Risk Management Framework Today

… and Tomorrow

January, 2018
Volume 8, Issue 1

Linked in

In this issue:

BAI Introduces RMF Supplemental Training

By P. Devon Schall, MS, MAEd, CISSP, RDRP

We are excited to announce the addition of RMF supplemental training courses to our training catalog. After extensive discussion regarding our 2018 curriculum, we felt we would benefit students the most by offering "bite-sized" courses to supplement our core four-day RMF for DoD IT and RMF for Federal Agencies classes. We recognize most of our students are working with already diminished resources and don't have the bandwidth to be out of the office to travel and attend multiple training days. Our goal is to continue to deliver **relevant and effective** RMF training solutions that will save time and money in the implementation of the RMF life cycle. See below for a brief synopsis of our newest one-day course offerings:

Continuous Monitoring Training Program:

The program seeks to equip learners with knowledge of the theory and policy background underlying continuous monitoring as well as the practical knowledge needed for effective implementation. The program focuses on Information Security Continuous Monitoring (ISCM) in accordance with NIST Special Publication (SP) 800-137, guidance from DoD and other federal agencies, and industry best practices. Completion of the full four-day RMF for DoD IT or RMF for Federal Agencies training program is a prerequisite.

eMASS eSSENTIALS^{TM} Training Program:

The Enterprise Mission Assurance Support Service, or eMASS, is a web-based Government off-the-shelf (GOTS) solution that automates a broad range of services for comprehensive, fully-integrated cyber security management, including controls scorecard measurement, dashboard reporting, and the generation of Risk Management Framework (RMF) package reports. The majority of DoD components have "standardized" on eMASS as the data repository for RMF Assessment and Authorization. We provide "how to" guidance for the most commonly-used eMASS functions.

RMF in the Cloud Training Program:

RMF in the Cloud Training is designed to answer foundational questions about RMF and cloud migration as well as offering BAI's real world experience in cloud migration as a provider of RMF consulting services. RMF in the Cloud is a vendor neutral course utilizing our first-hand consulting experience. Some RMF in the Cloud topics include Cloud Preparation, Fed Ramp, Cloud Inheritance, Common Pitfalls, Cloud Tools, and eMASS and the Cloud.

Certified Authorization Professional (CAP) Exam Preparation:

Backed by (ISC)^2, CAP credentialing aligns with the Risk Management Framework (RMF). The CAP recognizes knowledge, skills and abilities to authorize and maintain information systems within RMF. It demonstrates the ability to formalize processes to assess risk and establish security documentation. BAI's CAP Prep class focuses on exam preparation as well as analyzing the five domains in the (ISC)^2 CAP Common Body of Knowledge (CBK). We feel our core RMF for DoD IT and RMF for Federal Agencies courses provide the requisite foundational knowledge for the CAP exam, and this training focuses on helping our students take the next step and attain the CAP credential.

BAI Introduces CISSP Training

By Lon J. Berman, CISSP, RDRP

BAI has recently expanded its training program to include training for the Certified Information Systems Security Professional (CISSP) credential. Beginning in February, 2018, we are offering an intensive five-day course designed to prepare students for the CISSP certification exam.

CISSP is an internationally recognized certification in the field of information technology security. It is administered by the International Information Systems Security Certification Consortium, more commonly known as (ISC)^2. CISSP has been around for nearly 25 years and is widely considered as the "gold standard" of information security certifications.

"… Some studies have shown significant salary difference between certified and non-certified personnel…"

Professional certification can be a key factor in career advancement. Some studies have shown significant salary differences between certified and non-certified personnel. The Department of Defense (DoD) requires all personnel with cybersecurity responsibilities, including both government employees and contractors, to hold professional certifications appropriate to their roles. CISSP certification fulfills this requirement for the overwhelming majority of job categories as defined by DoD.

