INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

Certified CMMC Assessor (CCA) Boot Camp

Revised for the launch of the CMMC version 2.0. this bootcamp will teach you the skills and knowledge you need to pass your CMMC CCA exam and perform the duties required of a Certified Assessor of Organizations Seeking Certification (OSC) at CMMC Level 2.

Course description

Designed to help ensure appropriate levels of cybersecurity practices and processes were in place to protect federal contact information (FCI) and controlled unclassified information (CUI), this boot camp explores the updated CMMC version 2 which has been redesigned to offer a more streamlined and manageable maturity model for the DoD and its hundreds of thousands of partnering SMBs. The Certified CMMC Assessor (CCA) exam is intended for professionals who have completed the Certified CMMC Professional (CCP) exam and are seeking to advance to be e level 2 Certified CMMC Assessor (CCA) or who wish to help others on this path by serving as instructors for Certified CMMC Assessor courses.

Who should attend

- Certified Professionals (CCP) who want to continue the Certified Assessor (CCA) career path
- Consultants looking to provide CMMC guidance
- Anyone looking to build a foundation of knowledge around the CMMC Level 2 requirements and practices
- Those interested in providing or teaching CCA courses

Boot camp at a glance

What you'll learn

- ✓ Certified Assessor (CCA) ethics and resources
- ✓ CMMC assessment phases and methodology
- ✓ CMMC level 1 & 2 practices

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 5-day boot camp
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

What's included

- Five days of expert, live Certified CMMC Assessor training
- Exam Insurance
- Exam payment
- Unlimited practice exam attempts
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Knowledge Transfer Guarantee

Prerequisites

In order to become a Certified Assessor, you must first become a CMMC-AB Certified Professional (CCP). In addition, you must:

- Be a U.S. citizen
- Have participated in at least three level 2 CMMC assessments
- Achieved DoD suitability verification

Certified CMMC-AB Assessor (CCA) overview

Infosec's Certified CMMC Assessor Boot Camp prepares you to pass your assessor exam and become qualified to conduct level 2 CMMC-AB assesments. This course covers the core knowledge areas needed for the exam including

- Evaluating Organizations Seeking Certification (OSC) against CMMC Level 2 requirements
- Scoping CMMC level 2 assessments
- Understanding the CMMC Assessment Process (CAP)
- Assessing CMMC Level 2 Practices
- Utilizing NIST 800-171 standards

Certified CMMC Assessor (CCA) career path

CCAs are advanced assessment professionals and must have completed the following steps to qualify for the CCA exam and certification:

- **Complete Certified CMMC Professional (CCP):** An entry-level certification used as a prerequisite to become a Certified Assessor (CA) or to complete level 1 CMMC assessments.
- Participate in 3 level 2 assesments reviewing level 1 CMMC processes and practices
- Be a US Citizen who has achieved DoD suitability

Upon completion of their certification process CCA professionals will be ready for the following options and career paths:

- Serving as a Certified CMMC-AB Assessor capable of planning, conductn, and supervising level 1 and level 2 assessments
- Acting as an Instructor for future CCA and CCP training programs
- Preparing for future CCA Level 3 assessment requirements once the updated requirements are published

Cybersecurity maturity levels

The CMMC model has three increasingly progressive levels for measuring cybersecurity maturity. CMMC 2.0 eliminates all maturity processes and all CMMC unique security practices. In this boot camp, you'll learn what goes into each of the following levels:

- **CMMC 2.0 Level 1 (Foundational)**
  - » Annual Self Assessment
  - » 17 Practices
- **CMMC 2.0 Level 2 (Advanced)**
  - » 110 Practices
  - » Based on NIST SP 800-171
  - » Triennial 3rd party assessments for critical national security information
- **CMMC 2.0 Level 3 (Expert)**
  - » 110+ Practices
  - » Based on a subset of NIST SP 800-172

CMMC-AB Licensed Training Provider and Licensed Partner Publisher

Infosec is a Licensed Training Provider (LTP) and a Licensed Partner Publisher (LPP) for the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB), an independent accreditation entity created in January 2020 that's responsible for establishing, managing, controlling and administering the CMMC assessment, certification, training and accreditation processes for the defense supply chain.

Check out the Infosec CMMC resource hub for additional information.

What our students are saying

Incredible! I have attended classes where the instructor just read PowerPoints — our instructor added so much additional information to the class and knows the field of security inside and out! I was very pleased with his knowledge and instructional skills.

Sheree Moore
Mobile County Public Schools

I went to West Point for my bachelor's, Columbia for my master's and had multiple Army-led courses, and this ranks as one of the best, most engaging courses that I have ever had.

William Jack
Deloitte Consulting, LLC

The instructor was able to take material that prior to the class had made no sense and explained it in real-world scenarios that were able to be understood.

