Risk
Management
Framework
Today…

and Tomorrow

July, 2022 Volume 14, **Issue 3**

NIST Evaluation Tool for Continuous Monitoring Programs

By Lon J. Berman, CISSP, RDRP

Information Security Continuous Monitoring (ISCM) is arguably the most important step in the Risk Management Framework (RMF), since it is here that we ensure a system's level of risk is maintained at an acceptable level over the long term. The recent initiative to establish Continuous Authorization to Operate, i.e., Authorization to Operate (ATO) with no fixed expiration date, has further increased the dependency on a strong, robust ISCM program.

ISCM Publications

The National Institute of Standards and Technology (NIST) remains the number one source of information on ISCM. The key ISCM-related publications are:

- **NIST SP 800-137**
  Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (09/30/2011)
- **NIST SP 800-137A**
  Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment (05/21/2020)
- **NISTIR 8212**
  ISCMA: An Information Security Continuous Monitoring Program Assessment (03/31/2021)

The first of these (NIST SP 800-137) provides guidance on planning and establishing an ISCM program for the various information systems within your organization. The latter two publications (NIST SP 800-137A and NISTIR 8212) are all about assessing the effectiveness of an existing ISCM program.

NIST Special Publication (SP) 800-137A

This publication describes an approach for the development of Information Security Continuous Monitoring (ISCM) program assessments that can be used to evaluate ISCM programs within federal, state, and local governmental organizations and commercial enterprises. An ISCM program assessment provides organizational leadership with information on the effectiveness and completeness of the organization's ISCM program, including the review of ISCM strategies, policies, procedures, operations, and analysis of continuous monitoring data. The ISCM assessment approach can be used as presented or as the starting point for an organization-specific methodology. It includes example evaluation criteria and assessment procedures that can be applied to organizations.

NIST Interagency Report (IR) 8212

This publication describes an example methodology for assessing an organization's Information Security Continuous Monitoring (ISCM) program. It was developed directly from NIST guidance and is applicable to any organization, public or private. It can be used as documented or as the starting point for a different methodology. Included with the methodology is a reference implementation (ISCMAx tool) that is directly usable for conducting an ISCM assessment.

ISCMAx Tool

The ISCMAx tool – available from the NISTIR 8212 publication details page at: https://csrc.nist.gov/publications/detail/nistir/8212/final under "Supplemental Material" – is intended for use as a companion tool when conducting ISCM Program Assessment Reviews. ISCMAx is a macro-enabled Microsoft Excel application, suitable for use on Windows-based systems.
ISCMAx includes 128 "assessment elements."

The ISCMAx spreadsheet includes assessment objectives and recommended assessment procedures for each assess-

See NIST Evaluation Tool, Page 4 for more.

In this issue:

BAI Information Security Consulting & Training

Risk Management Framework Today...

and Tomorrow

"...We are tired of hearing that RMF is failing and inefficient. If you are interested in decreasing RMF implementation time and cost, this course is for you!"

Find us on LinkedIn

BAI Information Security Consulting & Training

Is RMF Project Management Advantage Right for Me?

By Philip D. Schall, Ph.D., CISSP, RDRP

First off, I would like to congratulate Director of Cybersecurity and Information Assurance at Army CIO/G-6, Nancy Kreidler on her recent retirement! As a self-proclaimed RMF nerd, I found one of her recent posts on LinkedIn humorous with the following lines "Step 1 – Retire. Step 2 - Recover. Step 3 - ?". In RMF circles, Ms. Kreidler is most recently known as being the champion of a project titled RMF Sentinel AKA RMF 2.0 (not be confused with Ron Ross's NIST RMF 2.0 initiative from 2017) which aimed to increase RMF efficiency and eliminate perceived RMF bottlenecks by leveraging threat-informed risk decisions.

For those who follow my articles/posts, you know that I often write about the common theme of DoD perceiving RMF as an inefficient/failed process. After being involved in thousands of RMF practitioners annually and my personal academic research being focused on improving RMF efficiency, I believe the best way to increase RMF efficiency is through delivering RMF training that was developed by RMF practitioners with the goals of getting students working RMF packages as efficiently and quickly as possible (practitioner focused training).

During an internal BAI RMF Resource Center meeting in early 2022, the question was posed of what curriculum we may be missing that could help in supporting our mission of empowering and educating the future RMF workforce. During that meeting, the idea of enlisting our senior Project Management Professional (PMP) and RMF SME to develop a one-day RMF for DoD IT Supplemental course targeted at leveraging project management best practices and BAI's real-world RMF experience was proposed.

