Course Outline

ProTech Professional Technical Services, Inc.

CMMC Certified CMMC Professional (CCP) 2.0

Course Summary

Description

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 its 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 a prerequisite for the Certified CMMC Assessor (CCA) certification.

Objectives

At the end of this course, students will be able to:

- 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 acquisition 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.

Topics

- Managing Risk within the Defense Supply Chain
- Handling Sensitive Information
- Ensuring Compliance through CMMC
- Performing CCP Responsibilities
- Scoping Certification and Assessment Boundaries
- Preparing the OSC
- Determining and Assessing Evidence
- Implementing and Evaluating Level 1
- Identifying Level 2 Practices
- Working through an Assessment

Course Summary (cont'd)

Audience

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.

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

Duration

Five days

Course Outline

CMMC Certified CMMC Professional (CCP) 2.0

Course Outline

I. *Managing Risk within the Defense Supply Chain*
   A. Identify Threats to the Defense Supply Chain
   B. Identify Regulatory Responses against Threats

II. *Handling Sensitive Information*
   A. Identify Sensitive Information
   B. Manage the Sensitive Information

III. *Ensuring Compliance through CMMC*
   A. Describe the CMMC Model Architecture
   B. Define the CMMC Program and Its Ecosystem
   C. Define Self-Assessments

IV. *Performing CCP Responsibilities*
   A. Identify Responsibilities of the CCP
   B. Demonstrate Appropriate Ethics and Behavior

V. *Scoping Certification and Assessment Boundaries*
   A. Use the CMMC Assessment Scope Documentation
   B. Get Oriented to the OSC Environment
   C. Determine How Sensitive Information Moves
   D. Identify Systems in Scope
   E. Limit Scope

VI. *Preparing the OSC*
   A. Foster a Mature Cybersecurity Culture
   B. Evaluate Readiness

VII. *Determining and Assessing Evidence*
   A. Determine Evidence
   B. Assess the Practices Using the CMMC Assessment Guides

VIII. *Implementing and Evaluating Level 1*
   A. Identify CMMC Level 1 Domains and Practices
   B. Perform a CMMC Level 1 Gap Analysis
   C. Assess CMMC Level 1 Practices

IX. *Identifying Level 2 Practices*
   A. Identify CMMC Level 2 Practices

X. *Working through an Assessment*
   A. Identify Assessment Roles and Responsibilities
   B. Plan and Prepare the Assessment
   C. Conduct the Assessment
   D. Report the Assessment Results
   E. Conduct the CMMC POA&M Close-Out Assessment

XI. *Evidence Collection Approach for CMMC Level 1 Practices*

XII. *Additional Documentation for CCPs*

XIII. *Mapping Course Content to the CCP Exam*