# CMMC CCP
Public | Virtual | On-Site

ecfirst

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!
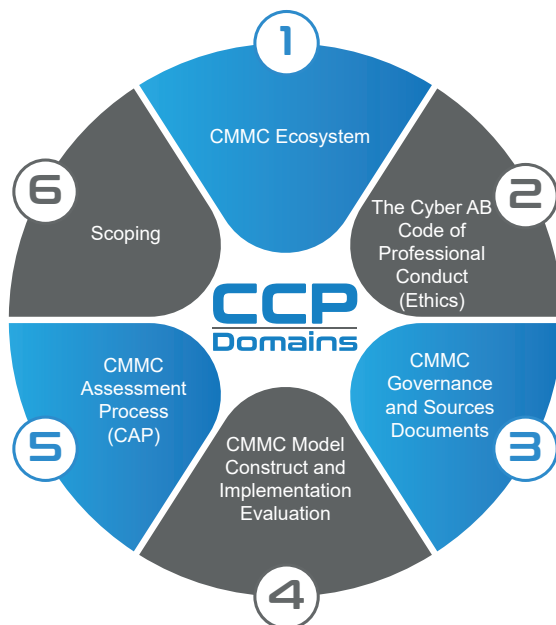
Exam Prerequisites

- 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 CCP Class offered by a Approved Training Provider (ATP).
- Pass DoD CUI Awareness Training no earlier than three (3) months prior to the exam.
  - A https://securityhub.usalearning.gov/index.html

CMMC Certified Professional (CCP)

1. CMMC Ecosystem
2. The Cyber AB Code of Professional Conduct (Ethics)
3. CMMC Governance and Sources Documents
4. CMMC Model Construct and Implementation Evaluation
5. CMMC Assessment Process (CAP)
6. Scoping

CCP Domains

CCP Exam Specifications

- Number of Questions: 170
- Types of Questions: Multiple Choice
- Length: 3.5 Hours
- Passing Score: 500 points
- This is not an open book exam

Domain Exam Weight

#	Domain	Exam Weight	CCP Program	2025 35.5 Hours
1	CCP Pre Program Prep			2 Hours
2	CMMC Ecosystem	5%	**Domain 1, 2 & 3** Tuesday, Day 1 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
3	Cyber-AB Code of Professional Conduct (Ethics)	5%		
4	CMMC Governance and Sources Documents	15%		
5	CMMC Model Construct and Implementation Evaluation	35%	**Domain 4** Wednesday, Day 2 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
6	CMMC Assessment Process (CAP)	25%	**Domain 5** Thursday, Day 3 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
7	Scoping	15%	**Domain 6 & Review** Friday, Day 4 8:30 am - 12:00 pm	3.5 Hours
8	Practice Exam & Review			

Intended Audience

- Employees of Organizations Seeking CMMC 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

CMMC CCP
Public | Virtual | On-Site

ecfirst

Domain 1
CMMC Ecosystem

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

Domain 2
The Cyber AB Code of Professional Conduct (Ethics)

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

Domain 3
CMMC Governance and Sources Documents

Task 1 — Demonstrate your 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 your understanding of the CMMC Source and Supplementary documents.

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 practices.

Task 2 — Apply your knowledge of the CMMC Assessment Criteria and Methodology to the appropriate CMMC practices.

Task 3 — Analyze the adequacy/sufficiency around the location/collection/quality/usage of evidence.

The Cyber AB Source
https://dodcio.defense.gov/CMMC/

Domain 5
CMMC Assessment Process

Task 1 — Choose the appropriate roles of the CCP in the CMMC Assessment Process when developing the assessment plan (Phase 1- Plan and Prepare 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 - Conduct Assessment).

Task 3 — Demonstrate your comprehension of the CCP role in the preparation of assessment report (Phase 3 - Report Assessment Results).

Task 4 — Demonstrate your comprehension of the CCP role in the process of evaluating outstanding assessment issues on Plan of Action and Milestones (POA&M) (Phase 4 - Evaluation of Outstanding Assessment POAM Items).

Task 5 — Given a scenario, determine the appropriate phases/steps to assist in the preparation/conducting/reporting on a CMMC Level 2 Assessment.

Domain 6
Scoping

Task 1 — Understand CMMC High-Level Scoping as described in the CMMC Assessment Process.

Task 2 — Given a Scenario, analyze the organization's environment to generate an appropriate scope for FCI Assets.

OSC — Organizations Seeking CMMC Certification

CMMC — Cybersecurity Maturity Model Certification

CoPC — Code of Professional Conduct

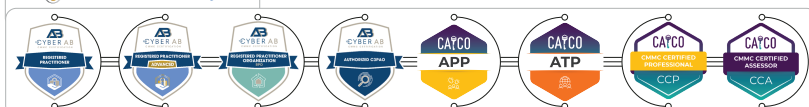**LTP** — Licensed Training Provider

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