A few months later, RMF Project Management Advantage was born!

Is RMF Project Management Advantage right for me? After chatting with our course developer, I can confidently say that RMF Project Management should appeal to a very broad audience. The audience for this course includes those with advanced and entry-level RMF experience looking to take a one-day course to brush up or learn new project managements skills and gain knowledge of project management principles.

We are tired of hearing that RMF is failing and inefficient. If you are interested in decreasing RMF implementation time and cost, this course is for you! Like RMF Sentinel, we are trying to do our part in making the RMF process more efficient without sacrificing security posture, and we are confident this one-day RMF project management intensive meets those needs!

RMF Project Management Advantage topics include:

- RMF Operation Order
- RACI Charts
- Self-Assessment Worksheet
- Understanding Common Controls
- RMF 5 Steps (as projects)
- Controls Implementation Worksheet
- RMF Project Plan
- Reporting RMF Project Progress

For additional information on RMF Project Management Advantage training, or to register for an upcoming class, please call BAI at 1-800-RMF-1903 (763-1903) or visit https://rmf.org/rmf-project-management-advantage/

"If you aren't tracking your progress through metrics, how can you tell how effective your cybersecurity program is performing?"

NIST to Update the CSF Based on Responses from Industry and More!

By Kathryn Daily, CISSP, CAP, RDRP

Back in February, NIST issued a public Request for Information (RFI) to identify how the Cyber Security Framework was being used and also for recommendations on improving the effectiveness of the Framework and its alignment with other cyber security resources.

"Every Organization needs to manage cybersecurity risk as part of doing business, whether it is in industry, government, or academia… it is critical to their resilience and our nation's economic security. There are many tools available to help, and the CSF is one of the leading frameworks for public sector cybersecurity maintenance. We want private and public sector organizations to help make it even more useful and widely used, including by small companies." - Commerce Deputy Secretary Don Graves

In response to the RFI, NIST received more than 130 responses from industry, non-profit, individuals, government, and academia.

Once NIST received the responses they were grouped into themes based on commonalities. A total of 7 themes were identified, to wit:

1. Focus on maintaining and building on the key attributes with the update.
It was generally recognized that the CSF has been effective in helping organizations understand and manage cybersecurity risk as it's flexible, easy-to-use and voluntary. That being said, many commenters requested avoiding changes to the fundamental structure of the CSF.

2. Align the CSF with existing efforts by NIST and others.
As CSF was created to provide a common organizational structure for standards, guidelines and practices, CSF supports coordination and communication within the US and internationally in an effort to strengthen cyber security. Since CSF 1.1 was released in 2018, NIST has updated several cyber resources such as the NIST SP 800-53 Rev. 5, The Privacy Framework, NICE Workforce Framework for Cyber Security, etc. Commenters recommended NIST provide guidance on how to use these frameworks and resources in concert with the CSF to achieve a more organized approach to cybersecurity.

3. Offer more guidance for implementing the CSF.
More than 500 references in the comments supported the need for more guidance on the implementation of CSF. CSF was designed to be vendor agnostic, scalable, and flexible to meet the needs of all sectors of private and public organizations. The CSF provides implementation guidance for various sectors through CSF profiles (I.e., manufacturing, election infrastructure, payroll, etc.). Comments requested that NIST offer more guidance on how to create profiles to align the CSF to more vertical markets than currently exist to aid in implementation of the CSF.

4. Ensure the CSF remains technology neutral but allows it to be readily applied to different technology issues – including new advances and practices.
Comments here emphasized the need for the CSF to stay vendor neutral while also keeping up with new technology implementations such as cloud, hybrid work, and zero trust. Additionally, suggestions were made to have NIST provide guidance on how to address cybersecurity risks in IT, OT, and IoT.

5.**Emphasize the importance of measurement, metrics, and evaluation using the CSF.**
If you aren't tracking your progress through metrics, how can you tell how effective your cybersecurity program is performing? Numerous respondents referenced a need for additional CSF guid-

See NIST to Update, Page 4 for more.

Find us on LinkedIn

Risk Management Framework Today…

and Tomorrow

"Commenters have suggested that NIST expand and improve the CSF to meet that need, rather than setting up an entirely different framework given the flexibility of the CSF to cover many sectors of industry."

