

Certified CMMC Professional (CCP) Training

COURSE CONTENT

GET IN TOUCH



Multisoft Systems
B - 125, Sector - 2, Noida



(+91) 9810-306-956



info@multisoftsystems.com



www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

The Certified CMMC Professional (CCP) training offered by Multisoft Systems is meticulously designed for IT professionals seeking to deepen their knowledge in cybersecurity compliance, particularly in securing Department of Defense (DoD) contracts. This course equips participants with the expertise necessary to understand and implement the requirements of the Cybersecurity Maturity Model Certification (CMMC).

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 Close-Out Assessment