Risk Management Framework Today…

and Tomorrow

In this issue:

Find us on LinkedIn

BAI Information Security Consulting & Training

*April, 2020 Volume 11, **Issue 2***

Online Personal Classroom™ Brings RMF Training to You

By Lon J. Berman, CISSP, RDRP

DoD and Federal agencies and their supporting contractors are struggling to adapt to the "new reality" of travel restrictions, mandatory telework and social distancing. While we don't know how long these conditions will last, we do know that all organizations must continue to perform their mission seamlessly. It is well known that a better trained workforce is able to perform more efficiently, but obtaining training in the face of these challenges can be problematic.

BAI to the rescue! Our Online Personal Classroom™ can help your organization meet its training objectives without the need for travel. The Online Personal Classroom combines the best features of web-based learning and traditional instructor-led classes. Using just a personal computer, teleworking students can fully participate in a live, instructor-led, interactive training experience.

The Online Personal Classroom is absolutely *not* computer-based training (CBT) in the traditional sense. All classes are live and instructor-led, and enable full interaction between the instructor and the class, and among the students themselves. As one of our former students put it, "It's everything you get in a physical classroom … except coffee and donuts!"

Some of the key benefits of Online Personal Classroom training are:

- Elimination of Student Travel – Online Personal Classroom allows your staff to receive training without the necessity of traveling to a classroom location. Clearly this is essential in the current environment, but even when there are no restrictions, it can be advantageous. By eliminating travel expenses, many organizations have realized dramatic cost savings, frequently on the order of 50%.

- Increased Efficiency – Online Personal Classroom training improves organizational efficiency by minimizing staff downtime such as travel days. No longer does a four-day training program entail a full week out of the office.

- Improved Morale – Online Personal Classroom training eliminates disruptions to personal and family life caused by travel – no more leaving home on Sunday to make a Monday morning training class.

- Increased Flexibility – Online Personal Classroom training enables more flexible scheduling of your staff for training.

And the best news of all is that this is not some hastily-conceived response to the current public health crisis.

BAI has been successfully delivering Online Personal Classroom training since 2012!

All regularly-scheduled BAI training programs are available for delivery via Online Personal Classroom. This includes our flagship offering, *RMF for DoD IT*, as well as numerous one and two-day supplemental programs. A complete schedule and registration information is included in this newsletter. Registration is available at https://register.rmf.org.

Additionally, BAI can arrange a "private online class" for your organization. You will have a dedicated instructor who will deliver a fully-interactive training experience using Online Personal Classroom technology. Just like our "on-site" classroom training, your organization will realize significant "per student" savings.

Of course, we realize some students and organizations strongly prefer traditional classrooms, and BAI plans to phase those back in once travel restrictions are relaxed, while continuing to offer Online Personal Classroom training!

In these difficult times, it is comforting to know BAI can truly "bring RMF to you".

