

Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB)

Certified CMMC Professional (CCP) Test Blueprint

SUMMARY:

This exam 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 exam will also assess the candidate's understanding of the CMMC ecosystem. A passing score on this exam is a prerequisite to Certified CMMC Assessor and Certified CMMC Instructor certifications. The Department of Defense (DOD) is the authoritative source for CMMC documentation, which can be found here:
<https://www.acq.osd.mil/cmmc/documentation.html>.

Intended Audience

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

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; and
- Suggested CompTIA A+ or equivalent knowledge/experience; and
- Complete Certified CMMC Professional Class offered by a Licensed Training Provider (LTP); and
- Pass DOD CUI Awareness Training no earlier than three months prior to the exam.
 - <https://securityhub.usalearning.gov/index.html>

Exam Specifications (TBD)

- Number of Questions: TBD
- Types of Questions: Multiple Choice
- Length: TBD
- Passing Score: TBD
- This is not an open book exam

DOMAINS

Upon successful completion of this exam, the candidate will be able to apply skills and knowledge to the below domains:

Domain	Exam Weight
1. CMMC Ecosystem	5%
2. CMMC-AB Code of Professional Conduct (Ethics)	5%
3. CMMC Governance and Sources Documents	15%
4. CMMC Model Construct and Implementation Evaluation	35%
5. CMMC Assessment Process (CAP)	25%
6. Scoping	15%

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 different types of entities participating in it
 - (1) Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB)
 - (a) Organizations:
 1. Organizations Seeking Certification (OSC)
 - (1) Purpose, Requirements, and benefits of OSC involvement in the ecosystem
 2. CMMC Third-Party Assessment Organizations (C3PAO)
 3. Registered Provider Organizations (RPO)
 - (1) Requirements and Benefits of RPO
 - (b) Individuals:
 1. Registered Practitioner (RP)
 - (1) RPs in the CMMC ecosystem provide advice, consulting, and recommendations to their clients. They are the “implementers” and consultants, but do not participate in Certified CMMC Assessments.
 - (2) CMMC Assessors and Instructors Certification Organization (CAICO)
 - (a) Organizations:
 1. Licensed Partner Publishers (LPP)
 - (1) Purpose, requirements, and benefits of LPPs
 2. Licensed Training Providers (LTP)
 - (1) Purpose, requirements, and benefits of LTPs
 - (b) Individuals:
 1. Provisional Assessors (PA)
 - (1) Purpose, requirements, and benefits of PAs
 - (2) Timeline for sunseting
 2. Provisional Instructors (PI)
 - (1) Purpose, requirements, and benefits of PIs
 - (2) Timeline for sunseting
 3. Certified CMMC Professional (CCP)
 - (1) Purpose, requirements, and benefits of CCPs’ active involvement in the ecosystem
 - (2) Timeline for CCP certification and assessments

4. Certified CMMC Assessor (CCA)
 - (1) Purpose, requirements, and benefits of CCAs' active involvement in the ecosystem
 - (2) Timeline for CCA certification and assessments
5. Certified CMMC Instructor (CCI)
 - (1) Purpose, requirements, and benefits of CCIs' active involvement in the ecosystem
 - (2) Timeline for CCI certification and assessments
6. Assessment Team Member
 - (1) CCP and CCA roles on the Assessment Team
7. CMMC Lead Assessor
 - (1) Lead Assessor role on the Assessment Team
 - (2) Timeline for Lead Assessor certification

Domain 2: CMMC-AB Code of Professional Conduct (Ethics)

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

1. General ethics topics
2. CMMC-AB Code of Professional Conduct (CoPC)
3. ISO/IEC
4. Department of Defense (DoD) requirements
5. Professionalism
6. Objectivity
7. Confidentiality
8. Proper use of methods
9. Information integrity
10. Conflicts of interest
11. Respect for intellectual property
12. Lawful and ethical practices
13. Contracts and non-disclosure agreements

Domain 3. CMMC Governance and Source Documents

Task 1. Demonstrate understanding of Federal Contract Information (FCI) and Controlled Unclassified Information (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 (C.F.R.)
 - B. Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the C.F.R
 - 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
2. CMMC Framework Tenets:
 - A. Key aspects of CMMC v.20 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. Rulemaking and timeline for CMMC v2.0
 - (1) Incentives, Assessments, and 9–24-month rule making
 - C. Levels of CMMC assessments and requirements
 - (1) Foundational/Level 1 (same as previous CMMC v1.0 level 1)
 - a. FAR Clause 52.204-21
 - a. Provide overview of the 17 basic safeguarding requirements and how procedures are applied within the CMMC L1/L2 practices/assessment framework
 - (2) Advanced/Level 2 (previous level 3)
 - b. NIST SP 800-171 (Requirements)
 - a. Provide overview of the 110 NIST SP 800-171 requirements and how they are applied within the CMMC Level 2 practices/assessment framework
 - D. Self-Assessments vs. Third-Party Assessments
 - (1) Define different criteria for various assessment type under CMMC v2.0 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 Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

1. Importance of data classification, collection, and analysis
 - A. CUI Basic versus 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. CMMC Model Overview
 - B. CMMC Level 1 Assessment Guide
 - C. CMMC Level 2 Assessment Guide
 - D. CMMC Level 1 Scoping Guidance
 - E. CMMC Level 2 Scoping Guidance
 - F. CMMC Assessment Process (CAP)
 - G. CMMC Glossary
 - H. CMMC Artifact Hashing Tool User Guide
2. 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
3. DoD CUI Registry
 - A. Types of labeled information on documents such as:
 - (1) Naval Nuclear Propulsion Information (NNPI)
 - (2) NNPI marking/labeling using DoD CUI Marking Aid

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.