Find us on LinkedIn

BAI Information Security Consulting & Training

NIST Evaluation Tool, from Page 1

ment element, as shown in the example below:
The ISCMAx assessment can be applied at each of the three organizational "levels" defined by NIST:

Level 1 – organization-wide level
Level 2 – organizational unit/business process level
Level 3 – information system level

ID	Assessment Element Text	Source	Assessment Procedure	Discussion
1-001	There is an organization-wide ISCM strategy that applies to the entire organization and is approved by a Level 1 official.	NIST SP 800-137 OMB Circular A-130	ASSESSMENT OBJECTIVE Determine if: 1-001(a) There is an organization-wide ISCM strategy that applies to the entire organization; and 1-001(b) The strategy is approved by a Level 1 official. POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: Published organization-wide ISCM strategy document. Interview: Level 1: CIO; SAISO.	Organization-wide ISCM strategy documents all available controls selected and implemented by the organization, including the frequency of and degree of rigor associated with the monitoring process. The organization-wide ISCM strategy also includes all common controls available for inheritance inherited by agency information systems. Any mission/business area may have its own ISCM strategy that is in accordance with organization-wide ISCM strategy. However, a mission/business level strategy is not required by NIST SP 800-137, 800-37R2, or OMB policy. However, for each system, there is a system-level ISCM strategy. A signature page on the ISCM strategy is preferred; email or validated meeting minutes indicating Level 1 official approval are also examples of evidence of approval but may need further supporting validation such as confirmation through interview.

NIST to Update, from Page 3

ance to support metrics and measurement, describing an opportunity to improve measurement of cybersecurity risk management in the CSF Update.

6. Consider cybersecurity risks in supply chains in the CSF.

Supply Chain Risk Management has become a hot new topic in the cybersecurity field as it introduces a lot of risk into an organization. Commenters have suggested that NIST expand and improve the CSF to meet that need, rather than setting up an entirely different framework given the flexibility of the CSF to cover many sectors of industry.

7. Use the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to align practices and provide effective practices, guidance, and tools to bolster cybersecurity supply chain risk management.

Along with Theme 6, many commenters suggested that NIST utilize the NIICS to include Supply Chain Risk Management into the CSF to address the need of companies to protect their supply chain. The general consensus was that having a single clearinghouse for guidance, templates, tools, and information sharing would be of great benefit.

Risk Management Framework Today...

and Tomorrow

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 consists of BAI's senior RMF consultants who have decades of RMF experience as well as peer-reviewed published RMF research. Dr. RMF submissions can be made at https://rmf.org/dr-rmf/.

"Death by POAM" writes:
I just started a new job and I am a bit surprised at what I am seeing with the POA&Ms for the various systems in my new agency. At my previous place of employment we carefully maintained POA&Ms for several systems. In all cases, each line item represented one "weakness" identified during testing or monitoring of the system's compliance. Within each line item there would be one or more "milestones" representing specific corrective steps which, in some cases, corresponded to the corresponding non-compliant controls or CCIs. When I saw the POA&Ms at my new place, I was shocked to say the least. They have a separate line item on the POA&M for each non-compliant control or CCI. It makes the POA&Ms so big and unwieldy! I mentioned this to one of the other ISSOs and she was very adamant that "this is the way RMF tells us to do it". If that's true, the POA&Ms at my old place were just wrong. Is she right about this? Have I been doing POA&Ms wrong all these years?

Dr. RMF Responds:
Dr. RMF is not aware of anything in the NIST or DoD RMF publications that speaks directly to this question of "granularity" in the POA&M. So long as all the non-compliances and security weaknesses are covered by the POA&M one way or another, it ought to be acceptable. In Dr. RMF's opinion, the way you were doing it on your old job, i.e., one line item per "weakness", actually makes more sense from a management perspective. I would much rather see a POA&M that clearly delineates the security weaknesses or issues that require attention rather than a ponderous list of controls and CCIs that may be technically accurate but does not clearly convey what is truly going on. For example, if my system does not have a functional alternate processing (COOP) site, there will probably be numerous controls and CCIs that are non-compliant, but the bottom line is this should best be viewed as a single security issue requiring attention (and resources).

"I would much rather see a POA&M that clearly delineates the security weaknesses or issues that require attention rather than a ponderous list of controls and CCIs that may be technically accurate but does not clearly convey what is truly going on."

