Certified CMMC Professional

Master the concepts and requirements of CMMC levels and practices, the CMMC ecosystem, and the CMMC assessment process and scoping.

Why should you attend?

By attending the Certified CMMC Professional training course, you will acquire knowledge about the structure of the CMMC 2.0 model including CMMC levels, domains, and practices. In addition, you will develop the ability to understand, differentiate, and explain the relationship between the CMMC and the primary reference documentation such as FAR 52.204-21, DFARS 252.204-7012, and NIST SP 800-171. You will be able to (a) identify, describe, and compare the roles and responsibilities of each member of the CMMC ecosystem, (b) identify and mitigate ethical concerns based on CMMC Code of Professional Conduct, (c) identify and analyze the CMMC model source and supplementary documents, (d) understand the implementation of CMMC practices and review of CMMC level 1 practices, (e) explain the CMMC assessment phases and the role of the Certified CMMC Professional in CMMC assessment process, and (f) understand how to define the CMMC high-level scoping.

This training course will allow you to become a valuable asset for CMMC Third-Party Assessment Organizations (C3PAOs), organizations demanding CMMC trained resources, and consultancy agencies.

The successful completion of the training course is followed by an exam. If you pass the exam, you can apply for the “Certified CMMC Professional” credential. For more information about the examination process, please refer to the **Examination** section.

Who should attend?

This training course is intended for:

- Professionals or managers involved in and concerned with the implementation of CMMC in an organization seeking CMMC certification
- Individuals interested in being part of the CMMC ecosystem as CMMC assessment team members or individuals aiming to become Certified CMMC Assessors
- Cybersecurity and technology consultants
- Federal employees
- Individuals seeking to gain knowledge about the CMMC model and its requirements
- Individuals interested in providing consultancy services for the CMMC preparation

Course agenda

Duration: 4 days

Certified CMMC Professional: Schedule of the training course

Day 1 | Introduction to CMMC stakeholders, ecosystem, references, FCI, and CUI

- Training course objectives and structure
- CMMC stakeholders and ecosystem
- DoD cybersecurity standards and regulations
- CMMC framework
- CMMC source documents
- Unclassified information categories

Day 2 | CUI protection, CMMC model, and CMMC domains

- CUI identification, marking, and safeguarding
- CUI storage, sharing, dissemination, and destruction
- CMMC model
- CMMC domains

Day 3 | CMMC levels 1 and 2

- CMMC level 1
- CMMC level 2

Day 4 | CMMC high-level scoping, CMMC assessment process, and code of professional conduct

- CMMC high-level scoping
- CMMC assessment process
- Code of professional conduct
- Closing of the training course

Learning objectives

Upon successfully completing the training course, participants will be able to:

- Comprehend the relationship between CMMC model, FAR clause 52.204-21, DFARS clause 252.204-7012, NIST SP 800-171, and other regulations and frameworks
- Explain CMMC levels, domains, and practices
- Interpret the requirements of CMMC model in the specific context of an Organization Seeking Certification (OSC)
- Support an organization in effectively planning, implementing, and attaining the required CMMC level
- Interpret the roles and responsibilities across the CMMC ecosystem and the CMMC Code of Professional Conduct
- Explain the CMMC assessment process and CMMC high-level scoping

Examination

Duration: 3 hours

The “Certified CMMC Professional” exam fully meets the requirements of the Cyber AB. It evaluates the participant’s knowledge of the CMMC model, its relevant supporting materials, applicable legal and regulatory requirements, and the CMMC ecosystem. The “Certified CMMC Professional” exam covers the following domains"

Domain 1 | CMMC Ecosystem

Domain 2 | CMMC-AB Code of Professional Conduct (Ethics)

Domain 3 | CMMC Governance and Sources Documents

Domain 4 | CMMC Model Construct and Implementation Evaluation

Domain 5 | CMMC Assessment Process (CAP)

Domain 6 | Scoping

PECB is an Approved Publishing Partner (APP) authorized by the Cyber AB to develop training courses based on the Cyber AB curricula and exam objectives. As such, the Certified CMMC Professional exam is developed and delivered by other organizations that are part of the Cyber AB certification process.

For additional information on CMMC-AB Exams, please visit www.cyberab.org.

Certification

The Cyber AB is authorized by the Department of Defense to serve as the sole non-governmental partner for monitoring CMMC compliance and managing CMMC training and certification. As such, for more information about the Cyber AB certification process, please visit www.cyberab.org.

The requirements for obtaining the "Certified CMMC Professional" credential are provided below.

Credential	Exam	Professional experience	CMMC project experience	Other requirements
Certified CMMC Professional	Certified CMMC Professional Exam	College degree in a cyber or information technical field or at least two years of related experience or education; or	None	Completing Certified CMMC Professional class provided by an LTP (Licensed Training Provider)
		Two or more years of equivalent experience (including military) in a cyber, information technology, or assessment field		Passing the DoD CUI Awareness Training

General information

- Participants will be provided with the training course materials containing over 450 pages of explanatory information, examples, best practices, exercises, and quizzes.
- An attendance record worth 28 CPD (Continuing Professional Development) credits will be issued to the participants who have attended the training course.