Cybersecurity Assessor and Instructor Certification Organization (CAICO)

Certified CMMC Assessor (CCA)

Exam Information and Objectives

Summary:

This exam will verify a candidate's readiness to perform as an effective Certified Assessor of Organizations Seeking Certification (OSC) at CMMC Level 2. A passing score on this exam is a prerequisite to a CMMC Lead Assessor designation. The Department of Defense (DOD) is the authoritative source for CMMC documentation, which can be found here: https://dodcio.defense.gov/CMMC/Documentation/.

Intended Audience

- Certified CMMC Professionals seeking to advance to Certified CMMC Assessor
- Certified CMMC Instructors who wish to teach the Certified CMMC Assessor course

Exam Prerequisites

- Certified CMMC Professional Credential

Exam Specifications

- Number of Questions: 150
- Types of Questions: Multiple Choice
- Length: 4 hours
- Passing Score: 500 points
- This is not an open book exam

Knowledge Areas

Upon successful completion of this exam, the student will be able to apply skills and knowledge to the below Knowledge Areas:

Knowledge Area	Exam Weight
1. Evaluating Organizations Seeking Certification (OSC) against CMMC Level 2 requirement	15%
2. CMMC Level 2 Assessment Scoping	20%
3. CMMC Assessment Process (CAP)	25%
4. Assessing CMMC Level 2 Practices	40%

Domain 1: Evaluating Organizations Seeking Certification (OSC) against CMMC Level 2 requirements

Task 1. Assess the various environmental considerations of Organizations Seeking Certification (OSCs) against CMMC L2 practices.

1. The difference between logical (virtual) and physical locations
2. The difference between professional and industrial environments
3. Single and multi-site environmental constraints and Evidence requirements
4. Cloud and hybrid environment constraints and Evidence requirements
5. On-premises environmental constraints
6. Environmental exclusions for a level 2 CMMC assessment

Domain 2: Scoping

Task 1. Analyze the CMMC Assessment Scope of Controlled Unclassified Information (CUI) Assets as they pertain to a CMMC assessment using the five categories of CUI assets as defined in the CMMC Level 2 Assessment Scoping Guide.

1. Categorization of CUI data in the form of Assets that are in scope:
   A. #1: Controlled Unclassified Information (CUI) Assets
      (1) Process, store, or transmit CUI
   B. #2: Security Protection Assets
      (1) Assets that provide security functions and capabilities to contractor's CMMC Assessment Scope
   C. #3: Contractor Risked Managed Assets
      (1) Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place
   D. #4: Specialized Assets
      (1) Assets that may/may not process, store, or transmit CUI
      (2) Assets include government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and test Equipment
   E. #5: Out-of-Scope Assets
      (1) Assets that cannot process, store, or transmit CUI

Task 2. Given a scenario, analyze the CMMC Assessment Scope based on the predetermined CUI categories within the CMMC Level 2 Assessment Scoping Guide.

1. CMMC assessment asset categories (In-scope)
   A. CUI Assets
   B. Security Protection Assets
   C. Contractor Risked Managed Assets
   D. Specialized Assets
2. CMMC assessment asset categories (Out-of-scope)
3. Separation Techniques
   A. Logical separation
      (1) Firewalls; and
      (2) Virtual Local Area Network (VLANs)
   B. Physical separation
      (1) gates;
      (2) locks;
      (3) badge access; and
      (4) guards

Task 3. Evaluate CMMC assessment scope considerations based on the CMMC Level 2 Assessment Scoping Guide.

1. FCI and CUI within the same Assessment Scope:
    A. Contractor defines FCI/CUI assets (In-scope), CMMC Assessor certifies implementation of Level 1 & 2 practices.
2. FCI and CUI NOT within the same Assessment Scope:
    A. Contractor defines Self-Assessment of FCI assets (In-scope)
    B. Contractor defines CUI assets (In-scope), CMMC Assessor certifies implementation of Level 1 & 2 practices
3. External Services Providers
    A. Evaluation of responsibility matrix
    B. Non-Duplication
    C. Agreements, Service-Level Agreements (SLAs)

Domain 3: CMMC Assessment Process (CAP) v5.X

Task 1. Given a scenario, apply the appropriate phases and steps to plan, prepare, conduct, and report on a CMMC Level 2 Assessment.

1. Phase 1—Plan and Prepare Assessments:
    a. Analyze requirements
    b. Develop assessment plan
    c. Verify readiness to conduct assessment
2. Phase 2—Conduct assessment:
    a. Collect and examine evidence
    b. Score Practices and validate preliminary results
    c. Generate final recommended assessment results
3. Phase 3—Report recommended assessment results:
    a. Deliver recommended assessment results

<u>Domain 4: CMMC Levels 2 Practices</u>

Task 1. Identify evidence verification/validation methods and objects for Practices based on the CMMC Level 2 Assessment Guide and CMMC Assessment Process (CAP) documentation.

