CMMC CCP

Public | Virtual | On-Site

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.

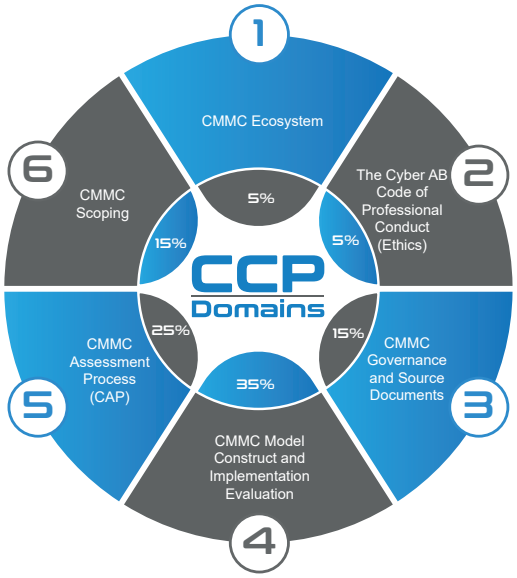
Why ecfirst for CCP Training?

- 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

CMMC CCP

Public | Virtual | On-Site

Detailed Course Description

Blueprint Domain 1 CMMC Ecosystem

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

1. Authorities
   a. Office of the Undersecretary of Defense (OUSD)
   (1) Cybersecurity standards and best practices and knowledge of how to map these controls and processes across several levels that range from basic to advanced cyber hygiene
   (2) Regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements
   b. CMMC ecosystem and the unique entities participating in CMMC assessments
   (1) The Cyber AB
      (a) Organizations and Individuals
         1. Organizations Seeking CMMC Certification (OSC)
            (1) Purpose, Requirements, and benefits of OSC involvement in the ecosystem
         2. Organizations Seeking Assessment (OSA)
            (1) Purpose, requirements, and benefits of OSA involvement in the ecosystem
         3. CMMC Third-Party Assessment Organizations (C3PAO)
            (1) Assessment Team Member
               (a) CCP and CCA roles on the Assessment Team
            (2) Lead CCA
               (a) Lead CCA role on the Assessment Team
         4. Registered Practitioner Organizations (RPO)
            (1) Requirements and Benefits of RPO
            (2) Registered Practitioner (RP)
               (a) RPs in the CMMC ecosystem provide advice, consulting, and recommendations to their clients. They are the "implementers" and consultants, but do not participate as a member of a CMMC Assessment Team.
   (1) CMMC Assessor and Instructor Certification Organization (CAICO)
      (a) Organizations
         1. Approved Partner Publishers (APP)
            (1) Purpose, requirements, and benefits of APPs
         2. Approved Training Providers (ATP)
            (1) Purpose, requirements, and benefits of ATPs
      (a) Individuals
         1. CMMC Certified Professional (CCP)
            (1) Purpose, requirements, and benefits of CCPs' active involvement in the ecosystem
         2. CMMC Certified Assessor (CCA)
            (1) Purpose, requirements, and benefits of CCAs' active involvement in the 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.

1. Guiding Principles
   a. Professionalism
   b. Impartiality
   c. Confidentiality
   d. Information integrity
   e. Lawful and ethical behavior
   f. Equal Opportunity
   g. Proper use of CMMC methods
   h. Proper Use of Technology and Artificial Intelligence
2. Conflicts of interest
3. CoPC Enforcement
4. Appeals
5. CMMC Position-Specific Professional Responsibilities

CMMC CCP

Public | Virtual | On-Site

Blueprint Domain 3 — CMMC Governance and Source Documents

Task 1 Demonstrate understanding of FCI and CUI in non-federal unclassified networks.

1. Current Department of Defense (DoD) Defense Industrial Base (DIB) Cybersecurity Efforts, Regulations, and Executive Orders pertaining to the CMMC program
   - A. Part 32 of the Code of Federal Regulations (CFR)
   - B. Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the CFR
   - C. DFARS Clause 252.204-7012
     - (1) National Institute of Standards and Technology (NIST) SP 800-171
     - (2) Technical Data (DFARS 252.227-7013)
     - (3) FedRAMP and DoD FedRAMP Equivalency Memo
2. CMMC Framework Tenets
   - A. Key aspects of CMMC program requirements
     - (1) Streamlined Model
       - (a) Focused on the most critical requirements
       - (b) Aligned with widely accepted standards
     - (2) Reliable Assessments
       - (a) Reduced assessment costs
       - (b) Higher accountability
     - (3) Flexible Implementation
       - (a) Spirit of collaboration
       - (b) Added flexibility and speed
   - B. Levels of CMMC assessments and requirements
     - (1) Level 1
       - (a) FAR Clause 52.204-21
     - (2) Level 2
       - (a) NIST SP 800-171 Rev. 2
       - (b) Self-assessment and C3PAO assessment
     - (3) Level 3
       - (a) Selected subset of requirements from NIST SP 800-172 Feb2021
       - (b) DCMA DIBCAC assessment
   - C. Self-Assessments vs. Third-Party Assessments
     - (1) Define different criteria for various assessment types under CMMC framework
3. Consequences of non-compliance
   - a. Failure to receive an award of contract
   - b. Contractual liability
   - c. False Claims Act
     - (1) US Department of Justice
       - (a) Civil Cyber-Fraud Initiative

