FAQ for current CMMC Certified Professional (CCP) and CMMC Certified Assessors (CCA)

This FAQ is intended for those individuals who have completed CCP and/or CCA training with a Licensed Training Provider (LTP), soon to be Approved Training Provider (ATP) **AND** have passed their CCP and/or CCA examination prior to the CMMC rule entering into force.

Q: What does "rule entering into force" mean?

A: Once the rule is published to the Federal Register, it will specify how many days until the program enters into force. For example, it might say 60 days to when the CMMC rule is effective-in-force. Therefore, the CMMC program will be considered an official DoD program 60 days from when the CMMC rule is published on the Federal Register, and the Title 32 rule will go into effect.

Q: What happens to CCPs and CCAs when the CMMC rule goes into effect?

A: All CCPs and CCAs who have **NOT** met the new requirements introduced in the proposed rule will be temporarily "suspended". They will be removed from The AB Marketplace and their badge will be disabled. Therefore, individuals will not be allowed to market themselves as "certified" CCPs and/or CCAs and use their badges.

Q: What are the "new" requirements for a CCP and/or CCA that must be met to be considered "certified"?

A: Both CCPs and/or CCAs are required to take and successfully complete training with an LTP/ATP and pass their examination through Meazure Learning. Once the rule goes into effect, to be considered "certified", per the DoD, to work on CMMC assessments will additionally require the following requirements being met:

September 25, 2024

CCP:

- Hold an active Tier 3 favorable determination

CCA:

- Hold an active Tier 3 favorable determination
- Have three (3) years of Cybersecurity experience
- Have one (1) year of audit or assessment experience
- Hold at least one (1) baseline certification aligned to the Intermediate Proficiency Level for Career Pathway Certified Assessor Job ID 612 from the DoD Manual 8140.3 found here: https://public.cyber.mil/dcwf-work-role/security-control-assessor/
    - **Note:** If you hold an Advanced Level certification from 8140.3 Job ID 612, that will still qualify you for meeting this CCA requirement.

Q: Does anything else on the 8140.3 Job ID 612 matrix, like a college degree, count for CCA?

A: No. The CMMC rule specifies **only** personnel certifications from Intermediate or above from 8140.3 Job ID 612 will count for the CCA role.

Q: How can I get my CCP and/or CCA reinstated?

A: Once you have met the new requirement(s) (noted above) and your profile has been updated the system will add you back to The AB Marketplace on the CCP, CCA, or both pages. Also, you will be able to download your new badge(s) from your profile as you did previously.

Q: Since I won't be on the Marketplace or have a CCP and/or CCA badge while I complete the requirements, is there anything I can show that will demonstrate I've successfully completed training and passed the exam?

A: Yes. We are creating a verification document that will validate successful training completion and testing for CCP and/or CCA that will be available in your profile. This is in development and once it's complete we will advise all CCPs and CCAs of the process for obtaining this document.

Q: Is there going to be a cost associated to reinstate a suspended CCP and/or CCA?

A: No. There will be no cost associated to this reinstatement. However, if your account is not in good standing with the CAICO you would be required to pay your annual renewal fee to keep your CCP and/or CCA account active.

Q: What happens if I never meet the new requirements?

A: You will remain in a "suspended" state and will not be listed on the Marketplace or hold a badge for CCP and/or CCA. If you continue to pay your annual maintenance fee to the CAICO, you will remain in the system. If you do not pay your annual maintenance fee, then you will no longer be active with the CAICO and therefore to get back into the program you would have to re-apply and start the process over.

Q: Is there any way to expedite my Tier 3?

A: No. This process is a first come first serve. However, if you have a current clearance that may expedite your application processing.

Q: What happens if I currently have an active Tier 3, and it expires during this suspension period?

A: You would be required to reapply for the Tier 3 or equivalent.

Q: What does equivalent mean in the context of Tier 3?

A: If you are eligible to apply for Tier 3, for example a US citizen, then you would apply for Tier 3. However, if you are not eligible the DoD will be providing the CAICO a list or "equivalent" background checks that would qualify the for meeting the Tier 3 requirement. That list will be shared once it has been provided by the DoD.

Q: Do I have to meet these requirements for CCA in any specific order?

A: Similar to our current process you have to apply, take your training with an LTP/ATP and then pass your exam. Those are sequential, however for submitting your cybersecurity and audit/assessment experience and validation of 8140 certification those can be submitted anytime after you apply for CCA.

Q: What happens to my certification expiration date?

A: Your certification expiration date will now be tied to the last thing you do for that certification. For example, if you are a CCA candidate and the last requirement you need to meet is your one (1) year of audit/assessment experience then once that is submitted and validated then you would be considered "certified" as a CCA and your three (3) year expiration would be based on the date your last requirement was met.

Q: Are the three (3) assessments still required?

A: No. With the addition of these new experience and certification requirements the three (3) assessment requirement has been removed.

September 25, 2024

Q: What do I need to submit for the new requirements?

A: Below is the recommendation for these new CCA requirements submissions.

3 or 5 years of cybersecurity experience (CCA, Lead CCA): The applicant has worked in a cybersecurity role(s). Examples include working in a security operations center (SOC), assessing cybersecurity compliance for an auditing firm, serving as a chief information security officer, and serving on a cybersecurity red team. Working in non-technical roles, or roles that do not have security responsibilities would not meet the requirement, even if the firm's line of business is cybersecurity.

The applicant should provide a resume that clearly describes the roles, tasks, and duration of these cybersecurity role(s).

1 or 3 year(s) audit or assessment experience (CCA, Lead CCA): The applicant participated on multiple assessments or audits in which the applicant's role was to work on the team conducting the internal or external audits/assessments. These audits/assessments should be based on a compliance standard and include examining and verifying evidence of the internal or external customer.

This requirement is intended to validate the ability to audit or assess by abiding to a compliance standard while applying skills in working with a team and applying rigor to the validation of an audit/assessment. Participation on a CMMC assessment team as a CCP is one example of appropriate experience. Other assessments or audits that might qualify include: CMMI, NIST 800-171, financial auditing, and FedRAMP assessments. These are just a few examples and not a comprehensive list.

The applicant should provide documentation that clearly details this prior experience. The information should include for each audit/assessment:

- Assessment or audit type
- Applicant's work role and responsibilities during the audit/assessment
- Length of the applicant's involvement in each audit/assessment

5 years managements experience (Lead CCA): The applicant has worked with a professional environment in a managerial capacity for a minimum of five years. This experience need not be in a formal role with a title of "manager." Serving as a project lead or assessment team lead would be acceptable, for example. Applicants should demonstrate that they can:

- Manage staff
- Drive results for internal or external stakeholders

- Effectively communicate
- Execute in difficult environments or situations
- Be organized and meet deadlines
- Resolve conflicts

The applicant should provide a resume that clearly denotes the roles, tasks, and duration of these management roles.

September 25, 2024