RMF TODAY ...AND TOMORROW
JANUARY 2023
VOLUME 15, ISSUE 1

NEWSLETTER

ARMC, PART 2: THE MISSION PROBLEM

BY PHILIP D. SCHALL, PH.D., CISSP, RDRP

"It has always been my perception that a big part of the "RMF problem" is that Authorizing Official's (AO's) often do not fully understand the RMF process which leads to frustration."

Cont. on Page 2

AUTHORIZING OFFICIALS – HOW MANY? ... AND WHY?

BY LON J. BERMAN, CISSP, RDRP

"The DoD Instruction does not specify how many AOs there should be within each Component; that detail is left to the discretion of each Component's leadership (Component Head, CIO, etc.)."

Cont. on Page 3

CAP BECOMES CGRC? WHAT DOES THIS MEAN?

BY KATHRYN DAILY, CISSP, CAP, RDRP

"This update sounds great. It should provide a greater opportunity for certified professionals to move to other positions in industry, rather than just the US federal government."

Cont. on Page 4

CLASSROOM RMF AND EMASS TRAINING ARE BACK!

Enjoy the scenery after class in Colorado Springs (top), Pensacola (bottom left), or San Diego (bottom right)!

BAI RMF Resource Center is pleased to announce the return of RMF and eMASS training classrooms with the addition of our new locations in Colorado Springs, San Diego, and Pensacola!

RMF for DoD IT and Federal Agencies & eMASS eSSENTIALS ™

Colorado Springs, CO — February 27th – March 3rd and May 22nd – 26th

San Diego, CA — March 27th – 31st and June 26th – 30th

Pensacola, FL — April 17th – 21st

Register today at www.register.rmf.org!

Risk Management Framework Today... *and Tomorrow*

In This Issue:

BAI Information Security RMF Resource Center

www.rmf.org

THE ARMY RISK MANAGEMENT COUNCIL (ARMC) – PART 2
THE MISSION PROBLEM

BY PHILIP D. SCHALL, PH.D., CISSP, RDRP

For those who missed my last article titled The Authorizing Official (AO) Problem & The Army Risk Management Council (ARMC), I will provide a quick summary to bring readers up to speed. It has always been my perception that a big part of the "RMF problem" is that Authorizing Official's (AO's) often do not fully understand the RMF process which leads to frustration. The Army has proposed/is shifting to a single centralized AO process which from my understanding would work in conjunction with a new group called the Army Risk Management Council (ARMC). Goals of ARMC are to deconflict positions between AO's and take pressure off AO's making risk decisions in a vacuum.

The last update I can find indicates ARMC was to be fully staffed by May 2022. During AFCEA Fort Belvoir Industry Days on 7-9 November, I had conversations with many Army RMF practitioners, and no one was aware of any updates on ARMC. This appears to be a trend I have seen over the last few years with these initiatives being introduced in keynote speeches at major events and then followed by very slow rollouts.

In general, those I spoke with at AFCEA Belvoir had no idea about ARMC. Most had heard talk of a shift to a single AO, but not much else. This ARMC query usually resulted in the typical RMF doesn't work conversation which led to statements like "RMF is just DIACAP on steroids" or "RMF is a check the box process and a waste of time" or my personal favorite "We just need to automate RMF", but a handful of people had a single very strong and, in my opinion, very valid concern about ARMC. As an aside, it is my position that the negative statements above derive from an improper understanding of RMF application, and these negative comments are perpetuated by those with limited RMF education who do not understand the spirit of RMF.

The primary concern about a single centralized AO and ARMC is that they will not understand all the mission elements of RMF packages in the entire Army. I applaud Army leadership for consistently striving to improve and make RMF more efficient, but I believe the mission concern above is very relevant. I am sure many RMF practitioners would read this and then think about the intricacies and relationships that their current system incorporates and feel uneasy with the idea that a centralized RMF council (who may be even more out of touch than their current AO) would be making their ATO decision. Again, I have no updates on ARMC, so I cannot verify if proposed solutions to the crux referenced above are being worked out, but in publishing these articles we attempt to create discussion around RMF policies and initiatives.

