CERTIFIED CMMC PROFESSIONAL CCP

Overview

The Cybersecurity Maturity Model Certification (CMMC), managed by The Cyber AB (formerly known as the CMMC Accreditation Body or the 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. Once rule-making has concluded and CMMC 2.0 has been implemented, all organizations providing products or services to the United States Department of Defense (DoD) must comply with the requirements of their applicable CMMC Level.

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

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.
- Prepare the OSC for an Assessment by evaluating readiness.
- Use the CMMC Assessment Guides to determine and assess the Evidence for practices.
- Implement and evaluate practices required to meet CMMC Level 1.
- Identify the practices required to meet CMMC Level 2.
- As a CCP, work through the CMMC Assessment process.

PREREQUISITES

To ensure your success in this course, you should have some foundational education or experience in cybersecurity. The Cyber 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.

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 required step toward becoming a Certified CMMC Assessor (CCA), so students might take this course to begin down the path toward CCA certification.

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: Describe the CMMC Model Architecture
Topic B: Define the CMMC Program and Its Ecosystem
Topic C: Define Self-Assessments

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: Use the CMMC Assessment Scope Documentation
Topic B: Get Oriented to the OSC Environment
Topic C: Determine How Sensitive Information Moves
Topic D: Identify Systems in Scope
Topic E: Limit Scope

Lesson 6: Preparing the OSC
Topic A: Foster a Mature Cybersecurity Culture
Topic B: Evaluate Readiness

Lesson 7: Determining and Assessing Evidence
Topic A: Determine Evidence
Topic B: Assess the Practices Using the CMMC Assessment Guides

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: Assess CMMC Level 1 Practices

Lesson 9: Identifying Level 2 Practices
Topic A: Identify CMMC Level 2 Practices

Lesson 10: Working through an Assessment
Topic A: Identify Assessment Roles and Responsibilities
Topic B: Plan and Prepare the Assessment
Topic C: Conduct the Assessment
Topic D: Report the Assessment Results
Topic E: Conduct the CMMC POA&M Close-Out Assessment

- Appendix A: Evidence Collection Approach for CMMC Level 1 Practices
- Appendix B: Additional Documentation for CCPs
- Appendix C: Mapping Course Content to the CCP Exam