Certified CMMC Professional (CCP)

This courseware is CMMC-AB Authorized Training Materials (CATM), and may be used by CMMC-AB Licensed Training Providers to offer Certified CMMC Professional classes.

Course Specifications

Course Number:

CCP

Course Length:

5 days

Course Description

Overview:

The Cybersecurity Maturity Model Certification (CMMC), managed by the CMMC Accreditation Body (CMMC-AB), is a program through which an organization's cybersecurity program maturity is measured by their initial and ongoing compliance with applicable cybersecurity practices, as well as their integration of corresponding policies and plans into their overall business operations. By Fiscal Year 2026, all organizations providing products or services to the United States Department of Defense (DoD) must obtain at least a CMMC Level 1 certification under this program.

This course prepares students for the CMMC-AB Certified CMMC Professional (CCP) certification, which authorizes the holder to use the CMMC-AB Certified CMMC Professional logo, to participate as an Assessment Team Member under the supervision of a Certified CMMC Assessor, and to be listed in the CMMC-AB Marketplace. The CCP certification is also prerequisite for the other Certified CMMC Assessor certifications (CCA-1, CCA-3, and CCA-5).

Course Objectives:

In this course, you will learn about the CMMC Model, framework, context, and application within the DoD, as well as the expectations and requirements imposed upon organizations that do business with the DoD. It will also help students to identify threats to cybersecurity and privacy within an IoT ecosystem and implement appropriate countermeasures.

You will:

- Identify the threats to the defense supply chain and the established regulations and standards for managing the risk.
- Identify the sensitive information that needs to be protected within the defense supply chain and how to manage it.
- Describe how the CMMC Model ensures compliance with federal acquisitions regulations.
- Identify responsibilities of the Certified CMMC Professional, including appropriate ethical behavior.
- Establish the Certification and Assessment scope boundaries for evaluating the systems that protect regulated information.
- Evaluate OSC readiness and determine the Objective Evidence you intend to present to the assessor.
- Use the CMMC Assessment Guides to assess Objective Evidence for processes and practices.
- Implement and evaluate practices required to meet CMMC Level 1.
- Identify processes and practices required to meet CMMC Levels 2 and 3.
- Identify processes and practices required to meet CMMC Levels 4 and 5.
- As a CCP, work through the logistics of a CMMC Assessment.

Target Student:

This course is a prerequisite for the Certified CMMC Professional program, and it prepares students for the Certified CMMC Professional (CCP) certification exam. Students might consider taking this course to learn how to perform CMMC certification readiness checks within their own organization or as a consultant to other Organizations Seeking Certification (OSC). The CCP certification is also a step toward becoming a Certified CMMC Assessor (CCA), so students might take this course to begin down the path toward CCA certification.

Prerequisites:

To ensure your success in this course, you should have some foundational education or experience in cybersecurity. The CMMC-AB has established prerequisites for those who wish to apply for CCP certification, such as:

- College degree in a cyber or information technical field with 2+ years of experience; or
- 2+ years of equivalent experience (including military) in a cyber, information technology, or assessment field.

This is an unofficial summary provided for your convenience. Always refer to the CMMC-AB website (**https://www.cmmcab.org**) for official requirements and be aware that CMMC requirements are subject to change.

Course-specific Technical Requirements

Hardware:

For this course, you will need one computer for each student and one for the instructor. Each computer will need the following minimum hardware configurations:

- 1 gigahertz (GHz) 64-bit (x64) processor.
- 4 gigabytes (GB) of Random Access Memory (RAM).
- 32 GB available storage space.
- Monitor capable of a screen resolution of at least 1,024 × 768 pixels, at least a 256-color display, and a video adapter with at least 4 MB of memory.
- Bootable DVD-ROM or USB drive.
- Keyboard and mouse or a compatible pointing device.
- Fast Ethernet (100 Mb/s) adapter or faster and cabling to connect to the classroom network.
- IP addresses that do not conflict with other portions of your network.
- Internet access (contact your local network administrator).
- (Instructor computer only) A display system to project the instructor's computer screen.

Software:

- Microsoft® 365® license (which provides the Microsoft Office apps)
- Microsoft® Windows® 10 Professional
- If necessary, software for viewing the course slides. (Instructor machine only.)

Course Content

Lesson 1: Managing Risk within the Defense Supply Chain

Topic A: Identify Threats to the Defense Supply Chain

Topic B: Identify Regulatory Responses against Threats

Lesson 2: Handling Sensitive Information

Topic A: Identify Sensitive Information

Topic B: Manage the Sensitive Information

Lesson 3: Ensuring Compliance through CMMC

Topic A: Identify Limitations of Self-Certification

Topic B: Identify the Benefits of CMMC

Topic C: Describe the CMMC Model Architecture

Lesson 4: Performing CCP Responsibilities

Topic A: Identify Responsibilities of the CCP

Topic B: Demonstrate Appropriate Ethics and Behavior

Lesson 5: Scoping Certification and Assessment Boundaries

Topic A: Get Oriented to the OSC Environment

Topic B: Determine How Sensitive Information Moves
Topic C: Identify Systems in Scope
Topic D: Limit Scope

Lesson 6: Initiating the Assessment Process

Topic A: Evaluate Readiness
Topic B: Determine Objective Evidence

Lesson 7: Assessing Objective Evidence

Topic A: Assess the Practices Using the CMMC Assessment Guides
Topic B: Assess the Processes Using the CMMC Assessment Guide Level 3

Lesson 8: Implementing and Evaluating Level 1

Topic A: Identify CMMC Level 1 Domains and Practices
Topic B: Perform a CMMC Level 1 Gap Analysis
Topic C: Perform a CMMC Level 1 Evidence Validation

Lesson 9: Identifying Levels 2 & 3

Topic A: Identify Process Requirements for CMMC Levels 2 & 3
Topic B: Identify CMMC Level 2 Practices
Topic C: Identify CMMC Level 3 Practices

Lesson 10: Identifying Levels 4 & 5

Topic A: Identify CMMC Level 4 Processes and Practices
Topic B: Identify CMMC Level 5 Processes and Practices

Lesson 11: Working through an Assessment

Topic A: Define the Assessment Logistics
Topic B: Define the Remediation Process

Appendix A: Additional Documentation for CCPs

Appendix B: Mapping Course Content to the CCP Exam