Task 2 Determine the appropriate roles/responsibilities/authority for FCI and CUI.

1. Importance of data classification, collection, and analysis
   - A. CUI Basic vs Specified
2. Contractor sensitive data categories
   - A. Federal Contract Information (FCI)
     - (1) Section 4.1901 of the Federal Acquisition Regulation (FAR)
   - B. Controlled Unclassified Information (CUI)
     - (1) Part 2002 of Title 32 CFR, 2002.4(h)
3. Government authority for identifying and marking CUI
   - A. Executive Order 13556
   - B. 32 Code of Federal Regulations, Part 2002 (Implementing Directive)
   - C. DoD Instruction 5200.48, Controlled Unclassified Information (CUI)
4. Contractor/Authorized holders' responsibilities in handling CUI
   - A. DoDI 5200.48
   - B. Part 2002 of Title 32 CFR

Task 3 Demonstrate understanding of the CMMC Source and Supplementary documents.

1. CMMC Source Documents
   - a. NIST SP 800-171 r2
   - b. NIST SP 800-171A Jun2018
   - c. CMMC Assessment Process (CAP)
   - d. CMMC Artifact Hashing Tool User Guide
2. CMMC Supplemental Guidance Documents
   - a. CMMC Model Overview
   - b. CMMC Assessment Guide - Level 1
   - c. CMMC Assessment Guide - Level 2
   - d. CMMC Assessment Guide - Level 3
   - e. CMMC Scoping Guide - Level 1
   - f. CMMC Scoping Guide - Level 2
   - g. CMMC Scoping Guide - Level 3
3. ISOO CUI Registry
   - a. NARA administers the CUI Registry
     - (1) Types of labeled information on documents such as:
       - (a) Export Controlled (SP-EXPT)
       - (b) Specified marking/labeling using NARA CUI Marking Handbook
4. DoD CUI Registry
   - a. Types of labeled information on documents such as:
     - (1) Naval Nuclear Propulsion Information (NNPI)
     - (2) NNPI marking/labeling using DoD DOPSR20-S-2093, "Controlled Unclassified Markings: September 3, 2020"

CMMC CCP

Public | Virtual | On-Site

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 practices.

(A CCP candidate can be evaluated on ALL CMMC requirements during the CCP exam.)

1. Model Architecture
2. Model Levels
   - a. Characteristics
   - b. CMMC Status required for specific contracts
     - (1) Level 1 (Self)
     - (2) Level 2 (Self)
     - (3) Level 2 (C3PAO)
     - (4) Level 3 (DIBCAC)
3. Requirements
   - a. Requirement Descriptions
     - (1) Requirement Numbering Scheme
     - (2) Objectives
     - (3) Assessment Methods and Objects
4. Domains
   - a. Access Control (AC)
   - b. Audit & Accountability (AU)
   - c. Awareness & Training (AT)
   - d. Configuration Management (CM)
   - e. Identification & Authentication (IA)
   - f. Incident Response (IR)
   - g. Maintenance (MA)
   - h. Media Protection (MP)
   - i. Personnel Security (PS)
   - j. Physical Protection (PE)
   - k. Risk Assessment (RA)
   - l. Security Assessment (CA)
   - m. System & Communications Protection (SC)
   - n. System & Information Integrity (SI)

Task 2 Apply knowledge of the CMMC Assessment Criteria and Methodology to the appropriate CMMC requirements.

1. The definition of each requirement
2. The Assessment Objectives
3. The Assessment Methods (Examine, Interview, and Test) to use for the requirements
4. What information to look for in requirement discussion
5. The Key References and their applicability to the requirements
   - a. Navigating and using the NIST SP 800-171A content
   - b. Determining the assessment method(s) that would be best for gathering sufficient and accurate evidence

Task 3 Analyze the application of sampling values for adequate depth and coverage of evidence.

1. The level of detail and rigor to implement the security requirement
2. Indicate the scope and comprehensiveness of the security requirement

CMMC CCP

Public | Virtual | On-Site

Blueprint Domain 5 CMMC Assessment Process

Task 1 Choose the appropriate roles of the CCP in the CMMC Assessment Process when evaluating OSC preparedness for an assessment of their CMMC L2 security requirement implementations (Phase 1 – Conduct the Pre-Assessment.)

