July, 2020 Volume 10, **Issue 3**

Risk Management Framework Today…

and Tomorrow

In this issue:

Find us on LinkedIn

BAI Information Security Consulting & Training

RMF and the COVID-19 Pandemic

By Lon J. Berman, CISSP, RDRP

2020 has been a turbulent year, to say the least. When it comes to operating and maintaining our information systems, a lot of the "usual routine" has been disrupted in the name of health and safety. In spite of all this turmoil, the need to sustain a high security posture is more critical than ever.

What are some of the security-relevant changes we're seeing?

- Some of the usual restrictions on handling of unclassified sensitive information are being waived in order to expedite telework. An extreme example of this is DoD's implementation of an enterprise collaboration suite in a cloud environment that is not normally authorized for sensitive information.
- Except for "emergency fixes", some organizations are choosing to postpone maintenance activities that require physical access to equipment.
- Agencies that typically employ on-site assessments as part of their RMF process are relying on remote assessments.
- Organizations are implementing expedited processes for extending existing ATOs without the need for the full RMF process.
- There's even talk that telework access to classified information may be coming down the pike!

Are these good things? Well, with the exception of the last item (and we'll let you make up your own mind on that one), the answer is probably *Yes*… at least in the short run. It seems reasonable to make these *short-term* accommodations to allow the mission to continue without compromise. However, if any of these things become the "new normal", then it gets much more complicated.

We can only hope good quality risk assessments were done before these changes occurred. Unfortunately, given the pace at which most of these things were implemented, it is questionable to what extent *real* risk management is being practiced. Were the threats and vulnerabilities carefully evaluated and appropriate security controls put in place as countermeasures? Are there plans in place, *and* are they being executed, to continuously monitor the effectiveness of these controls and make appropriate adjustments? We don't really know.

What we do know with virtual 100% certainty is that the "usual suspects" (aka. the bad guys) are carefully studying all of this, looking for new weaknesses they can exploit to cause disruption of services or even gain unauthorized access to government systems and data. And they can do it all while isolating themselves and practicing social distancing!

Risk Management Framework Today…

and Tomorrow

"If you're hosting your CUI in the cloud, be sure that you are using a FedRAMP high baseline or an IL 4 service provider. If you aren't, you will have to ensure the Cloud Service Provider (CSP) is compliant with the CMMC requirements."

Find us on LinkedIn

BAI Information Security Consulting & Training

CMMC Assessors Requirements Announced

By Kathryn Daily, CISSP, CAP, RDRP

Despite the current pandemic, the CMMC AB (Cybersecurity Maturity Model Certification Accreditation Body) is moving right along. They have now announced the requirements to become a Certified Professional (CP), Certified Assessor (CA), Certified Third Party Assessment Organization (C3PAO), or Registered Practitioner.

The C3PAO will contract with OSCs (Organizations Seeking Certification) via the CMMC-AB Marketplace that is due to be released at some point this summer. They will schedule assessments, hire and train certified assessors and manage the overall assessment. In order to be a C3PAO, the organization must sign the C3PAO license agreement, provide verification of insurance (minimum coverage amounts are TBD). Insurance policies must consist of General Liability with CMMC Accreditation Body as a Named Insured, Errors and Omissions Policy and Cybersecurity Breach Policy. They will also need to pay the application fee and a C3PAO activation fee (good for 1 year). C3PAOs will be subject to an organizational background check through Dun & Bradstreet and have a DUNS number.

C3PAOs are required to maintain an association with at least one Registered Professional (RP), Certified Professional (CP), or CA (Certified Assessor). There is a 30-day grace period for this requirement. Lastly the C3PAO is required to provide a commercial background check for all ML-1 assessment team members and be a 100% U.S. Citizen Owned Business. Currently foreign ownership considerations are under exploration for all C3PAOs. If performing assessments at Maturity Level 2 (ML-2) and above the CP3AO themselves must be certified at ML-3 or above.

If you're hosting your CUI in the cloud, be sure that you are using a FedRAMP high baseline or an IL 4 service provider. If you aren't, you will have to ensure the Cloud Service Provider (CSP) is compliant with the CMMC requirements.

Certified Assessors and Certified Professionals have their own set of requirements. CPs and CA-1s only need to be a U.S Person (i.e. granted US citizenship or a green card vs being born or naturalized). If they participate as a team member on an ML-2 assessment, U.S. Citizenship is required. CA-3 and above require US Citizenship. One can be a CP with a college degree, 2+ years in cyber or other IT Field, gain CMMC-AB approval of submitted application, complete CMMC-AB Certified professional class from an LPT (Licensed Training provider) and be able to pass a commercial background check.

