Cybersecurity Maturity Model Certification (CMMC) Training Course

Course: **00074**
Filter: **Beginner**
Duration: **5 days**
Category:: **Cyber Security**
Price: **3500,00 €**

About Course

The CMMC certification training (Cybersecurity Maturity Model Certification), managed by Cyber AB (Accreditation Body), 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 rulemaking has concluded, and CMMC 2.0 has been implemented, all organizations providing products or services to the United States DoD (Department of Defense) must comply with their applicable CMMC Level requirements. This course prepares students for the Cyber AB CCP (Certified CMMC Professional) certification, which authorizes the holder to use the Cyber AB Certified CMMC Professional logo, participate as an Assessment Team Member under the supervision of a Lead Assessor, and be listed in the Cyber AB Marketplace. The CCP certification is also a prerequisite for the CCA (Certified CMMC Assessor) certification.

What you'll learn

- 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 the 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 (Organizations Seeking Certification) 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.

Targeted audience

- This course prepares students for the Cyber AB CCP (Certified CMMC Professional) certification

Pre-requisites

- CMMC Certification Training Prerequisites To ensure success in this course, you should have some foundational education or experience in cybersecurity. Therefore, Cyber AB has established prerequisites for those who wish to apply for CCP certification, such as:
- Favorable background checks. Additional citizenship and clearance credentials are also required to perform higher-level duties, such as participating as an ML-2 (Maturity Level-2) assessment team member.
- A college degree in a cyber or information technology field with 2+ years of experience or 3+ years of equivalent experience (including military) in a cyber, information technology, or assessment field.
- At least two years of experience in cybersecurity or another information technology field.
- Prior to registering for this class, you must have Cyber AB approval of your application.
- If you have not completed and received approval from Cyber AB you can apply for CCP here: REGISTER WITH CYBER AB You will receive a CPN number from Cyber AB, which is required for your registration to class.

- Please note that there is a $200 registration fee imposed by Cyber-AB before issuing the mandatory CPN number. Learning Tree is not involved in this step of the process.
- This is an unofficial summary provided for your convenience. Always refer to the Cyber AB website (https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles/Assessors) for official requirements, and be aware that CMMC requirements are subject to change.

Curriculum

Module 1: Managing Risk within the Defense Supply Chain

- Identify Threats to the Defense Supply Chain
- Identify Regulatory Responses against Threats

Module 2: Handling Sensitive Information

- Identify Sensitive Information
- Manage the Sensitive Information

Module 3: Ensuring Compliance through CMMC

- Describe the CMMC Model Architecture
- Define the CMMC Program and Its Ecosystem
- Define Self-Assessments

Module 4: Performing CCP Responsibilities

- Identify Responsibilities of the CCP
- Demonstrate Appropriate Ethics and Behavior

Module 5: Scoping Certification and Assessment Boundaries

- Use the CMMC Assessment Scope Documentation
- Get Oriented to the OSC Environment
- Determine How Sensitive Information Moves

- Identify Systems in Scope
- Limit Scope

Module 6: Preparing the OSC

- Foster a Mature Cybersecurity Culture
- Evaluate Readiness

Module 7: Determining and Assessing Evidence

- Determine Evidence
- Assess the Practices Using the CMMC Assessment Guides

Module 8: Implementing and Evaluating Level 1

- Identify CMMC Level 1 Domains and Practices
- Perform a CMMC Level 1 Gap Analysis
- Assess CMMC Level 1 Practices

Module 9: Identifying Level 2 Practices

- Identify CMMC Level 2 Practices

Module 10: Working through an Assessment

- Identify Assessment Roles and Responsibilities
- Plan and Prepare the Assessment
- Conduct the Assessment
- Report the Assessment Results
- Conduct the CMMC POA&M (Plan Of Action And Milestones) Close-Out Assessment