If you have updates or thoughts on ARMC, I would love to hear them, please email me devon@rmf.org or drrmf@rmf.org.

ASK DR. RMF!

A reader who calls herself "Teamwork? I think not!" writes:

Dear Dr. RMF,

I am trying to put together a team to work the RMF process for a new system that's under development. I got the bright idea of having each of the team members take responsibility for the security controls that are pertinent to their area of responsibility, to include entering the data for their controls into eMASS. Sounds great, right? Well, I am getting all kinds of pushback from several of my team members. They are just not willing to go through all the steps (e.g., taking eMASS training and passing a test) required to get access to eMASS. They would rather send me their input and have someone else (i.e., me) enter it into eMASS. After all, they say, "they are not the security person", I am. My feeling about what they are doing is that it's nothing but "work avoidance" on their part. I think they are trying to take advantage of the fact that I am young and have never led a team before. What do you think, Dr. RMF? Am I justified in bringing this to the attention of my boss to see if he can use his "weight" to get these people in line?

Dear Teamwork,

What you are suggesting sounds like a good approach in theory, but the reality is eMASS does not readily support it. Your approach would work if eMASS access for each individual could be restricted to only the set of controls assigned to them. Unfortunately, eMASS does not have that level of "granularity" in its access controls. Dr. RMF feels it is not worth the risk of error to open up access to all the security controls to inexperienced individuals whose responsibility only includes a select few of the controls. It will be better in the long run if you accept the team members' input by e-mail or a shared file system and do the actual eMASS data entry yourself. Better still, Dr. RMF recommends you assign at least one other team member as your "backup" for eMASS data entry and make sure that person is fully trained and has full access to the eMASS record for your new system. With a backup person in place, the two of you could potentially "share the labor" of data entry.

AUTHORIZING OFFICIALS – HOW MANY? … AND WHY?

BY LON J. BERMAN, CISSP, RDRP

DoDI 8510.01, entitled Risk Management Framework for DoD Information Technology, specifies that "each DoD Information System (IS) … must have an authorizing official (AO) responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture." Within each DoD Component, the Component Head is responsible for appointing the AO(s) within the Component. The DoD Instruction does not specify how many AOs there should be within each Component; that detail is left to the discretion of each Component's leadership (Component Head, CIO, etc.).

Most DoD Components have opted for a single AO with responsibility for authorizing all systems within the Component. Other Components (most notably Army) have opted for a multiple AO approach, with each AO responsible for authorizing systems within a specific command or agency within the Component. In this article, I will try to explain the benefits and detriments of each approach, and perhaps provide some insight into the question of which approach is "better".

The Single AO approach is by far the most prevalent within DoD, and non-DoD departments/agencies as well. A senior official, typically a General Officer or civilian Senior Executive Service member, is appointed by the Component Head to serve as AO. Often, particularly in the larger DoD Components, the AO will employ a staff whose job it is to review incoming authorization packages and present them to the AO for final review and signature. The Single AO approach facilitates "consistency" in AO decision-making across the Component, since the same AO and staff is making all the authorization decisions.

Army is the most prominent proponent of the Multiple AO approach. Individual AOs are assigned to major commands, Program Executive Offices, etc. The principal benefit is that each AO is likely to have more familiarity with the operational needs of the specific command and thus better able to make informed authorization decisions that balance risk level against mission need. A detriment of the multiple AO approach is the potential for "inconsistency" in the decision-making process among the various AOs, as well as potentially higher aggregate cost of supporting multiple AOs.

So which approach is "better"? Clearly, for a small DoD Component (or civil agency) with relatively few IS, the Single AO approach makes the most sense. For a larger DoD Component with hundreds or even thousands of IS, serious consideration should be given to the Multiple AO approach.