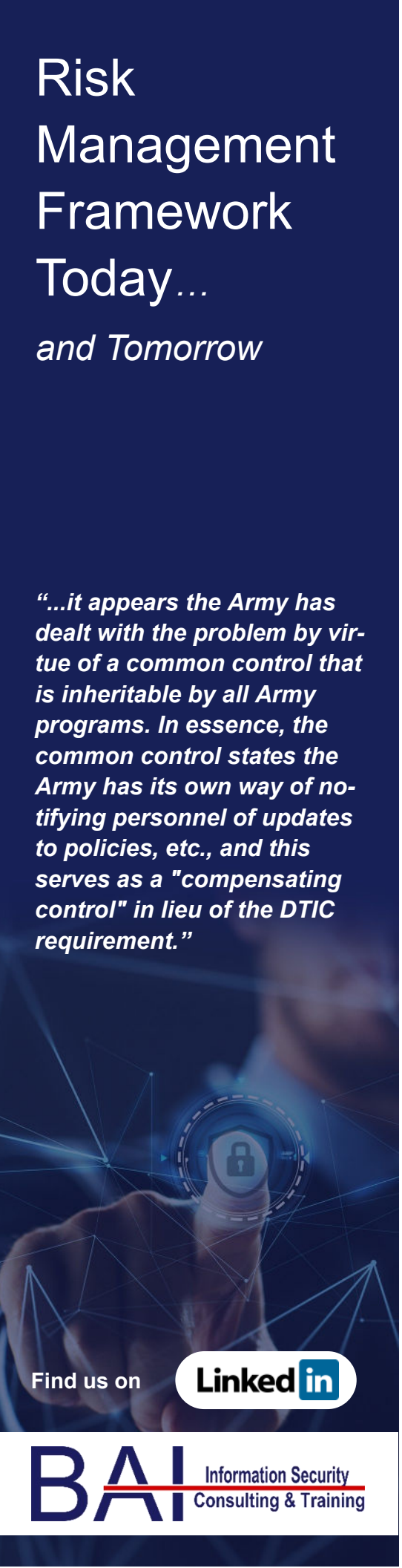
There is a training program and exam for each level of Certified Assessor that must be taken/passed in order to assess at that level. The levels themselves are cumulative, to wit, in order to be a CA-5, you'll need to pass the CA-1 Exam through the CA-5 exam. CA-1 and CA-2 require one to pass a Commercial background check but CA-3 and higher require a National Agency Check (NAC). A clearance is also required and the DoD is providing a mechanism for the CMMC-AB to sponsor clearances for CAs who work for a C3PAO that doesn't have a contract with the Government that requires a clearance. More information on that should be released in the near future.

See scheduled dates for *CMMC Readiness Workshop*...Page 7

Risk Management Framework Today…

and Tomorrow

"...it appears the Army has dealt with the problem by virtue of a common control that is inheritable by all Army programs. In essence, the common control states the Army has its own way of notifying personnel of updates to policies, etc., and this serves as a "compensating control" in lieu of the DTIC requirement."



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 the intent of RMF Control SA-4(9), i.e., whether it can be inherited or if it is intended to be system -specific. The control description states organization but the compelling evidence call for SSP. Furthermore, the AP procedures calls for contract / agreements 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. Other are saying that since the control says organization then it could be inherited. We have had similar debates over other controls written like this? Is there a standard rule of thumb that could be applied? What is the best way to address controls written like this one? System specific or Inheritable thru a common control boundary?

RMF Control Dispute,

Thank you for submitting your question to Dr. RMF. Firstly, I'm not 100% sure about which control/CCI you are referring to. I do see a CCI on the subject of contracts and agreements, and it is under SA-4, not SA-4(9). That 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,

What is the purpose of having all personnel register at the DTIC website to receive update notifications? If we do not implement this, do we need to submit POA&M for risk acceptance to the AO?

Why DTIC,

Regarding CA 1.6, the expression "What were they thinking?" comes to mind. Dr. RMF has no idea why they thought it so important that *everyone* in an organization subscribe to DTIC. That said, you pretty much have no choice but to mark that CCI non-compliant and, as you said, approach your AO for an "acceptance of risk".