Erik Heiss
United States Air Force

Skill up and get certified, guaranteed

Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

Certified CMMC-AB Assessor (CCA) Boot Camp details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4	Day 5
Morning session	Introduction Domain 1: Evaluation OSC against CMMC level 2 - Task 1 part 1	Domain 2: CMMC Level 2 Assessment Scoping - Tasks 1-2	Domain 3: CMMC Assessment Process (CAP) - Task 1 part 1	Domain 4: Assessing CMMC Level 2 Practices - Task 1 part 1	Course and CMMC CCA certification process recap and review Overview of next steps and exam information
Afternoon session	Domain 1: Evaluation OSC against CMMC level 2 - Task 1 part 2	Domain 2: CMMC Level 2 Assessment Scoping - Task 3	Domain 3: CMMC Assessment Process (CAP) - Task 1 part 2	Domain 4: Assessing CMMC Level 2 Practices - Task 1 part 2	CMMC-AB CCA Exam practice and prep
Evening session	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

Ethics of assessors

- Describe tasks and functions to be performed
- Describe Code of Professional Conduct rules for assessors
- Describe Code of Professional Conduct rules for assessment team members
- Describe leadership training for running an assessment team
- Define referral, "bounties," relationships with preparatory firms, consulting agencies or other conflicts of interest
- Identify who and how to contact in case of questions or risks to the integrity of the assessment process

Federal contractor culture

- Describe handling contractors new to cybersecurity and compliance in different sectors
  - Trades, construction and factories
  - Non-IT office and administrative organizations
  - IT and high-tech organizations
  - Higher education and research institutions
  - Other organizations
- Assessment standards
  - Define "performed"
  - Define evidence requirements
  - Evidence to be collected
    - Evidence could be a physical or data artifact in such a format that verification is possible. Archiving methods must be utilized in order to preserve the integrity of what has been collected.
  - Historical time requirement for evidence
    - How far back should or could evidence be checked, tested and collected?

- Describe samples of evidence that could be collected for each practice
- Identify evidence collection methodology
- Evidence preservation
- Practice testing
  - How to test each practice
  - What to look for
  - Fraudulent artifacts
  - How to deal with fraudulent artifacts and their creators
- Describe role of an assessor
  - Assistive to those new to the process; the goal is to support, rather than disqualify

Identify and describe CMMC reference and source documents

- NIST 800-171
- NIST 800-172
- DFARS 7012
- NIST 800-53

Define and describe Federal Contract Information (FCI)

- What is FCI?
- FCI authoritative sources
- What components and fields does it contain?
  - What is allowed?
  - Auto-deny anything else
- Which of those are public and not protected?
- Which of those are private and have mandatory protections?
- Are any of them potentially CUI or Classified?
- Do different agencies use FCI differently?
- Where can FCI be stored?
- Where can public FCI or protected FCI be used?
- What controls and practices are layered on FCI?
- What are the effective and theoretical differences between FCI and CUI?

Define and describe assessment methodology

- Phase 1: Plan and prepare assessment
  - Analyze requirements
    - Scoping discussion
  - Develop assessment plan
  - Verify readiness to conduct assessment
- Phase 2: Conduct assessment
  - Collect and examine objective evidence
  - Rate practices and validate preliminary results
  - Generate final recommended assessment results
- Phase 3: Report recommended assessment results
  - Deliver recommended assessment results
    - Where to send the results?
    - How to display the results to an organization?
    - Where to send the evidence artifacts?
    - How to access those artifacts, by the assessor, OSC, etc?
- Phase 4: Remediation of outstanding assessment issues
  - Identify remediation approach
  - Execute remediation approach and review
  - CMMC assessment adjudication
- Phase 5: Describe business matters
  - Define payment matters
  - Define referrals
  - Identify contract clauses applicable in your jurisdiction
  - Describe disputes
    - Client disputes
    - Assessment disputes
  - Describe business insurance
    - General liability
    - Error & omission (E&O)
    - Umbrella
    - Anything specific to your jurisdiction or vertical

Assess organizational capabilities

- Access control (AC)
  - C001 – Establish system access requirements.
  - C002 – Control internal system access.
  - C003 – Control remote system access.
  - C004 – Limit data access to authorised users & processes.
- Awareness & Training (AT)
  - C011 – Conduct security awareness activities
  - C012 – Conduct training.
- Audit and Accountability (AU)
  - C007 – Define audit requirements.
  - C008 – Perform auditing.
  - C009 – Identify and protect audit information.
  - C010 – Review and manage audit logs.
- Configuration Management (CM)
  - C013 – Establish configuration baselines.
  - C014 – Perform configuration and change management.
- Identification and Authentication (IA)
  - C015 – Grant access to authenticated entities.
- Incident Response (IR)
  - C016 – Plan incident response.
  - C017 – Detect and report events.
  - C018 – Develop and implement a response to a declared incident.
  - C019 – Perform post incident reviews.
  - C020 – Test incident response.
- Maintenance (MA)
  - C021 – Manage maintenance.
- Media Protection (MP)
  - C022 – Identify and mark media
  - C023 – Protect and control media.
  - C024 – Sanitize media.
  - C025 – Protect media during transport.
- Personnel Security (PS)
  - C026 – Screen personnel.
  - C027 – Protect CUI during personnel actions.
- Risk Assessment (RA)
  - C031 – Identify and evaluate risk
  - C032 – Manage risk
  - C033 – Manage supply chain risk
- System Communications Protection (SC)
  - C038 – Define security requirements for systems and communications.
  - C039 – Control communications at system boundaries.
- System Information Integrity (SI)
  - C040 – Identify and manage information system flaws.
  - C041 – Identify malicious content.
  - C042 – Perform network and system monitoring.
  - C043 – Implement advanced email protections.

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC