



CMMC
**Certified
Professional**



CMMC Certified Professional


CMMC Certified Professional training course enables participants to acquire a comprehensive understanding of the Cybersecurity Maturity Model Certification (CMMC) model and its requirements. It is also a gateway for assessors and instructors, as it is a prerequisite to Certified Assessor Level 1, Certified Assessor Level 3, and Certified Instructor certifications.

Duration
4 DAYS



Why should you attend?

By attending the CMMC Certified Professional training course, you will acquire knowledge about the structure of the CMMC model including CMMC levels, domains, capabilities, processes, and practices. In addition, you will develop the ability to understand, differentiate, and explain the relationship between the CMMC and the primary reference documentation such as FAR 52.204-21, DFARS 252.204-7012, DFARS 252.204-7019-7021, NIST SP 800-171, NIST 800-172, NIST 800-53, CUI Definitions and Guidelines from NARA and DOD, and CERT RMM.



You will also be able to (a) identify, describe, and compare the roles and responsibilities of each member of the CMMC-AB ecosystem, (b) know what are the CMMC assessment methodology phases, (c) identify and mitigate ethical concerns based on CMMC-AB Code of Professional Conduct, and (d) define and determine the roles and responsibilities for Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

This training course will allow you to become a valuable asset for consultancy agencies, CMMC Third-Party Assessor Organizations (C3PAO), and organizations demanding CMMC trained resources.

The successful completion of the training course is followed by an exam. If you pass the exam, you can apply for a "CMMC Certified Professional" credential.

Who **should** attend?

Individuals interested in being part of the CMMC-AB ecosystem such as Certified Assessors and Certified Instructors.

01

Individuals seeking to gain knowledge about the CMMC model and its requirements.

02

Individuals interested in providing consultancy services for the CMMC preparation.

03

Individuals working for suppliers of the Department of Defense (DoD) and Defense Industrial Base (DIB) and for other organizations seeking CMMC certification.

04

Cybersecurity and technology consultants and CMMC assessment team members.

05

Learning objectives

01

Gain a comprehensive understanding of the CMMC domains, capabilities, levels, processes, and practices of the CMMC model.

Acknowledge the correlation between CMMC model, FAR clause 52.204-21, DFARS clause 252.204-7012, NIST SP 800-171, and other standards and frameworks.

02

03

Acquire the ability to interpret the requirements of the CMMC model in the specific context of an Organization Seeking Certification (OSC).

Obtain the necessary knowledge to support an organization in effectively implementing and managing the requirements of the CMMC model for the required CMMC level.

04

05

Acquire knowledge on the CMMC assessment methodology and process across all CMMC levels.

Educational **approach**

1

Contains lecture sessions illustrated with graphics, examples, and discussions.

2

Encourages interaction between participants by means of questions, suggestions, exercises based on a case study, quizzes, etc.

3

Includes quizzes which are a simulation of the questions of the certification exam.

| Prerequisites

There is no specific prerequisite for participating in this training course, however, it is recommended to have a general knowledge of cybersecurity and information technology concepts and principles.

Course is including the Official Materials and Exam Voucher.

GET IN TOUCH

www.iExperts.co

info@iExperts.co

Follow @iExperts10 on :