The CISSP curriculum, known as the Common Body of Knowledge (CBK), includes eight subject areas or domains:

- Security and Risk Assessment
- Asset Security
- Security Engineering
- Communications & Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

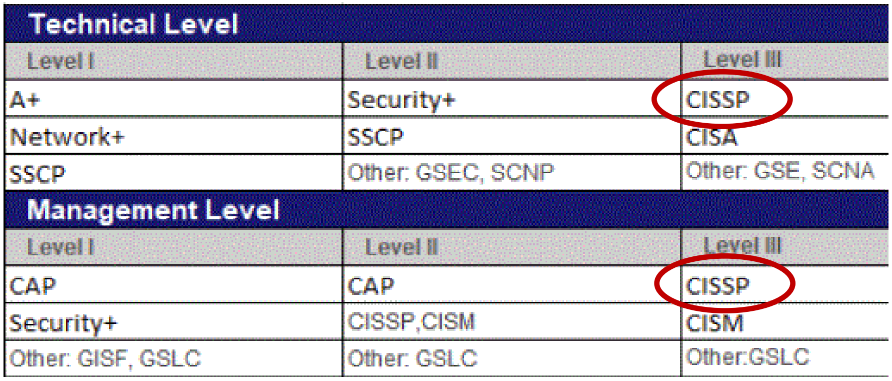
In the BAI training program, students learn the subject matter in each of these domains. Beyond that, instruction is provided on the best approach to the certification exam. Numerous sample test questions are provided, both during the class and as "take home" exercises. Additional self-study resources are also provided.

The CISSP certification exam is extremely challenging because it is not a simple test of factual knowledge. Rather, the test questions frequently present a "scenario" and then ask the student to identify the "best approach" to deal with the given situation. BAI training prepares students to handle these types of questions.

The five-day CISSP Preparation class will be offered in several BAI training sites in 2018, starting with Oakland (February), Dallas (March), and National Capital Region (April). These classes will be taught by instructors with extensive experience in preparing students for CISSP as well as other professional certifications. BAI is also offering an online, instructor-led version of the CISSP Preparation class on May 14th - 18th.

For further information, or to register for one of our upcoming classes, please visit BAI at www.rmf.org/register. For additional information on the certification exam itself, please see www.isc2.org.

See the chart below from DoD 8570.01 Information Assurance Workforce Improvement Program indicating a list of certification requirements for DoD job roles. Note that higher Level certification requirements fulfill lower levels. So, CISSP meets requirements for Level I, II, and III.



Technical Level		
Level I	Level II	Level III
A+	Security+	CISSP
Network+	SSCP	CISA
SSCP	Other: GSEC, SCNP	Other: GSE, SCNA
Management Level		
Level I	Level II	Level III
CAP	CAP	CISSP
Security+	CISSP,CISM	CISM
Other: GISF, GSLC	Other: GSLC	Other:GSLC

NIST 171—What's That?

By Kathryn Daily, CISSP, RDRP

If you heard a whooshing sound on New Years Eve, that was probably the deadline for compliance with NIST 171 flying by. A lot of you might be asking "What is NIST 171?" NIST 171 is a set of requirements documented in the NIST Special Publication 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations).

> *"... CUI is a broad category encompassing many different types of sensitive, but not classified information..."*

NIST 800-171 contains 110 security requirements, in 14 families, that all contractors and subcontractors are required to implement on contractor owned, and contractor operated IT systems (e.g., a contractor receiving and processing DoD information on their own corporate network) containing Controlled Unclassified Information (CUI). CUI is a broad category encompassing many different types of sensitive, but not classified, information. For example, personally identifiable information (PII) such as health documents, proprietary material and information related to legal proceedings would all count as CUI. It is also important to reiterate NIST 800-171 does not apply to contractors providing support to government-owned IT systems.

