Becoming a Cybersecurity Maturity Model Certification (CMMC) Assessor

Thank you for your interest in becoming a CMMC Assessor. This role is vital for protecting our nation by assessing the cybersecurity resilience of Defense Industrial Base (DIB) companies who provide goods and services to the Department of Defense (DoD).

This document is designed to provide you the information needed to navigate becoming a CMMC assessor.

As The Cyber AB and Cybersecurity Assessor & Instructor Certification Organization (CAICO) are implementing the CMMC program on behalf of the DoD's Program Management Office (PMO), it is recommended that before you begin (if you haven't already done so), you should familiarize yourself with the CMMC program information found here: About CMMC (defense.gov). This is a key site in which the DoD provides updates and documentation as the program evolves, which as an assessor will be important to keep current. Another resource available for monthly CMMC updates is The Cyber AB Town Halls. To register for notifications for upcoming town halls, go to The Cyber AB website (CyberAB > Home) and click on the "Register Now" message at the top of the page. Lastly, CMMC is based on National Institute Standards and Technology (NIST) 800-171r2 which can be found here: SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations | CSRC (nist.gov) . There will be other resources as part of your CMMC training, but these are important sites to be aware of.

Am I qualified to become a CMMC Assessor?

Do you have the right skills to participate on assessing the cybersecurity stance of a DIB company? Do you have both the technical and collaborative skills to work on a team of assessors directly working with clients?

To understand the certification requirements, please review the following skills and/or professional/educational experience for pursuing the CMMC assessor certification(s):

CMMC Certified Professional (CCP)

Certification Requirements for CCP:

1. Apply and Remain in good standing with the CAICO;
    a. Sign and Comply with agreements as part of the application process
    b. Pay Fees (initial application and annual renewal fees)
2. Complete CMMC Certified Professional class/course offered by an Approved Training Provider (ATP), formerly referred to as a Licensed Training Provider (ATP);
3. Pass CMMC Certified Professional Examination; and
4. Obtain or have a Tier 3 determination from DoD or equivalent background check. The DoD will provide what will qualify as equivalent for the CMMC program for non-eligible Tier 3 candidates

Important Note: You cannot apply for Tier 3 until after passing the CCP exam. By the 10th of the following month of your exam you will be sent an email with detailed instructions on how to apply for Tier 3. This process is not managed by the CAICO, other than to collect the initial information. Once your information is received by the CAICO and sent to the DoD PMO office, the CAICO will have no updates or visibility as to the status of the application. You will be notified by WHS to begin the investigation. The CAICO will notify you once the Tier 3 background has completed and a determination has been made. This can be a lengthy process and can take many months. If you hold a current clearance equivalent to a Tier 3 or above, the process could be expedited by submitting a statement from your FSO (or equivalent) that includes your clearance information.

Upon meeting these requirements, the candidate will be able to download their official CMMC Certified Professional badge and will be listed on The Cyber AB Marketplace under the CCP category.

Note: You may not be planning to become a CMMC Assessor but find obtaining your CCP important for demonstrating your CMMC knowledge. Therefore, if you successfully complete your CCP training and pass your CCP examination you will receive a certificate from the CAICO to demonstrate your achievement to others.

To be successful, the recommended educational and/or experience for the CCP program is outlined below:

- College degree in a cyber or informational technology field or 2+ years of related experience or education or 2 years of equivalent experience (including military) in a cyber, information technology, or assessment field; and
- CompTIA A+ certification or equivalent knowledge/experience; and
- DoD CUI Awareness Training DoD Mandatory Controlled Unclassified Information (CUI) Training (usalearning.gov)

Steps for becoming a CCP:

1. Complete CCP Application - Assessing and Certification | Cyber-AB (cyberab.org) , select “CCP Enroll Here”

2. Pay CCP Application Fee, you will obtain CMMC Professional Number (CPN)

3. Sign Code of Professional Conduct (CoPC)

4. Sign Individual Service Agreement – referred to as “Agreement.”

5. Successfully complete CCP training with an Approved Training Provider (ATP). Your selected ATP will provide your completion information to the CAICO, you will see your training entitlement checked off once this has been completed, typically takes 3-5 business days from completion of training.