Having said all that, is it likely that there will be major changes from Multiple AO to Single AO, or vice versa? The answer is probably No – the inertia of "doing things as they've always been done" will most likely win out over other considerations. Army has given some indication they are considering a move from Multiple AO to Single AO, but they are encountering considerable resistance. Bottom line is system owners just need to deal with whatever AO structure is in place for their component/agency.

ASK DR. RMF!

A friend who calls himself "AO Picking on Us?" writes:

Dear Dr. RMF,

We have dutifully followed all the RMF process steps and created all the documentation deliverables (Security Plan, Security Assessment Report, POA&M, etc.). The package was approved by the Security Control Assessor (SCA) and sent on to the AO for final ATO approval and signature … or so we thought! Now we received word that we will be required to do a formal "presentation" of our package to the AO. We were sent a Powerpoint template we will need to complete and be prepared to present. What the……? Just when we thought we were finished, another task has been thrown in our path. Nowhere in the RMF publications (DoDI 8510.01, etc.) is there any mention of such a presentation. Are we being singled out for some reason, or is this a part of everyone's RMF process (albeit undocumented)?

Dear Picking on Us,

You are correct in one sense. An AO presentation is not a part of the standard RMF process. Evidently, however, your AO does require it. Dr. RMF is quite certain your AO requires it of all system owners within his/her purview. You are not being singled out. Whether you like it or not, your AO has the authority to impose these kind of "additions" to the process, so long as they do not contradict the letter and spirit of the RMF process and security controls. Dr. RMF recommends you just "go along with it" and your life will be easier … no use trying to fight the very person who will be signing your ATO!

CAP BECOMES CGRC? WHAT DOES THIS MEAN?

BY KATHRYN DAILY, CISSP, CAP, RDRP

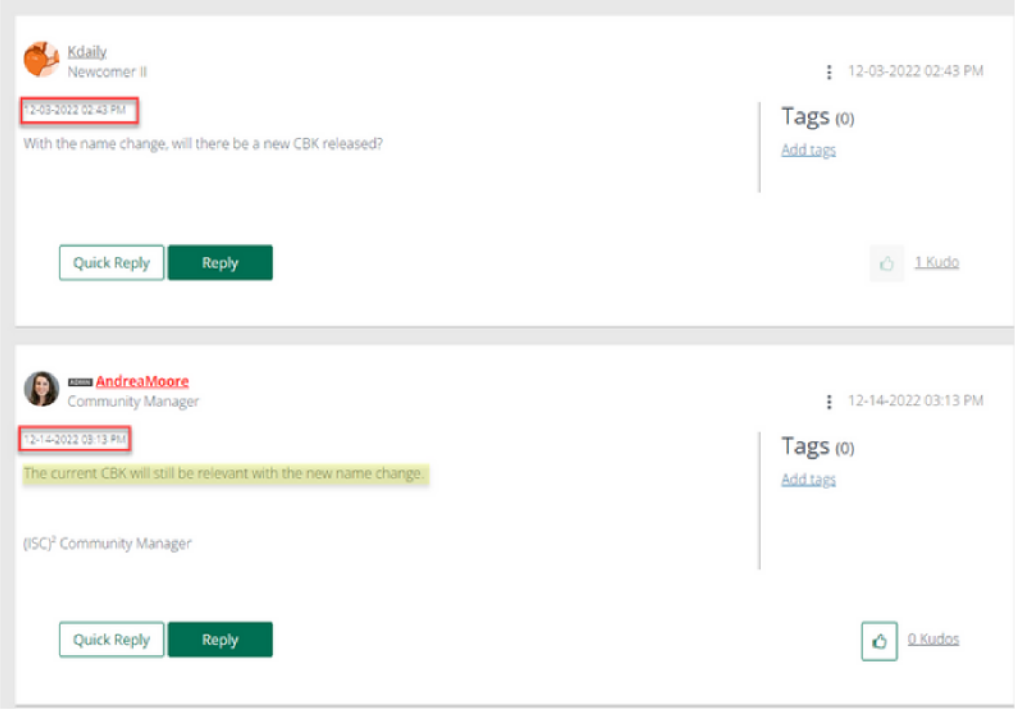
What is GRC? GRC stands for Governance, Risk, and Compliance. GRC is a set of processes and procedures to help organizations achieve business objectives, address uncertainty, and act with integrity.