Risk Management Framework Today…

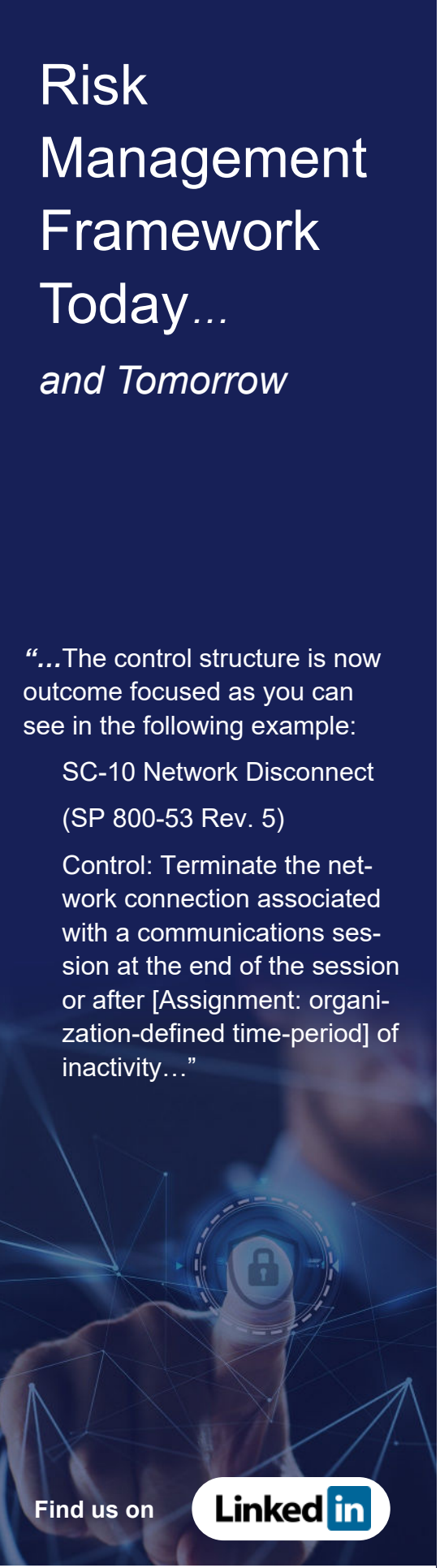
and Tomorrow

*"…*The control structure is now outcome focused as you can see in the following example:

SC-10 Network Disconnect

(SP 800-53 Rev. 5)

Control: Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time-period] of inactivity…"



Find us on LinkedIn

BAI Information Security Consulting & Training

NIST SP 800-53 Rev. 5—A Summary of What is to Come

By Kathryn Daily, CISSP, CAP, RDRP

In an effort to strengthen the trustworthiness and resilience of the information systems, component products and services that the federal government depends on in every critical infrastructure sector and which support the economic and national security interests of the United states, NIST has released an updated version of the NIST SP 800-53, to wit, NIST SP 800-53 Rev 5. Changes are as follows:

- Creates security and privacy controls that are more outcome-based by changing the structure of controls
- Fully Integrating privacy controls into the security control catalog, creating a consolidated and unified set of controls
- Adding two new control families for privacy and supply chain risk management
- Integrating the Program Management control family into the consolidated catalog of controls
- Separating the control selection process from the controls—allowing controls to be used by different communities of interest
- Separating the control catalog from the control baselines
- Promoting alignment with different risk management and cybersecurity approaches and lexicons, including the NIST Cybersecurity and Privacy Frameworks
- Clarifying the relationship between security and privacy to improve the selection of controls necessary to address the full scope of security and privacy risks
- Incorporating new, state-of-the-practice controls based on threat intelligence, empirical attack data, and systems engineering and supply chain risk management best practices, including controls to:
  - ◊ Strengthen security and privacy governance and accountability;
  - ◊ Support secure system design; and
  - ◊ Support cyber resiliency and system survivability.

The control structure is now outcome focused as you can see in the following example:

SC-10 Network Disconnect

(SP 800-53 Rev. 5)

Control: **The information system** terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time-period] of inactivity.

SC-10 Network Disconnect

(SP 800-53 Rev. 5 FPD)

Control: Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time-period] of inactivity.

There exist new systems security engineering control enhancements. In Rev. 4 we have SA-8 Security and Privacy Engineering Principles. In Rev. 5 we have added Enhancements (1)-(6) as follows: (1) Clear Abstractions, (2) Least Common Mechanism, (3) Modularity and Layering, (4) Partially Ordered Dependencies, (5) Efficiently Mediated Access, and (6) Minimized Sharing. These new control enhancements link to security design in the NIST SP 800-160, Vol 1 (Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems).

Appendix J has been reorganized to A) align some privacy controls in previously existing control families and B) A new family, to wit, PII Processing and Transparency (PT).