Important Note: to access the exams, training must be conducted by an Approved Training Provider (ATP) found on The Cyber AB marketplace. If the provider is not listed on this site, they are not approved to offer “official” CMMC training for the certification programs, therefore you will not have access to the exams. Below is the link to the Marketplace: CyberAB > Directory.

6. Pay your exam fee

7. Take and successfully pass the CCP examination

8. Upon passing your CCP exam you will receive an email that will provide the details for applying for Tier 3 (US citizens). Upon earning Tier 3 or equivalent the CCP certification process is complete.

CMMC Certified Assessor (CCA)

Certification Requirements for CCA:

- Hold an active CMMC Certified Professional Certification;
- Obtain or have a Tier 3 determination from DoD or equivalent background check. The DoD will provide what will qualify as equivalent for the CMMC program for non-eligible Tier 3 candidates;
- Remain in good standing with the CAICO;
    a. Sign and Comply with agreements as part of the application process
    b. Pay Fees (initial application and annual renewal fees)
- Complete CMMC Certified Assessor class/course offered by an Approved Training Provider (ATP), formerly referred to as a License Training Provider (ATP);
- Pass CMMC Certification Assessor examination;
- Have at least 3 years of cybersecurity experience;
- 1 year of assessment or audit experience; and
- Hold at least one baseline certification aligned to the Intermediate and/or Advanced Proficiency Level for the Career Pathway Certified Assessor 612 from the DoD Manual 8140.3 Cyberspace Workforce Qualification & Management Program. https://public.cyber.mil/dcwf-work-role/security-control-assessor/

    Note: please check this site as the DoD may update qualifying certifications on this page. Below is a table of qualifying certifications for CCA's as of September 2024.

8140.3 – 612 Certifications

Intermediate	Advanced
• (ISC)2 **CGRC/CAP or** • CompTIA **CASP+ or** • CompTIA **Cloud+ or** • CompTIA **PenTest+ or** • CompTIA **Security+ or** • GIAC **GSEC**	• ISACA **CISM or** • United American Technologies, LLC dba Mile2 **CISSO or** • United American Technologies, LLC dba Mile2 **CPTE or** • CompTIA **CySA**+ **or** • Federal IT Security Institutes **FITSP-A or** • GIAC **GCSA or** • ISACA **CISA or** • (ISC)2 **CISSP or** • (ISC)2 **CISSP-ISSEP or** • GIAC **GSLC or** • GIAC **GSNA**

Steps for becoming a CCA:

1. Complete CCA Application - Assessing and Certification | Cyber-AB (cyberab.org) , select “CCA Enroll Here”

2. Pay CCA Application Fee

3. Sign Code of Professional Conduct (CoPC) – this will only be required again if the agreement has changed or if one (1) year has passed from the last signature

4. Sign Individual Service Agreement – referred to as “Agreement.” – this will only be required again if the agreement has changed or if one (1) year has passed from the last signature

5. Self-Attest and provide evidence of educational and experience requirements:

   a. 3 years of cybersecurity experience
   b. 1 year of audit or assessment experience
   c. 8140.3 612 certification (list above)

6. Provide Tier 3 or equivalent background information

> **Note:** Steps 5 and 6 can be completed anytime, but certification will not be granted until **all** the steps have been completed.

7. Successfully complete CCA training with an Approved Training Provider (ATP). Your selected ATP will provide your completion information to the CAICO, you will see your training entitlement checked off once this has been completed, typically takes 3-5 business days from completion of training.

Important Note: to access the exams, training must be conducted by an Approved Training Provider (ATP) found on The Cyber AB marketplace. If the provider is not listed on this site, they are not approved to offer “official” CMMC training for the certification programs, therefore you will not have access to the exams. Below is the link to the Marketplace: CyberAB > Directory.

8. Pay your exam fee

9. Take and successfully pass certification the CCA examination

For detailed information on the application and exam registration process please go to: How to Register for the CMMC Certified Professional.pdf (cyberab.org) , these processes are also for pursuing CCA.

Do I have to be a United States (US) citizen to become a CMMC Certified Assessor?

No, becoming a CMMC Certified Assessor requires successfully meeting the requirements for the certification.

Those that are eligible for Tier 3 (US citizens) are required to pursue this background check. Those that are not eligible to apply for Tier 3 will need to pursue a DoD approved background check. At this time, the DoD has not provided that list of approved background checks. We will update the website and this document as that information is provided.

How do I prepare for my certification examination?

The selected ATP is responsible for providing the training and resources needed for preparing for an exam. Pure self-study is **NOT** allowed for the CMMC certification programs. As these are high-stakes cybersecurity exams, the candidate should plan for a rigorous study program following the completion of training, these are **NOT** open book exams.

To better understand what is fair game on a CMMC examination you should first review the objectives blueprints.

CCP - cmmc-ab-ccp-blueprint-10-17-22-final-v7.4 Final (Public).pdf (cyberab.org)
CCA - cmmc-ab-cca-blueprint-12-14-22-Final v3.3 (Public).pdf (cyberab.org)

Note: The selected ATP will provide the candidate with the correct version of the CMMC Assessment Process (CAP) document (version 5.6.1), do **NOT** use the one posted to The Cyber AB website.

What happens after completing training with an ATP?

The selected ATP is responsible for providing the successful training completion data to the CAICO, **do not** submit it yourself it will not be counted.

The ATPs are requested to submit training rosters to the CAICO no later than the EOD Monday following the completion of training. Training entitlement will be marked as completed on your profile no later than EOD Wednesday. You must provide your CPN to the ATP at the time of training. Training will only be marked complete if a CPN is provided as part of the submission.

After training is marked complete, you can then pay for the exam. Once payment is made, your information is transmitted to Meazure Learning, which will trigger the Notice to Schedule email from Meazure Learning. This could take up to 24 hours for the email to be sent.

Important: We always recommend you use your personal and not a work email address for anything related to pursuing training and certification. This will help important emails, such as the exam registration email, from being caught by a spam filter.

How do I register for an examination?

As noted above please review the steps in the following document: How to Register for the CMMC Certified Professional.pdf (cyberab.org).

Important: Please also familiarize yourself with all exam policies found here: Certified CMMC Exam Information | Cyber-AB (cyberab.org).

What happens if I fail the exam on the first attempt?

If an exam is failed on the first attempt, there is a 30-day waiting period before you can go back into your profile to pay for your second exam attempt to trigger a new exam registration email. The 30-days starts from the date of failing the exam on the first attempt.

To understand how the exams are scored please review the following information:
CCP - CMMC CCP Scale Scores FINAL.pdf (cyberab.org)
CCA - CMMC CCA Scale Scores FINAL.pdf (cyberab.org)

Note: Each candidate is **only allowed two paid attempts per exam (i.e. CCP, CCA)**. If fail an exam twice then they will be required to retrain with an ATP before gaining two more paid exam attempts.

How do I apply for Tier 3?

Though The Cyber AB and CAICO have nothing to do with Tier 3 investigations themselves, the CAICO does submit your information to the DoD. After that submission the CAICO has no visibility to status of the investigation until it completes. At that time, the CAICO will be notified of the determination. The CAICO will then notify you of the determination.

After passing the CCP exam, you will receive an email from the CAICO with all the information for applying. This email will be sent by the 10th of the following month in which you passed the CCP exam. **Important:** Please read **all** of the information included in this email carefully and completely. Failure to comply with any of the requirements will result in rejection of your application.

Individuals must be US citizens to apply for Tier 3.

This process can take anywhere from 2 months to a year, we've have seen both scenarios. Though on average it typically takes 4-6 months. If you already hold a DoD Tier 3 favorable determination this could expedite the processing time.

Things that can impact your Tier 3 processing:

1. Not completing the application fully
2. Not providing a current resume when submitting the application
3. Not responding to the investigator within 5 business days from receiving your investigation email. Not responding could result in being removed from the "queue" and having to start the application process over.

If you are not eligible for Tier 3, the DoD will be providing a list of equivalent background checks that will meet the Tier 3 requirement. This list will be made available as soon as the DoD has provided it to the CAICO.

What is the submission recommendation for the CCA requirements (cybersecurity and audit and assessment experience)?

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.

Who do I contact if I have any questions?

Please send questions to support@cyberab.org. The team will respond in 3-5 business days.