That said, however, I do know quite a few Authorizing Officials, and, in some cases, even entire commands, do recommend … or even require … the "one line item per non-compliant control/CCI" approach. Some even go so far as to require a separate POA&M line item for every non-compliant STIG item! Ouch!

Dr. RMF's advice is to pose this very question to your AO or AO Designated Representative and see what they have to say. That should clear up any ambiguity going forward.

"New AO, new game?" writes:
We just found out our Authorizing Official will be retiring next month and there is still no word on who his replacement will be. What sort of problems can we anticipate when a new AO takes over the reins? How much flexibility will he/she have to "change the rules of the game", so to speak? What additional problems would we face if there turns out to be a "gap" between the old AO's retirement and the appointment of a new one?

Dr. RMF Responds:
Transitioning to a new AO should be a smooth and seamless transition. It will not invalidate your existing ATOs, nor should it necessitate any new system assessments. That doesn't mean there will

Find us on LinkedIn

BAI Information Security Consulting & Training

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

Dr. RMF, from Page 5:

be absolutely no changes, though. Perhaps the new AO will ask for some additional reporting on a regular basis, especially if there are numerous systems within their purview. Sometimes a new AO will request a one-time brief from each system owner to help him/her become familiar with their systems.

If there turns out to be a "gap" between old and new AOs, this will only be a problem if an existing ATO is due to expire during the gap. If you see that coming, it is important you reach out to the existing AO (or AO Designated Rep) now to get some guidance on how to best handle the situation. Perhaps the existing AO has already arranged for someone to be able to sign ATOs during the gap. In some cases, the existing AO will agree to sign a short-term "ATO Extension" to bridge the gap and allow the new AO some time to "settle in" before having to address your next ATO.

> ***"In some cases, the existing AO will agree to sign a short-term "ATO Extension" to bridge the gap and allow the new AO some time to "settle in" before having to address your next ATO."***

"Let's Get Physical" asks:

Control Enhancement AT-3(2) states "The organization provides … training in the employment and operation of physical security controls". Our system is hosted in the cloud (by a commercial cloud service provider) and therefore we have no physical security controls within our system boundary. At first we thought this should be covered by inheritance, so we requested a list of inheritable controls from our cloud service provider. On there we found the entire Physical and Environmental (PE) family of controls, but nothing in the Awareness and Training (AT) family. If it's not inheritable, that seems to leave AT-3(2) in our hands. What is the best way to handle this situation in our RMF package?

Dr. RMF Responds:

First of all, Dr. RMF wonders about the name "Let's Get Physical". Are you old enough, like me, to remember 1970's country/pop singer Olivia Newton-John's hit song? Or do you just watch lots of vintage shows on cable TV?

In any case, Dr. RMF sees two possible approaches to your dilemma. Probably the "most correct" approach would be to approach your cloud service provider and ask them to add AT-3(2) to their list of inheritable controls. The downside of this is it could take lots of time for your request to work its way through the proper channels to get this done and allow you to inherit compliance.

A simpler way would be to declare AT-3 (2) as "Not Applicable" in your RMF package and explain the situation in your Security Plan. The one thing that is clear is that your organization does not need to provide any additional training to your personnel in response to this control.

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

Classroom RMF and eMASS Training is Back!

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, Pensacola, San Diego, and Alexandria!

RMF for DoD IT and Federal Agencies & eMASS eSSENTIALS ™

Pensacola, FL — October 24th – 28th

Colorado Springs, CO — September 19th – 23rd and November 7th – 11th

San Diego, CA — August 8th – 11th and December 5th – 9th

Alexandria, VA—September 12th – 16th

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

New Course Announcement: RMF for DoD IT & Federal Agencies
*****CAP Bootcamp*****

Due to demand, BAI is now offering a CAP bootcamp taught by our in-house certification expert William Alan Matthey II, FITSP-M, CISSP/CAP/CCSP, CISM, MCSE/MCT, RDRP! This course will be focused on delivering BAI's practitioner based RMF training and prepare students to sit for the CAP exam! Seats currently available for 18-22 July and 8-12 August, sign up now!

To register, contact alice@rmf.org or go to register.rmf.org.