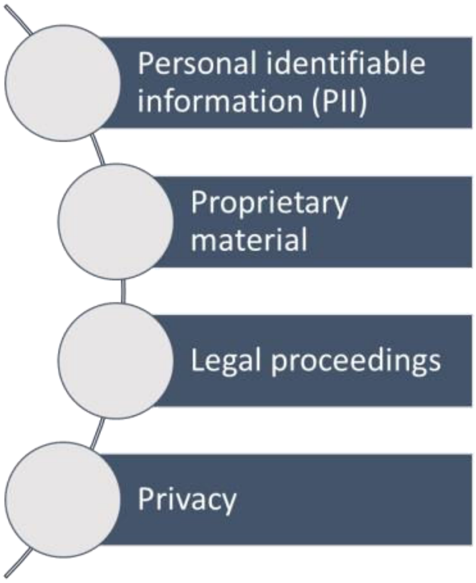
While many are incorrectly under the impression that they are required to be fully compliant with all 110 requirements, the reality is that one simply needs to have done an initial assessment of the security requirements and have developed a System Security Plan (SSP) and a Plan of Actions and Milestones (POA&M). The POA&M will provide a roadmap for the organization to become fully compliant.

Many contractors were previously tasked with going through the Risk Management Framework process because previously there wasn't a standard for contractors. With the advent of NIST 171, this could actually reduce your workload as RMF was developed for federal agencies and many of the RMF requirements are not easily met by contractors.

Some notable differences between RMF and NIST 171 are no requirement for an authorization to operate (ATO) or even the presence of an Authorizing Official (AO). Although eliminating ATO's and AO's are a huge benefit from a time resource perspective, it raises some concern for the accountability of NIST 171 implementation. With no AO requirement, the burden of verifying NIST 171 compliance would fall on the contracting officer who may or may not have a baseline understanding of cybersecurity.

While DFARS contracts don't specify what happens to companies that aren't fully in compliance, each non-compliant company is supposed to notify the Department of Defense compliance personnel and receive permission, however, many won't. Sooner or later, it is likely that audits and proof of compliance will follow with actual contract penalties or default for those who don't comply. What may happen in the nearer term is that primes will enforce proof of compliance and security audits on subs to ensure their own compliance. If nothing else, non-compliant organizations are unlikely to win new business so it's extremely important to get on board with NIST 171 sooner rather than later.

Does your system have CUI?



Top Ten—Preparing for RMF Questions

By P. Devon Schall, CISSP, RDRP

With the addition of Step 0 to the RMF life cycle (a preparation step that BAI has been preaching for years which is now being implemented in SP 800-37 Rev. 2), we decided to make this month's top ten list based on preparation. Preparation is often one of the most overlooked aspects of RMF. The road to an ATO is often paved with unexpected setbacks, these setbacks can be overcome with proper preparation. It is critical to answer the key questions below in RMF project preparation.

10. Has the system been registered with the DoD Component Security Program?

Registering your system and obtaining an appropriate ID number should occur early in the RMF life cycle. If you are using eMASS to manage your RMF project, a registration number, such as a DITPR ID number, is required in order get started. Overlooking this step will likely cause unnecessary delays to your RMF efforts down the line.

9. What is the system boundary?

Having a clear understanding of system boundaries is critical. Start conversations internally with your team to verify everyone is on the same page regarding system boundaries.

> *"...Preparation is often one of the most overlooked aspects of RMF ..."*

8. What is the system's mission?

We often find folks don't always understand the details of their system's mission. Start a conversation with your team about your system. Don't let insecurity about a possible lack of knowledge interfere with forward progress.

7. Does the system handle PII/PHI?

The handling of PII and PHI could require a privacy overlay which can greatly increase the scope and amount of controls assigned to your system. Perform an assessment of the system and establish if it handles PII/PHI.

6. What controls are inheritable?

At BAI, we love inheritable controls. Inheritable controls can save you massive amounts of RMF project time. A great example is the utilization of cloud service providers which includes the inheritance of many control families including physical and media protection. Note that inheritable controls must come from a validated source and only systems or services with an ATO can provide inheritable controls.

5. Will we be using an automated tool such as eMASS or Xacta?

eMASS and Xacta can potentially be BIG time savers. "Hand jamming" controls is very time consuming. Find out early in the project if you will be using automated tools and if your staff has the appropriate security permissions AND TRAINING to use these tools.

4. Who is the Authorizing Official (AO) or Authorizing Office Designated Representative (AODR)?

Start conversations with your AO/AODR early in the project to maximize transparency and communication channels. The AO staff are very busy, and it is highly recommended to get on their radar as soon as possible.