(At a minimum CCP candidate must be evaluated on CMMC L1 Practices during CCP exam)

1. Model Architecture
2. Model Levels:
 - A. Cumulative Nature
 - B. Characteristics
 - C. Levels required for specific contracts
 - (1) Level 1
 - (2) Level 2
3. Practices:
 - A. Practices Descriptions
 - (1) Practice Numbering Scheme
 - (2) Objectives
 - (3) Assessment Methods and Objects
4. Domains:
 - A. Access Control (AC)
 - (1) AC.L1-3.1.1 – Authorized Access Control
 - (2) AC.L1-3.1.2 – Transaction & Function Control
 - (3) AC.L1-3.1.20 – External Connections
 - (4) AC.L1-3.1.22 – Control Public Information
 - B. Audit & Accountability (AU)
 - C. Awareness & Training (AT)
 - D. Configuration Management (CM)
 - E. Identification & Authentication (IA)
 - (1) IA.L1-3.5.1 – Identification
 - (2) IA.L1-3.5.2 – Authentication
 - F. Incident Response (IR)
 - G. Maintenance (MA)
 - H. Media Protection (MP)
 - (1) MP.L1-3.8.3 – Media Disposal
 - I. Personnel Security (PS)
 - J. Physical Protection (PE)
 - (1) PE.L1-3.10.1 – Limit Physical Access
 - (2) PE.L1-3.10.3 – Escort Visitors
 - (3) PE.L1-3.10.4 – Physical Access Logs
 - (4) PE.L1-3.10.5 – Manage Physical Access
 - K. Risk Assessment (RA)
 - L. Security Assessment (CA)
 - M. System & Communications Protection (SC)
 - (1) SC.L1-3.13.1 – Boundary Protection
 - (2) SC.L1-3.13.5 – Public-Access System Separation

N. System & Information Integrity (SI)

- (1) SI.L1-3.14.1 – Flaw Remediation
- (2) SI.L1-3.14.2 – Malicious Code Protection
- (3) SI.L1-3.14.4 – Update Malicious Code Protection
- (4) SI.L1-3.14.5 – System & File Scanning

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

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

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

1. Appraised Evidence is adequate
2. Measure if the Evidence is sufficient

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).

1. Validation criteria of OSC’s assessment evidence
2. Analyzing the CMMC practice requirements
3. What needs to be included in a CMMC Assessment Plan
4. The CMMC Readiness Review Process

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).

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 practice
3. Communication skills to interview or observe tests/demonstrations for assessment practices
4. How Assessment Team Members rate practices and validate preliminary results
5. How Assessment Team Members assist in the preparation of final findings
6. How to score practices 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 – Report Assessment Results).

1. The evidence presented for each practice
2. How Assessment Team Members score practices, validate, and deliver assessment preliminary results
3. How the Assessment Lead drafts and scores the final findings
4. How the final findings and associated information are incorporated into the Assessment Report
5. How the Lead Assessor submits the assessment report, including the 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 evaluating outstanding assessment issues on Plan of Action and Milestones (POA&M) (Phase 4 – Evaluation of Outstanding Assessment POA&M Items).

1. The evaluation of assessment POA&M items
 - A. DoD Assessment Methodology, POA&M scoring criteria
 - (1) Minimum assessment score
 - (2) Qualifying POA&M items
 - B. CMMC AG CA.L2-3.12.2, 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 assessment plan.
 - C. CMMC CCP must be able to assist in verifying readiness to conduct assessment.
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 practices 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

Domain 6: Scoping

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

1. Defining organizational scoping
 - A. Organization
 - B. Host Unit
 - C. Supporting Units

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

1. Defining FCI data in the form of Assets that:
 - A. Process
 - B. Store
 - C. Transmit
2. Out-of-Scope Assets
3. Specialized Assets
 - A. Government Property
 - B. Internet of Things (IoT)/ Industrial Internet of Things (IIoT)
 - C. Operational Technology (OT)
 - D. Restricted Information Systems
 - E. Test Equipment
4. Scoping Activities
 - A. People
 - B. Technology
 - C. Facilities
 - D. External Service Providers (ESP)

Revision History:

Version Number	Change criteria	Date
1	Initial document draft	6/24/21
2	Corrected KA percentages,	7/9/21
3	Final public draft	8/4/21
4	Removed skill statements, formatting update	8/11/21
5	Corrected “rule-based” to role-based” in Domain 1, Task 8; corrected Domain 7, Task 3.6; deleted “existing” Domain 2, Task 1.1; Domain 2, Task 2, item e changed “professional” to “Provider”; Added versioning history	8/20/21
6	Update Blueprint to CMMC Framework v2.0; removed outdated content based on new framework.	1/12/2022
7	Updated Blueprint based on meetings with the PMO. This is considered the final objectives blueprint for CCP.	1/21/2022
7.1	Updated by Scantron editorial	1/24/2022
7.2	Final public draft	3/14/2022
7.3	Updated Public Draft	8/10/2022