Upon further research, it appears the Army has dealt with the problem by virtue of a common control that is inheritable by all Army programs. In essence, the common control states the Army has its own way of notifying personnel of updates to policies, etc., and this serves as a "compensating control" in lieu of the DTIC requirement. I hope that helps.

Dear Dr. RMF,

In my research I cannot find any Agency level documentation that states this, however, I have located examples of contracts that have PII guidance pertaining to contractors. So, would it be considered compliant if I have examples of the contracts or should this be documented at Agency level to provide guidance for everyone? From my interpretation this needs to be documented at an Agency level.

AR-3.4: The organization establishes privacy roles for service providers.
AR-3.5: The organization establishes privacy responsibilities for service providers.
AR-3.7: The organization includes privacy requirements in contracts.
AR-3.8: The organization includes privacy requirements in other acquisition-related documents.

RMF Agency Level Documentation,

I agree the use of the word "organization" in AR-3 (and elsewhere throughout NIST SP 800-53) is subject to interpretation. Based on the other verbiage in the control and underlying CCIs, I agree the intent is for the overarching "organization" (i.e., at command or agency level) to have documented standards for these things.

By the way, in NIST SP 800-53 Rev 5 (new version not yet formally adopted by DoD), the use of terms like "The system owner will do this..." or "The organization will do this..." have been replaced with imperative statements, i.e., "Do this...". In other words, they are stressing the "what to do" over the "who does it". Whether or not this resolves some of the confusion or adds to it remains to be seen.

See *Ask Dr. RMF*...Page 4 for more.

Ask Dr. RMF!... Continued from Page 3

Dear Dr. RMF,

I have a boundary for a web application. My SISO wants to move another web application into this approved boundary. The move is because both have similar operating characteristics, security and privacy requirements, and reside in the same environment of operation. As the SCA for the receiving boundary, what official documentation is required to make the migration official? The moving web application is already in the process of sending me the SSP, STIGs, PIA, etc. What I am more concerned with the changing of my boundary what is required to make the move official? I am being told that no re-adjudication is required for my boundary. I was told my boundary can officially be adjudicated during the annual assessment. Right now, my boundary's ISSO is drafting an SSP and was told to write a brief security assessment. Once those two items are done, then "poof" the move is complete. I can't find in NIST SP or DODI 8510.01 what the correct process is.

RMF Boundary Changes,

Thank you for contacting Dr. RMF with your RMF question.

You are absolutely correct. There is plentiful information from DoD and NIST about establishing system boundaries, but precious little about boundary adjustments. That said, I'll try to be as helpful as I can.

The short answer to your specific situation is that you should treat it as any other change management action, i.e., it should be thoroughly reviewed by the Change Control Board (CCB) of the receiving boundary before any further action takes place. As a part of that review, the CCB should determine if this constitutes a "major change" that should go before the Authorizing Official for a final decision before moving forward. My sense with something like this is that the answer would be YES, so the AO should be engaged early in the process. Since in your case the SISO is the proponent of the change, AO approval is pretty likely.

Once approved, merging the documentation for the two systems will be a major part of the activity. That of course includes producing a consolidated hardware/software inventory, system diagram, etc. The CCB should also ensure that technical compliance such as STIG checklists, ACAS scans, etc., are completed on the consolidated system. Even something as seemingly simple as the name and acronym of the merged system needs to be carefully considered. If you are merging a system called "Apple" into a the boundary of system called "Banana", is it reasonable to continue calling the merged system "Banana", or is this likely to create confusion?

Also, if the system being "merged into" the consolidated boundary has its own ATO, or even a partially completed eMASS record, those need to be properly "decommissioned". If the system being merged also has its own DITPR number (and APMS registration in the case of an Army system), a decision needs to be made about whether to keep those separate or merge them as well.

All things considered, one system boundary is better than two, at least in terms of the RMF level of effort, i.e., cost, so as a citizen and taxpayer, I hope the process goes well for you.

Risk Management Framework Today…

and Tomorrow

"RMF Supplement for DCSA Cleared Contractors is a one-day class designed as a follow-on to RMF for DoD IT training. This class focuses on the "delta" between "standard" RMF and the process mandated in the DCSA Assessment and Authorization Process Manual (DAAPM)."

Find us on LinkedIn

BAI Information Security Consulting & Training

New Training Opportunity!