1. Confirm Availability of Evidence
2. Determine Readiness for Assessment
3. Quality Assurance of the Pre-Assessment Form

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.)

1. How to assist/support the Assessment Team during an assessment
2. The three possible assessment methods (Examine, Interview, and Test) and scoring evidence successfully for each requirement
   a. Enduring Exceptions and Temporary Deficiencies
3. Communication skills to interview or observe tests/demonstrations for assessment practices
4. How Assessment Team Members rate security requirements
5. How Assessment Team Members assist in the preparation of the assessment results report
6. How to score requirements that are on a Plan of Action and Milestone (POA&M)

Task 3 Demonstrate comprehension of the CCP role in the preparation of assessment report (Phase 3 – Complete and Report Assessment Results.)

1. The evidence presented for each requirement
2. How Assessment Team Members score requirements, validate, and deliver assessment results
3. How the Lead CCA drafts and scores the final security requirement findings
4. How the final findings and associated information are incorporated into the Assessment Report
5. How the Lead CCA submits the assessment report, including the quality assurance review process, submitting to the C3PAO and the OSC
6. How to package and archive the assessment results for a record to support any future questions that maybe asked

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.)

1. The evaluation of assessment POA&M items
   a. CMMC Scoring Methodology, POA&M requirements
      (1) Minimum assessment score
      (2) Qualifying POA&M items
      (3) POA&M duration
   b. CMMC CA.L2-3.12.2, Operational Plan of Action objectives and requirements

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

1. Plan and Prepare Assessments
   a. CMMC CCP must be able to assist in analyzing requirements
   b. CMMC CCP must be able to assist in developing pre-assessment report
   c. CMMC CCP must be able to assist in verifying readiness to conduct assessments
2. Conduct Assessment
   a. CMMC CCP must be able to assist in collecting and examining Evidence
   b. CMMC CCP must be able to assist in scoring requirements and validating preliminary results
   c. CMMC CCP must be able to assist in generating final assessment results
3. Report Recommended Assessment Results
   a. CMMC CCP must be able to assist in delivering recommended assessment results
4. Remediate Outstanding Assessment Issues
   a. Awareness of the CCP's Role in the POA&M Process

CMMC CCP

Public | Virtual | On-Site

ecfirst

CAICO CMMC CERTIFIED PROFESSIONAL CCP

Blueprint Domain 6 CMMC Scoping

Task 1 Understand CMMC Scoping as described in the 32 CFR § 170.19 CMMC Scoping.

1. Defining CMMC scoping requirements
   a. FCI Assets
   b. CUI Assets

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.

1. Defining CMMC Level 2 Asset categories
   a. CUI Assets that process, store, or transmit CUI data
   b. Security Protection Assets
   c. Contractor Risk Managed Assets
   d. Specialized Assets
   e. Out-of-Scope Assets
2. Scoping requirements
   a. People
   b. Technology
   c. Facilities
   d. External Service Providers (ESP)

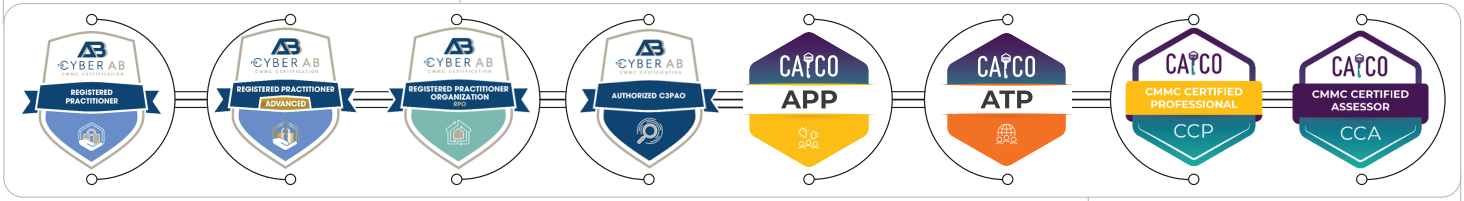
FCI	Federal Contract Information
CUI	Controlled Unclassified Information
OSC	Organizations Seeking CMMC Certification
CMMC	Cybersecurity Maturity Model Certification
CoPC	Code of Professional Conduct
ATP	Approved Training Provider
CCP	CMMC Certified Professional
CAP	CMMC Assessment Process
POA&M	Plan of Action and Milestones

The Cyber AB Source

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

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

The ecfirst DoD CMMC Ecosystem



Achieve CMMC Certification