...continued on Page 5

Risk Management Framework Today…

and Tomorrow

*"...*The control you cite absolutely meets the definition of an inheritable control. The "information system" cited in the control actually refers to the network/hosting provider (enclave) within which your system resides. *..."*

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,

In my office we are disputing whether RMF Control SA-4 can be inherited, or if it needs to be system-specific. The control description includes the work "Organization", but the compelling evidence (per eMASS) calls for SSP. Furthermore, the Assessment Procedure calls for the contract/agreement to be inspected. I am saying that since this control is talking about contracts / agreements and each contract / agreement is unique to the system, this control is meant to be system specific. Others are saying that since the control says organization then it could be inherited.

RMF Hatfield-McCoy,

SA-4 appears to be a system-specific requirement since the number and types of contracts/agreements in place will vary from system to system. In my experience, the contracts/agreements themselves are presented as artifacts in support of this CCI, rather than the SSP itself.

For what it's worth, the term "organization" is used throughout the control baseline and most often refers to the system owner rather than the "upper command".

Dear Dr. RMF,

I have an information system that is currently being assessed and authorized and the boundary consists of desktops, laptops, printers, a major OS, and about 10 to 15 applications, which is spread throughout an enterprise. In reviewing the DoDI 8510.01 and the definition of IT products it speaks to HW/SW/Applications as assess only. My question is instead of treating this boundary as assess and authorize, could we make this assess only? (Enclosure 3 (pg. 12 bullet a)).

RMF Assess Only,

The purpose of Assess Only is to facilitate approval of an IT product to be accepted into a larger system that already has a A&A ATO. If the enterprise you speak of has an existing ATO, Assess Only may work for you. You would need to coordinate with the Authorizing Official of the system into which you wish to add these products.

Dear Dr. RMF,

I am doing an annual review for an information system I have. Originally, this was inherited from our network boundary, but in reviewing this again it speaks specifically to information systems, which from my understanding this cannot be inherited. If I am reading this control correctly it speaks to the information system controlling this service. So if the application I am reviewing does not provide this service would this be N/A, or an exception to the rule and inheritable from the network boundary?

SC-22: Architecture And Provisioning For Name / Address Resolution Service
Control Description

RMF Inheritance Challenges,

The control you cite absolutely meets the definition of an inheritable control. The "information system" cited in the control actually refers to the network/hosting provider (enclave) within which your system resides. Inheritance is in play because the control: a) is implemented outside your system boundary; and b) inures to the benefit of your system. In order to be fully compliant with your claim of inheritance you should also verify that there is a formal relationship between your system owner and the owner of the hosting enclave (i.e., an MOA, MOU, SLA or contract), and that the hosting enclave is in fact compliant with said control.

All that said, it is possible the hosting provider simply has not chosen to offer this control up as inheritable. That would be an oversight on their part, in my opinion, if they are in fact providing the service. In such a case you could certainly approach the hosting provider and try to convince them to offer this control up as inheritable. Failing that, you could probably get away with declaring the control to be "Not Applicable" to your system, with the following justification: "System XXX does not provide address resolution services", which would be a true statement.

Risk Management Framework Today…

and Tomorrow

*"...*BAI, in partnership with CompTIA, recently produced a one-hour video on the basic concepts of Risk Management Framework (RMF) presented in 10-15 minute segments*..."*

Find us on LinkedIn

BAI Information Security Consulting & Training

Reflections on RMF Training from a BAI College Scholarship Recipient

By Grace Brammer, RDRP

As an undergraduate computer science student, I often find it difficult to connect my work in academia to real-world cybersecurity implementation. While demand in the tech industry continues to grow, studying for a technical degree in college is both exciting and stressful. Unfortunately, the stress compounds upon itself as I look at securing a job once I graduate.

As a Freshman, I was awarded a student scholarship from BAI RMF Resource Center and given the opportunity to attend both a weeklong course on RMF for DoD IT and a one-day STIG 101 class. My goal in attending these courses were to get a sense of what real-world cybersecurity work looks like. Being the youngest student in the history of BAI attending the training and with little prior knowledge of the field, I was nervous attending class for the first time. After a few tough days, I was relieved to find my confidence with the material grew faster than I had anticipated! One of the most exciting aspects of the class was working with my classmates knowing that many of them already had the cybersecurity jobs I was training to one day fill.