RMF Supplement for DCSA Cleared Contractors

By Lon J. Berman, CISSP, RDRP

In a previous edition (January, 2020) of *RMF Today … and Tomorrow,* we presented an overview of the adoption of RMF and eMASS by the Defense Counterintelligence and Security Agency (DCSA) for use by cleared contractor companies operating within the National Industrial Security Program (NISP). BAI is pleased to announce that RMF training is now available specifically for cleared contractor companies operating under the purview of DCSA!

RMF Supplement for DCSA Cleared Contractors is a one-day class designed as a follow-on to RMF for DoD IT training. This class focuses on the "delta" between "standard" RMF and the process mandated in the DCSA Assessment and Authorization Process Manual (DAAPM).

If your company has a Facility Clearance (FCL) and maintains one or more on-premise, Classified IT systems, this is the class for you!

Topics include:

- Introduction to DCSA
- RMF Roles and Responsibilities
- Security Training
- Types of Systems
- Authorization Boundaries
- RMF Life Cycle
- Documentation Artifacts
- Type Authorization … and more
- Security Control Inheritance
- NISP eMASS
- Support Tools and Resources

RMF Supplement for DCSA Cleared Contractors is being offered regularly in an online, instructor-led format through our Online Personal Classroom™ technology. The schedule of classes and registration information can be found on the back page of this newsletter, or at https://register.rmf.org. Additionally, BAI instructors are available to present a private class for your organization, either online or at your site.

BAI's Hands-on eMASS Simulator

By P. Devon Schall, PhD, CISSP, RDRP

BAI recognizes that eMASS is a stumbling block for many new RMF practitioners. To mitigate these challenges, our instructional designers felt the creation of an eMASS sandbox environment where our students could practice working in eMASS without being scared to submit incorrect data or follow the correct procedures would be highly beneficial!

After working with a software development partner over the last year, BAI is pleased to announce completion of development on our new eMASS eSSENTIALS simulator. Our eMASS simulator activities will replace pre-recorded eMASS simulations which are currently offered in BAI's eMASS training.

Some facts about our new eMASS Simulator:

- Live hands on cloud-based eMASS smulation environment
- The simulator will be available to all students who attend BAI's one-day eMASS eSSENTIALS training course
- The eMASS Simulator provides guidance and the capability for the most commonly-use eMASS functions including:
  - System Registration
  - Security Controls and Test Results
  - Artifacts
  - Asset Manager
  - Plan of Action and Milestones (PO&AM)

We anticipate formally integrating the new eMASS eSSENTIALS Simulator into our classes later this summer.

For additional information or a live demo, please contact BAI Executive Director of Training Services, Devon Schall, Ph.D, CISSP devon@rmf.org.

Risk Management Framework Today…

and Tomorrow

"Federal agencies, many of which are tasked with matters of national security, are now obliged to follow these newer standards in order to hire the best and brightest."

Find us on LinkedIn

BAI Information Security Consulting & Training

Federal Hiring Process Overhaul: Stressing Skills vs Traditional Academic Achievement

By Amanda Jones

On June 26, 2020, President Donald J. Trump issued the Executive Order on Modernizing and Reforming the Assessment and Hiring of Federal Job Candidates, in an effort to bring government agencies up to speed with newer hiring standards in the private sector. This comes in the wake of immense economic disruption caused by the COVID-19 pandemic, during which many businesses across America have restructured, conducted mass lay-offs, or shut down altogether. For those who are unemployed due to these developments, or for recent graduates looking to make their professional start, finding a job is vital. The question is: who gets hired and whose resume is tossed?

For decades, it seemed a college education was a "golden ticket" of sorts to a promising career, creating highly lucrative opportunities for graduates. In today's "Age of Information," a Bachelor's or Master's degree is often a pre-requisite for several entry-level positions. The problem? Employers can attest that a college degree is not always indicative of a good employee.

As a student pursuing a B.S. in Computer Science with a cognate in cyber security, I must confess that, despite the quality of the curriculum and of my professors, my coursework alone is insufficient to fully prepare me for a longstanding career in my desired specialty. Take the field of penetration testing as an example, where technical chops take years to develop. Since I benefit from an honors scholarship, grades are my top priority, which means I devote as much time to courses in mathematics as those in programming or networking. The result is a broad yet shallow expanse of knowledge—a good baseline for a variety of career paths. Without supplementary practice, training, and internship experience, however, I am ill-equipped to join a contracting red team.