In August of 2021 ISC2 updated the exam outline and content. On the ISC2 Community Forum I asked for clarification on the change. Toni Hahn stated, "With this new outline, the CAP is expanding its horizons. Everyone always thinks of it as the RMF certification but it is not - it is the Certified Authorization Professional. During the JTA and throughout the past few years, we have seen a lot of people earning their CAP who do not work for the government and do RMF. There are many risk management frameworks and under Domain 1 on the new outline you will see some listed (COBIT, ISO 27001, ISO 31000) and those are just some of the risk management frameworks out there that a Certified Authorization Professional should know about and therefore the CAP outline was expanded. The whole purpose of having a Job Task Analysis every 3 years and updating the exam outline is to see what is new and how the certification is being used. "If you reference the ISC2 CAP updated exam outline that became effective in August 2021 you'll notice they changed the domains to reflect the move away from the Risk Management Framework to include broader terminology. Domain 2 changed from "Categorization of Information Systems to Scope of Information Systems. Domain 3 and 4 changed to include privacy controls which is likely a reflection of the updated NIST SP 800-53 Rev. 5. Domain 5 changed from Assessment of Security Controls to Assessment/Audit of Security and Privacy Controls. Domain 6 changed from Authorization of Information Systems to Assessment/Audit of Security and Privacy Controls. The addition of the terms audit and assessment definitely point to the inclusion of other frameworks which tracks with the guidance provided above.

This update sounds great. It should provide a greater opportunity for certified professionals to move to other positions in industry, rather than just the US federal government.

Fast forward to December 2022, ISC2 announced the name of the certification will change from Certified Authorization Professional (CAP) to Certified in Governance, Risk, and Compliance (CGRC). Again, they stated, "This change better represents the knowledge, skills and abilities required to earn and maintain this certification. The subject matter is broader and more inclusive to frameworks used around the world." Again, this tracks with the information provided when the exam outline changed. They appear to be including other frameworks. I of course followed this up by asking if a new CBK will be published, as the current CBK, "OFFICIAL (ISC2)2 GUIDE TO THE CAP CBK, Second Edition," has a copyright date of 2013. This didn't track in my head, so I dug further. I asked in the ISC Community Forum if ISC was planning to release a new CBK. See the response below, dated 12-14-2022:

STORY CONTINUES ON PAGE 5...



CAP BECOMES CGRC? WHAT DOES THIS MEAN? (*CONT.)*

BY KATHRYN DAILY, CISSP, CAP, RDRP

Now, let's take a look at the CAP Exam Outline, (Effective Date: August 15, 2021).

Domain 1: Understand the foundation of an organization information risk management program

One bullet item states, "Risk management frameworks (e.g., National Institute of Standards and Technology (NIST), cyber security framework, Control Objectives for Information and Related Technology (COBIT), International Organization for Standardization (ISO) 27001, International Organization for Standardization (ISO) 31000". Again, this tracks with the certification moving away from pure RMF. If we look at the "still applicable CBK" we find that the only *ISO standard mentioned is ISO 17799 which has been withdrawn and incorporated into the ISO 27000 series.

Under regulatory and legal requirements, we see Federal Information Security Modernization Act (FISMA) which was released 3 years after this book was published, in 2015, so we know that's not included. The next regulatory requirement is the Federal Risk and Authorization Management Program (FedRAMP) which was released in 2011, but not included in the CBK. Next, we see General Data Protection Regulation (GDPR) which was approved by the EU Parliament in 2016 so again, we know that regulation is not included in the CBK.

Domain 3: Selection and Approval of Security and Privacy Controls

Section 3.4 mentions Information Security Management System, a component of the ISO 27001, which we've already seen is not included in the CBK.