The RMF and STIG courses I attended gave me a sense of what it might be like should I pursue my interest in the field of government cybersecurity as working on a team for the different exercises didn't feel like a normal college group project, but rather a reflection of what a job might actually look like. Knowing and understanding how RMF works on a deeper level than the brief mention it has received in my typical college classes has given me a better feel for what a career might look like, and this opportunity has piqued my interest in pursuing a career as an RMF practitioner.

Overall, I am very thankful that BAI helped me in bridging the gap between academia and real-world cybersecurity training.

Now I just need to learn more about how to implement those pesky NIST 800-53 controls!

Thanks, BAI!

Editor's note; Grace will soon be a rising junior at Liberty University and is looking forward to a summer internship at BAI!

BAI Announces RMF Micro Edition Video Series

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

BAI RMF Resource Center is pleased to announce the RMF Micro Edition Video Series created in collaboration with CompTIA. Below is a summary of the course content as described by BAI's lead trainer, Linda Gross:

"BAI, in partnership with CompTIA, recently produced a one-hour video on the basic concepts of Risk Management Framework (RMF) presented in 10-15 minute segments. The video has a target audience of individuals who need to know what RMF is really all about. For organization managers or for individuals working on the periphery of the system world (i.e. training, procurement, personnel, finance, etc.) this provides an opportunity to understand what those three letters "R", "M", and "F" actually represent.

In organizations where the system owners or project managers are involved in the development of a system RMF package, individuals not normally part of this system world may need to be called in for understanding or assistance with implementation of certain security controls. This video series can provide those individuals with some basic training. Or sometimes there is just a sense of curiosity.

This quick overview of the history, documents, roles, lifecycle steps, and system authorization can point an individual in the right direction and possibly give them a realization that they may need additional or extensive training in the process. We hope our students will enjoy this new video as the first step in their RMF journey."

Use the following link to view the RMF Micro Edition Video Series:

https://rmf.org/video/

Risk Management Framework Today…

and Tomorrow

"...Additionally, there will be a new control family for your supply chain, The Supply Chain Risk Management (SR). New controls will consist of SR-1 Policy and Procedures, SR-2 Supply Chain Risk Management and SR-4 Provenance..."

Find us on LinkedIn

BAI Information Security Consulting & Training

NIST SP 800-53 Rev. 5... Continued from Page 2

The PT family will consist of the following controls:

- PT-1 Policy and Procedures
- PT-2 Authority to Process Personally Identifiable Information
- PT-3 Personally Identifiable Information Processing Purposes
- PT-4 Minimalization
- PT-5 Consent
- PT-6 Privacy Notice
- PT-7 System of Records Notice
- PT-8 Specific Categories of Personally Identifiable Information
- PT-9 Computer Matching Requirements

The Program Management (PM) family of controls will have some added privacy controls at the program level. For example, as you know, PM-1 refers to the Information Security Program Plan. Rev. 5 introduces PM-18, Privacy Program Plan. PM -2 refers to the Information Security Program Leadership Role. PM-19 refers to the Privacy Leadership role. Rev 5 is baking in privacy specific controls at the program management level.

Additionally, there will be a new control family for Supply Chain Risk Management (SR). New controls will consist of SR-1 Policy and Procedures, SR-2 Supply Chain Risk Management and SR-4 Provenance. The remaining 8 controls in the family are repurposed from the SA family of controls already existing in Rev. 4.

One topic that NIST specifically wants feedback on is the Security and Privacy Collaboration Index. The idea here is that it will provide better guidance on control implementation collaboration between security and privacy programs. There are 2 options to choose from:

Option one is a 5-point scale, as follows:

- S—Controls are primarily implemented by security programs—minimal collaboration needed between security and privacy programs.
- S_P—Controls are generally implemented by security programs—moderate collaboration needed between security and privacy programs.
- SP—Controls are implemented by security and privacy programs—full collaboration needed between security and privacy programs.
- P_S—Controls are generally implemented by privacy programs—moderate collaboration needed between security and privacy programs.
- P—Controls are primarily implemented by privacy programs—minimal collaboration needed between security and privacy programs.

