

Summary

The CMMC Certified Professional (CCP) credential will verify a candidate's knowledge of the Cybersecurity Maturity Model Certification (CMMC), relevant supporting materials, and applicable legal and regulatory requirements to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The CCP exam will assess the candidate's understanding of the CMMC ecosystem. A passing score on the exam is a prerequisite to CMMC Certified Assessor (CCA) and CMMC Certified Instructor certifications.

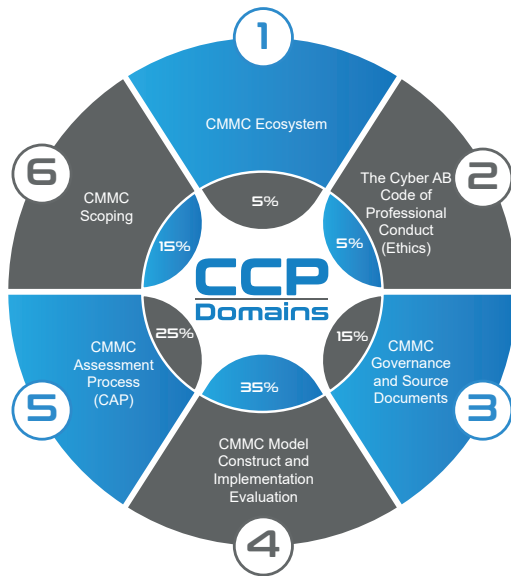
Why ecfirst for CCP Training?

- ◆ Our auditors are our trainers!
- ◆ ecfirst is all in for CMMC (RPO, APP, ATP & C3PAO).
- ◆ ecfirst's Academy Portal gives students access to all training materials, resource documents, study guides, and quizzes to solidify learning in one location.
- ◆ 25 years of privacy and security compliance training experience.
- ◆ 24 years of compliance audit/assessment experience (HIPAA, PCI DSS, HITRUST, GDPR, NIST SP 800-171, multiple state regulations).
- ◆ One of the first organizations to take the training to market!

Exam Prerequisites

- ◆ College degree in a cyber or information technical field or 2+ years of related experience or education; or 2+ years of equivalent experience (including military) in a cyber, information technology, or assessment field.
- ◆ Suggested CompTIA A+ or equivalent knowledge/experience.
- ◆ Complete CMMC Certified Professional class offered by an Approved Training Provider (ATP).
- ◆ Pass DoD CUI Awareness Training no earlier than three (3) months prior to the exam.
 - ◇ <https://securityawareness.usalearning.gov/cui/index.html>

CMMC Certified Professional (CCP)



CCP Exam Specifications

- ◆ Number of Questions: 170
- ◆ Types of Questions: Multiple Choice
- ◆ Length: 4 Hours
- ◆ Passing Score: 500 Points
- ◆ This is not an open book exam

Domain Exam Weight

#	Domain	Exam Weight	CCP Program	36 Hours
1	CCP Pre Program Prep			2 Hours
2	CMMC Ecosystem Blueprint Domain 1	5%	Domain 1, 2 & 3 Tuesday, Day 1 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
3	The Cyber AB Code of Professional Conduct (Ethics) Blueprint Domain 2	5%		
4	CMMC Governance and Source Documents Blueprint Domain 3	15%		
5	CMMC Model Construct and Implementation Evaluation Blueprint Domain 4	35%	Domain 4 Wednesday, Day 2 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
6	CMMC Assessment Process (CAP) Blueprint Domain 5	25%	Domain 5 Thursday, Day 3 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
7	CMMC Scoping Blueprint Domain 6	15%	Domain 6 & Review Friday, Day 4 8:30 am - 12:30 pm	4 Hours
8	Practice Exam & Review			

Intended Audience

- ◆ Employees of Organizations Seeking Assessment (OSA) and Organizations Seeking Certification (OSC)
 - ◇ IT and Cybersecurity Professionals
 - ◇ Regulatory Compliance Officers
 - ◇ Legal and Contract Compliance Professionals
 - ◇ Management Professionals
- ◆ Cybersecurity and Technology Consultants
- ◆ Federal Employees
- ◆ CMMC Assessment Team Members

Blueprint Domain 1

CMMC Ecosystem

Task 1 Identify and compare roles/responsibilities/requirements of authorities across the CMMC ecosystem.

Blueprint Domain 2

The Cyber AB Code of Professional Conduct (Ethics)

Task 1 Identify and apply knowledge of the Guiding Principles and Practices of The Cyber AB Code of Professional Conduct (CoPC)/ISO/IEC/DoD requirements.

Blueprint Domain 3

CMMC Governance and Source Documents

- Task 1 Demonstrate understanding of FCI and CUI in non-federal unclassified networks.
- Task 2 Determine the appropriate roles/responsibilities/authority for FCI and CUI.
- Task 3 Demonstrate understanding of the CMMC Source and Supplementary documents.

Blueprint Domain 4

CMMC Model Construct and Implementation Evaluation

- Task 1 Given a scenario, apply the appropriate CMMC Source Documents as an aid to evaluate the implementation/review of CMMC requirements.
- Task 2 Apply knowledge of the CMMC Assessment Criteria and Methodology to the appropriate CMMC requirements.
- Task 3 Analyze the application of sampling values for adequate depth and coverage of evidence.

The Cyber AB Source

<https://dodcio.defense.gov/CMMC/>

Blueprint Domain 5

CMMC Assessment Process

- Task 1 Choose the appropriate roles of the CCP in the CAP when evaluating OSC preparedness for an assessment of their CMMC L2 security requirement implementations (Phase 1 - Conduct the Pre-Assessment.)
- Task 2 Apply CMMC Assessment Process requirements pertaining to the role of the CCP as an assessment team member while conducting a CMMC assessment (Phase 2 - Assess Conformity to Security Requirements.)
- Task 3 Demonstrate comprehension of the CCP role in the preparation of assessment report (Phase 3 - Complete and Report Assessment Results.)
- Task 4 Demonstrate comprehension of the CCP role in the process of certificate issuance and evaluating outstanding assessment issues on Plan of Action and Milestones (POA&M) (Phase 4 - Issue Certificate & Close OUT POA&M.)
- Task 5 Given a scenario, determine the appropriate phases/steps to assist in the preparation/conducting/reporting on a CMMC Level 2 Assessment.

Blueprint Domain 6

CMMC Scoping

- Task 1 Understand CMMC High-Level Scoping as described in the CMMC Assessment Process.
- Task 2 Given a Scenario, analyze the organization environment to generate an appropriate scope for CUI assets, based on 32 CFR § 170.19 CMMC Scoping.

OSC Organizations Seeking CMMC Certification

CMMC Cybersecurity Maturity Model Certification

CoPC Code of Professional Conduct

ATP Approved Training Provider

CCP CMMC Certified Professional

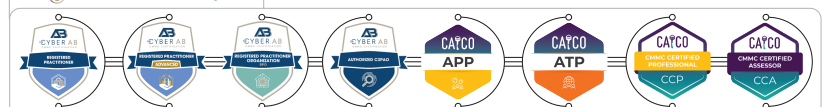
CAP CMMC Assessment Process

POA&M Plan of Action and Milestones



Peter Harvey Peter.Harvey@ecfirst.com www.ecfirst.com

The ecfirst DoD CMMC Ecosystem



Achieve CMMC Certification