Domain 4: Implementation of Security and Privacy Controls

First, we see the inclusion of Technical Security Standard for Information Technology (TSSIT) out of Canada. There is no mention of this in the CBK. Additionally, the United States Government Configuration Baseline (USCGB) and the Center for Internet Security (CIS) benchmarks are not mentioned in the CBK.

Based on this we can clearly see that the CBK published in 2013 does not include many of the topics listed in the updated exam outline. So let's move on to the provided supplementary resources provided.

The first observation is that they are ALL NIST 800 series documents. There are no references for the other frameworks and regulatory requirements [...] provided. It also lists the CBK and lists the publication date as April 2016. The issue there, is the Amazon page that is linked states that the book was published in 2012. There are 2 other reference books not published by ISC2 which were published in 2020, but that is still before the exam outline change in 2021 so the applicability is questionable. ISC2 even advertising this book seems unethical to me given that the references page clearly states the updated NIST publications and not the superseded or non-existent publications at the time of the CBK publishing.

Given this information, if the supplied CBK and references are accurate, this does NOT reflect the objective of the exam update and name change. If the CBK and references are NOT accurate, and these other frameworks are included, ISC is providing zero resources or guidance on the level of knowledge required for these other frameworks. Their blog post seems to indicate that any professional with experience in any of the GRC frameworks are qualified to sit for the exam, but I'm not so sure that's true.It also sounds like employers can assume that job applicants that possess the CGRC certification are knowledgeable in these other frameworks, and that too is questionable.

***** UPDATE 1-16-2023 *****

I wrote this article about 2 weeks ago, and since then it's been in the review phase prior to publishing. During that time, ISC updated their references list to include the ISOs, but none of the other frameworks. They also removed the reference to the Official CBK that they said a month ago was still relevant. Based on a search of http://web.archive.org, the change was made after December 2, 2022, but I was unable to ascertain an exact date. That change, resolves several of the issues I outlined above. It's curious that they changed the list of references in December of 2022/January 2023, immediately preceding the name change, a change that is JUST to reflect the update of the exam that occurred a year and a half ago.

WHAT IS REGISTERED DOD RMF PRACITIONER?

The Registered DoD RMF Practitioner (RDRP) program was created in response to BAI RMF Resource Center recognizing the need for a credential which shows competency and proficiency in the understanding and application of RMF for DoD. RDRP is comprised of a network of information security professionals specializing in supporting Risk Management Framework (RMF) in the Department of Defense (DoD) programs. The requirements to join RDRP are very straightforward:

Step 1: Attend 4 days or more of RMF for DoD IT training.
Step 2: Remit the initial credentialing fee.
Step 3: Complete the 50 questions "RMF for DoD IT Competency Test" with a passing score of 70%.

Being part of the RDRP registry not only adds credentialing value, but it also shows employers and government officials that registrants have a comprehensive understanding of RMF as it is implemented within DoD. Registrants are also joining a community that fosters RMF inquiry as well as networking opportunities amongst colleagues.

The only cost associated with becoming an RDRP is a one-time $100 administration fee that covers program administration. Once an RDRP candidate passes the RDRP exam and remits their $100 registration fee, they will become a lifetime RDRP member.

BAI's students who have completed 4-days or more of RMF DoD IT training may go to www.rmf.org/rdrp to begin the registration process.

Want to see more of Dr. RMF? Watch our Dr. RMF video collection at https://www.youtube.com/c/BAIInformationSecurity

What are People are Saying About Us?

Looking Forward to the Next One
"Excellent course! Great content for even those of us with limited experience in the DOD/Compliance space. Looking forward to the next one."
- Sanford
Epirus

Phenomenal
"The instructor for this course was phenomenal. Her knowledge of RMF was very helpful in answering some scenarios that I was confused on."

- Darrell
DoD Army Futures Command

Fantastic Real-World Experience
"The class was great. The instructor had fantastic real-world experience to share that helped to solidify the concepts."