3. What is our system categorization?

Learning about the information types your system handles is a critical part of system categorization. Start early with system categorization and researching on information types in NIST SP 800-60 volumes 1 & 2.

2. What will system assessment be performed?

Each DoD component has its own process for independent assessment. Independent assessors often have a backlog of work and cannot perform an assessment on short notice. plan in advance to avoid any time hindrances.

1. Do we need RMF training?

Some things in life are easier to understand by doing extensive Googling and avoiding traditional training delivery methods. RMF is not one of those things. RMF has many intricacies, and it is highly recommended your staff attend baseline RMF training. The time saved in proper RMF education is well worth training time invested. If you can't attend one of our many training locations, our classes are delivered via The Online Personal Classroom™ monthly.

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.

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. The program consists of a one day "Fundamentals" class, followed by a three day "In Depth" class.
- **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. The program consists of a one day "Fundamentals" class, followed by a three day "In Depth" class.
- **Certified Information Systems Security Professional (CISSP) Preparation** – this 5-day class is recommended for anyone interested in preparation for the "gold standard" Certified Information Systems Security Professional (CISSP) certification.
- **eMASS eSSENTIALS** – designed as an add-on to RMF for DoD IT. Recommended for government employees and contractors working (or planning to work) in the DoD environment, this one-day 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 In Depth**– open to all, however prior knowledge of RMF is recommended. This is a three day "in depth" program.
- **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. Recommended for government employees and contractors working (or planning to work) in the cloud environment, this one-day training program will provide students the knowledge needed to begin shifting their RMF efforts to a cloud environment.
- **Certified Authorization Professional (CAP) Preparation** – designed as a one-day add-on to RMF for DoD IT. Recommended for government employees and contractors interested in preparation for the Certified Authorization Professional (CAP) certification administered through $(ISC)^2$.

Our training delivery methods:

- **Traditional classroom** – regularly-scheduled training programs are offered at various locations nationwide, including Colorado Springs, Huntsville, National Capital Region (Pentagon/Crystal City area), Dallas, Oakland 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 April, 2018:

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

- ♦ **National Capital Region ▪ 29 JAN-1 FEB ▪ 9-12 APR**
- ♦ **Huntsville ▪ 26 FEB-1 MAR**
- ♦ **Pensacola ▪ 7-10 MAY**
- ♦ **Colorado Springs ▪ 26-29 MAR ▪ 11-14 JUN**
- ♦ **San Diego ▪ 12-15 MAR ▪ 4-7 JUN**
- ♦ **Dallas ▪ 12-15 FEB**
- ♦ **Online Personal Classroom™ ▪ 22-25 JAN ▪ 12-15 FEB ▪ 19-22 MAR ▪ 16-19 APR ▪ 14-17 MAY ▪ 18-21 JUN**

CISSP Preparation—5 day program

- ♦ **Oakland ▪ 26 FEB - 2 MAR**
- ♦ **Dallas ▪ 19-23 MAR**
- ♦ **National Capitol Region ▪ 16-20 APR**
- ♦ **Online Personal Classroom™ 14-18 MAY**

eMASS eSSENTIALS—1 day program

- ♦ **Online Personal Classroom™ ▪ 6 FEB ▪ 7 MAR ▪ 5 APR ▪ 4 MAY ▪ 5 JUN**

Continuous Monitoring Overview —1 day program

- ♦ **Online Personal Classroom™ ▪ 8 FEB ▪ 9 MAR ▪ 3 APR ▪ 2 MAY ▪ 7 JUN**

RMF in the Cloud—1 day program

- ♦ **Online Personal Classroom™ ▪ 9 FEB ▪ 6 MAR ▪ 4 APR ▪ 3 MAY ▪ 8 JUN**

CAP Prep—1 day program

- ♦ **Online Personal Classroom™ ▪ 7 FEB ▪ 8 MAR ▪ 6 APR ▪ 1 MAY ▪ 6 JUN**