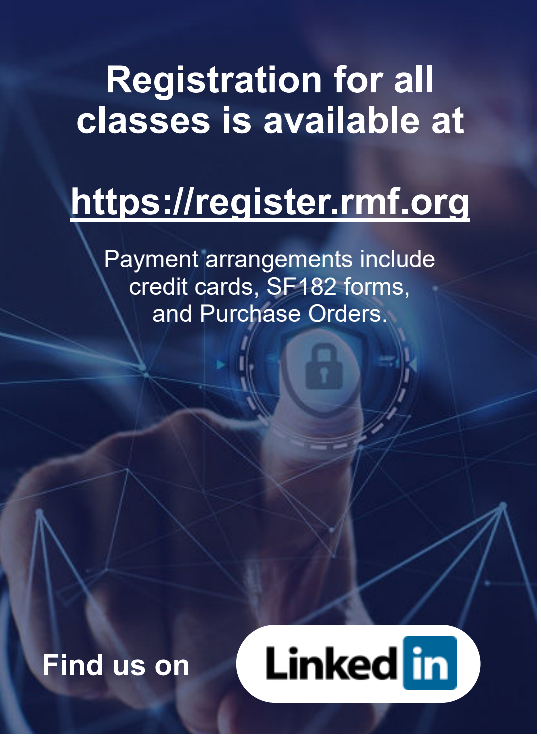
Risk Management Framework Today…

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, 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$^{\text{TM}}$ (interactive, live, instructor-led)**
- **Private group classes for your organization (on-site or online instructor-led)**

Regularly-scheduled classes through December, 2022:

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

- **Online Personal Classroom™ ▪ 18 - 21 JUL ▪ 25 - 28 JUL ▪ 8 - 11 AUG ▪ 29 AUG - 1 SEP ▪ 19 - 22 SEP ▪ 26 - 29 SEP ▪ 17-20 OCT ▪ 24-27 OCT ▪ 7-10 NOV ▪ 14-17 NOV ▪ 28 NOV - 1 DEC**
- **Colorado Springs, CO ▪ 19 - 22 SEP ▪ 7-10 NOV**
- **Pensacola, FL ▪ 24-27 OCT**
- **San Diego, CA ▪ 8 - 11 AUG ▪ 5-8 DEC**
- **Alexandria, VA ▪ 12-15 SEP**

RMF for DoD IT and Federal Agencies + CAP Bootcamp—5 day program

- **Online Personal Classroom™ ▪ 18 - 22 JUL ▪ 8 - 12 AUG**

eMASS eSSENTIALS—1 day program

- **Online Personal Classroom™ ▪ 29 JUL ▪ 15 AUG ▪ 2 SEP ▪ 23 SEP ▪ 30 SEP ▪ 21 OCT ▪ 28 OCT ▪ 11 NOV ▪ 18 NOV ▪ 2 DEC ▪ 16 DEC ▪ 19 DEC**
- **Colorado Springs, CO 23 SEP ▪ 11 NOV**
- **Pensacola, FL ▪ 28 OCT**
- **San Diego, CA ▪ 12 AUG ▪ 9 DEC**
- **Alexandria, VA ▪ 16 SEP**

Security Controls Implementation & Assessment Workshop—4 day program

- **Online Personal Classroom™ ▪ 18 - 21 JUL ▪ 1 - 4 AUG ▪ 22 - 25 AUG ▪ 12 - 15 SEP ▪ 3-6 OCT ▪ 5-8 DEC**

STIG 101—1 day program

- **Online Personal Classroom™ ▪ 22 JUL ▪ 29 JUL ▪ 5 AUG ▪ 26 AUG ▪ 6 SEP ▪ 16 SEP ▪ 7 OCT ▪ 13 OCT ▪ 1 NOV ▪ 22 NOV ▪ 9 DEC ▪ 21 DEC**

RMF Supplement for DCSA Cleared Contractors—1 day program

- **Online Personal Classroom™ ▪ 12 OCT**

Information Security Continuous Monitoring—1 day program

- **Online Personal Classroom™ ▪ 18 AUG ▪ 9 SEP ▪ 4 NOV ▪ 21 NOV**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 16 AUG ▪ 7 SEP ▪ 14 OCT ▪ 2 NOV ▪ 23 NOV**

Certified Authorization Professional (CAP) Supplement—1 day program

- **Online Personal Classroom™ ▪ 22 JUL ▪ 12 AUG ▪ 8 SEP ▪ 31 OCT**

RMF Project Management Advantage (PMA)—1 day program

- **Online Personal Classroom™ ▪ 29 JUL ▪ 26 AUG ▪ 23 SEP ▪ 3 NOV ▪ 20 DEC**