- Matthew
National Guard

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.
- **RMF for Federal Agencies –** recommended for Federal Agency employees and contractors that require detailed RMF knowledge and skill training; covers the RMF life cycle, documentation, and security controls with an additional emphasis on Federal application.
- **RMF Supplement for DCSA Cleared Contractors –** covers the specifics of RMF as it applies to cleared contractor companies under the purview of the Defense Counterintelligence and Security Agency (DCSA).
- **eMASS eSSENTIALS –** provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS is exemplified in our eMASS eXPERIENCE™ simulation 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.
- **Security Controls Implementation Workshop –** provides an in-depth look into Step 3 of the Risk Management Framework process Implement Security Controls. Upon completion of the course the student can confidently return to their respective organizations and ensure the highest level of success for the most difficult part of the RMF process.
- **Security Controls Assessment Workshop –** provides a current approach to evaluation and testing of security controls to prove they are functioning correctly in today's IT systems.
- **Information Security Continuous Monitoring –** 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.
- **RMF Project Management Advantage –** provides "how to" guidance for the most commonly-used RMF strategies in project management.

OUR TRAINING DELIVERY METHODS:

- Traditional classroom
- Online Personal Classroom™ (interactive, live, instructor-led)
- Private group classes for your organization (on-site or online instructor-led)

REGULARLY-SCHEDULED CLASSES THROUGH DECEMBER, 2023:

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

- Online Personal Classroom™ ▪ 30 JAN - 2 FEB ▪ 13 - 16 FEB ▪ 13 - 16 MAR ▪ 27 - 30 MAR ▪ 3 - 6 APR ▪ 8 - 11 MAY ▪ 12 - 15 JUN ▪ 26 - 29 JUN
- Colorado Springs, CO ▪ 27 FEB - 2 MAR ▪ 22 - 25 MAY
- San Diego, CA ▪ 27 - 30 MAR ▪ 26 - 29 JUN
- Pensacola, FL ▪ 17 - 20 APR

RMF for Federal Agencies—4 day program (Fundamentals and In Depth)

- Online Personal Classroom™ ▪ 6-9 FEB ▪ 1-4 MAY

CAP Exam Prep—1 day program

- Online Personal Classroom™ ▪ 5 MAY

eMASS eSSENTIALS—1 day program

- Online Personal Classroom™ ▪ 27 JAN ▪ 3 FEB ▪ 17 FEB ▪ 17 MAR ▪ 31 MAR ▪ 7 APR ▪ 12 MAY ▪ 16 JUN ▪ 30 JUN
- Colorado Springs, CO ▪ 3 MAR ▪ 26 MAY
- San Diego, CA ▪ 31 MAR ▪ 30 JUN
- Pensacola, FL ▪ 21 APR

Security Controls Implementation & Assessment Workshop—4 day program

- Online Personal Classroom™ ▪ 6 - 9 FEB ▪ 6 - 9 MAR ▪ 24 - 27 APR ▪ 15 - 18 MAY ▪ 5 - 8 JUN

STIG 101—1 day program

- Online Personal Classroom™ ▪ 19 JAN ▪ 24 FEB ▪ 22 MAR ▪ 13 APR ▪ 19 MAY ▪ 2 JUN ▪ 20 JUN

Information Security Continuous Monitoring—1 day program

- Online Personal Classroom™ ▪ 18 JAN ▪ 22 FEB ▪ 23 MAR ▪ 11 APR ▪ 30 MAY ▪ 21 JUN

RMF in the Cloud—1 day program

- Online Personal Classroom™ ▪ 20 JAN ▪ 23 FEB ▪ 24 MAR ▪ 12 APR ▪ 1 JUN ▪ 22 JUN

RMF Project Management Advantage (PMA)—1 day program

- Online Personal Classroom™ ▪ 10 FEB ▪ 10 MAR ▪ 28 APR ▪ 9 JUN

RMF Supplement for DCSA Cleared Contractors (DCSA)—1 day program

- Online Personal Classroom™ ▪ 21 FEB ▪ 10 APR ▪ 31 MAY ▪ 23 JUN