At the same time, somewhere else in the world, a young pentester-in-the-making is unable to attend college, but has spent many sleepless nights learning the ins and outs of various Linux distros and knocking her head on the table trying to find the bug(s) in her Python script. In both cases, the apprentice is taught to persevere. After four years, one becomes a jack of many trades and earns a diploma, and one becomes rather advanced in their specialty, perhaps picking up a few certifications along the way.

Which is the better hire? There are many factors which set a candidate apart for hire in technical fields. If the sole difference is an advanced skillset vs. a Bachelor's degree, the specialist in the relevant skillset will always be preferable. Hence why job postings in technology stress the importance of certifications, technical proficiencies, side projects, and experience during the hiring process. Federal agencies, many of which are tasked with matters of national security, are now obliged to follow these newer standards in order to hire the best and brightest.

The end-goal is to remove the barrier to entry in federal agencies by rectifying an "overreliance on college degrees" when choosing a new hire, focusing more on competencies and experience. Being a young and green professional in infosec, I cannot predict what exact organizational changes will be incited among federal agencies as a result. I can only recommend that my fellow students continue developing relationships, practical job experience, and skills in order to bolster the standard of expertise among graduates in the American workforce.

The Executive Order can be read in full at https://www.whitehouse.gov/presidential-actions/executive-order-modernizing-reforming-assessment-hiring-federal-job-candidates/.

Editor's note; Amanda is a rising junior at Liberty University and a Business Development intern at BAI. She is also President of LU's Cyber Defense Club, and a member of the LU Collegiate Cyber Defense Competition team.

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 Supplement for DCSA Cleared Contractors** – This one-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.

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 December, 2020:

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

- **Colorado Springs ▪ 10 - 13 AUG ▪ 5 - 8 OCT**
- **Pensacola ▪ 24 - 27 AUG ▪ 26 - 29 OCT**
- **San Diego ▪ 14 - 17 SEP ▪ 2 - 5 NOV**
- **Herndon, VA ▪ 28 SEP - 1 OCT**
- **Virginia Beach ▪ 16 - 19 NOV**
- **Online Personal Classroom™ ▪ 20 - 23 JUL ▪ 3 - 6 AUG ▪ 17 - 20 AUG ▪ 31 AUG - 3 SEP ▪ 14 - 17 SEP ▪ 21 - 24 SEP ▪ 5-8 OCT ▪ 19-22 OCT ▪ 26-29 OCT ▪ 2-5 NOV ▪ 16-19 NOV ▪ 7-10 DEC ▪ 14-17 DEC**

RMF Supplement for DCSA Cleared Contractors—1 day program

- **Online Personal Classroom™ ▪ 24 JUL ▪ 21 AUG ▪ 8 SEP ▪ 18 SEP ▪ 27 OCT ▪ 10 NOV**

CMMC Readiness Workshop—3 day program

- **Online Personal Classroom™ ▪ 14-16 JUL ▪ 11-13 AUG ▪ 21-23 SEP ▪ 19-21 OCT ▪ 1-3 NOV ▪ 15-17 DEC**

eMASS eSSENTIALS—1 day program

- **Colorado Springs ▪ 14 AUG ▪ 9 OCT**
- **Pensacola ▪ 28 AUG ▪ 30 OCT**
- **San Diego ▪ 18 SEP ▪ 6 NOV**
- **Herndon, VA ▪ 2 OCT**
- **Virginia Beach ▪ 20 NOV**
- **Online Personal Classroom™ ▪ 24 JUL ▪ 21 AUG ▪ 25 AUG ▪ 10 SEP ▪ 18 SEP ▪ 23 OCT ▪ 6 NOV ▪ 23 NOV ▪ 18 DEC**

STIG 101—1 day program

- **Online Personal Classroom™ ▪ 10 JUL ▪ 7 AUG ▪ 26 AUG ▪ 4 SEP ▪ 9 SEP ▪ 25 SEP ▪ 9 OCT ▪ 30 OCT ▪ 20 NOV ▪ 24 NOV ▪ 11 DEC**

Continuous Monitoring Overview—1 day program

- **Online Personal Classroom™ ▪ 10 SEP ▪ 12 NOV**

RMF in the Cloud—1 day program

- **Online Personal Classroom™ ▪ 8 SEP ▪ 9 NOV**

SCA Workshop—2 day program

- **Online Personal Classroom™ ▪ 28-29 JUL ▪ 24-25 SEP ▪ 9-10 NOV ▪ 8-9 DEC**