Option two is a 3-point scale, as follows:

- S—Security programs have primary responsibility for implementation—minimal collaboration needed between security and privacy programs
- SP—Security and privacy programs both have responsibilities for implementation—more than minimal collaboration is needed between security and privacy programs.
- P—Privacy programs have primary responsibility for implementation—minimal collaboration needed between security and privacy programs.

Keep in mind this is the Final Public Draft. There will be not be a third public comment period. The current public comment period is 16 March to 29 May 2020. Comments can be submitted via email using the comment template (xls) provided under supplemental material (at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft) to sec-cert@nist.gov

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 DCSA** – This three-day course covers the specifics of RMF as it applies to cleared contractor companies under the purview of the Defense Counterintelligence and Security Agency (DCSA). Companies holding a Facility Clearance who also maintain "on premise" information technology (such as standalone computers and small networks) will benefit from this training.
- **CMMC Readiness Workshop**—prepares DoD contractors for the impending mandatory Cybersecurity Maturity Model Certification.
- **eMASS eSSENTIALS** – provides practical guidance on the key features and functions of eMASS. "Live operation" of eMASS (in a simulated environment) is utilized.
- **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 Assessment (SCA) Workshop** – provides a current approach to evaluation and testing of security controls to prove they are functioning correctly in today's IT systems.
- **Continuous Monitoring Overview** – 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.

In response to DoD travel restrictions, BAI RMF Resource Center has moved all regularly scheduled classes to The Online Personal Classroom, where training will be delivered live instructor-led. BAI is closely monitoring the situation and will add physical classroom locations when deemed safe and appropriate. If you have any questions email rmf@rmf.org.

Our training delivery methods:

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

Regularly-scheduled classes through September, 2020:

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

- **Online Personal Classroom™ ▪ 13-16 APR ▪ 27-30 APR ▪ 4-7 MAY ▪ 11-14 MAY ▪ 18-21 MAY ▪ 8-11 JUN ▪ 22-25 JUN ▪ 29 JUN - 2 JUL ▪ 6 - 9 JUL ▪ 20 - 23 JUL ▪ 3 - 6 AUG ▪ 17 - 20 AUG ▪ 31 AUG - 3 SEP ▪ 14 - 17 SEP ▪ 21 - 24 SEP**

RMF for DCSA —3 day program (Fundamentals and In Depth)

- **Online Personal Classroom™ ▪ 24 JUL ▪ 21 AUG ▪ 8 SEP ▪ 18 SEP**

CMMC Readiness Workshop—3 day program

- **Online Personal Classroom™ ▪ 5-7 MAY ▪ 23-25 JUN ▪ 14-16 JUL ▪ 11-13 AUG ▪ 21-23 SEP**

eMASS eSSENTIALS—1 day program

- **Online Personal Classroom™ ▪ 17 APR ▪ 22 APR ▪ 1 MAY ▪ 8 MAY ▪ 22 MAY ▪ 26 MAY ▪ 4 JUN ▪ 12 JUN ▪ 19 JUN ▪ 26 JUN ▪ 3 JUL ▪ 24 JUL ▪ 21 AUG ▪ 25 AUG ▪ 10 SEP ▪ 18 SEP**

STIG 101—1 day program

- **Online Personal Classroom™ ▪ 17 APR ▪ 24 APR ▪ 15 MAY ▪ 27 MAY ▪ 2 JUN ▪ 19 JUN ▪ 10 JUL ▪ 7 AUG ▪ 26 AUG ▪ 4 SEP ▪ 9 SEP ▪ 25 SEP**

Continuous Monitoring Overview—1 day program

- **Online Personal Classroom™ ▪ 3 JUN ▪ 10 SEP**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 1 JUN ▪ 8 SEP**

SCA Workshop—2 day program

- **Online Personal Classroom™ ▪ 26-27 MAY ▪ 28-29 JUL ▪ 24-25 SEP**