please let me know if you have any questions.

Dr. RMF

DrRMF@rmf.org

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 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 (STIGGs).

Our training delivery methods:

- **Traditional classroom** – regularly-scheduled training programs are offered at various locations nationwide, including Colorado Springs, Huntsville, National Capital Region, 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 June, 2019:

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

- **National Capital Region ▪ 28-31 JAN ▪ 8-11 APR**
- **Huntsville ▪ 11-14 MAR ▪ 13-16 MAY ▪ 10-13 JUN**
- **Pensacola ▪ 11-14 FEB ▪ 6-9 MAY**
- **Colorado Springs ▪ 18-21 MAR ▪ 24-27 JUN**
- **San Diego ▪ 28-31 JAN ▪ 29 APR-2 MAY**
- **Dallas ▪ 25-28 FEB ▪ 13-16 MAY**
- **Online Personal Classroom™ ▪ 25-28 FEB ▪ 25-28 MAR ▪ 15-18 APR ▪ 20-23 MAY ▪ 17-20 JUNE**

eMASS eSSENTIALS—1 day program

- **Online Personal Classroom™ ▪ 24 JAN ▪ 21 FEB ▪ 6 MAR ▪ 23 APR ▪ 29 MAY ▪ 18 JUN**
- **National Capital Region ▪ 1 FEB ▪ 12 APR**
- **Huntsville ▪ 15 MAR ▪ 14 JUN**
- **Pensacola ▪ 15 FEB ▪ 10 MAY**
- **Colorado Springs ▪ 22 MAR ▪ 28 JUN**
- **San Diego ▪ 1 FEB ▪ 3 MAY**
- **Dallas ▪ 1 MAR ▪ 17 MAY**

STIG 101—1 day program

- **Online Personal Classroom™ ▪ 24 APR ▪ 21 JUN ▪ 20 FEB ▪ 29 MAR ▪ 24 MAY ▪ 26 JUN ▪ 1 MAY ▪ 19 APR ▪ 30 MAY**

Continuous Monitoring Overview—1 day program

- **Online Personal Classroom™ ▪ 5 MAR ▪ 20 JUN**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 8 MAR ▪ 19 JUN**

SCA Workshop—2 day program

- **Online Personal Classroom™ ▪ 20-21 FEB ▪ 21-22 MAY**