1. Methods and objects for determining evidence
    - A. Examine
    - B. Interview
    - C. Test

2. Adequacy and sufficiency related to evidence around all below practices
    - A. Characteristics of acceptable evidence
    - B. Evidence of enabling persistent and habitual application of practices
        - (1) Policy
        - (2) Plan
        - (3) Resourcing
        - (4) Communication
        - (5) Training
    - C. Characterization of evidence
        - (1) Validate that evidence effectively meets intent of standard
        - (2) An objective and systematic examination of evidence for the purpose of providing an independent assessment of the performance of CMMC

3. CMMC Level 2 Assessment Practice objectives including potential methods, objects, and assessment considerations (by domain):
   (at a minimum the practices listed below must be evaluated for CCA candidates)
    - A. Access Control (AC)
        - (1) AC.L2-3.1.3 – Control CUI Flow
        - (2) AC.L2-3.1.4 – Separation of Duties
        - (3) AC.L2-3.1.5 – Least Privilege
        - (4) AC.L2-3.1.6 – Non-Privileged Account Use
        - (5) AC.L2-3.1.7 – Privileged Functions
        - (6) AC.L2-3.1.8 – Unsuccessful Logon Attempts
        - (7) AC.L2-3.1.9 – Privacy & Security Notices
        - (8) AC.L2-3.1.10 – Session Lock
        - (9) AC.L2-3.1.11 – Session Termination
        - (10) AC.L2-3.1.12 – Control Remote Access
        - (11) AC.L2-3.1.13 – Remote Access Confidentiality
        - (12) AC.L2-3.1.14 – Remote Access Routing
        - (13) AC.L2-3.1.15 – Privileged Remote Access
        - (14) AC.L2-3.1.16 – Wireless Access Authorization
        - (15) AC.L2-3.1.17 – Wireless Access Protection
        - (16) AC.L2-3.1.18 – Mobile Device Connection
        - (17) AC.L2-3.1.19 – Encrypt CUI on Mobile

(18) AC.L2-3.1.21 – Portable Storage Use

B. Awareness & Training (AT)

(1) AT.L2-3.2.1 – Role-Based Risk Awareness
(2) AT.L2-3.2.2 – Role-Based Training
(3) AT.L2-3.2.3 – Insider Threat Awareness

C. Audit & Accountability (AU)

(1) AU.L2-3.3.1 – System Auditing
(2) AU.L2-3.3.2 – User Accountability
(3) AU.L2-3.3.3 – Event Review
(4) AU.L2-3.3.4 – Audit Failure Alerting
(5) AU.L2-3.3.5 – Audit Correlation
(6) AU.L2-3.3.6 – Reduction & Reporting
(7) AU.L2-3.3.7 – Authoritative Time Source
(8) AU.L2-3.3.8 – Audit Protection
(9) AU.L2-3.3.9 – Audit Management

D. Configuration Management (CM)

(1) CM.L2-3.4.1 – System Baselining
(2) CM.L2-3.4.2 – Security Configuration Enforcement
(3) CM.L2-3.4.3 – System Change Management
(4) CM.L2-3.4.4 – Security Impact Analysis
(5) CM.L2-3.4.5 – Access Restrictions for Change
(6) CM.L2-3.4.6 – Least Functionality
(7) CM.L2-3.4.7 – Nonessential Functionality
(8) CM.L2-3.4.8 – Application Execution Policy
(9) CM.L2-3.4.9 – User-Installed Software

E. Identification & Authentication (IA)

(1) IA.L2-3.5.3 – Multifactor Authentication
(2) IA.L2-3.5.4 – Replay-Resistant Authentication
(3) IA.L2-3.5.5 – Identifier Reuse
(4) IA.L2-3.5.6 – Identifier Handling
(5) IA.L2-3.5.7 – Password Complexity
(6) IA.L2-3.5.8 – Password Reuse
(7) IA.L2-3.5.9 – Temporary Passwords
(8) IA.L2-3.5.10 – Cryptographically-Protected Passwords
(9) IA.L2-3.5.11 – Obscure Feedback

F. Incident Response (IR)
   (1) IR.L2-3.6.1 – Incident Handling
   (2) IR.L2-3.6.2 – Incident Reporting
   (3) IR.L2-3.6.3 – Incident Response Testing

G. Maintenance (MA)
   (1) MA.L2-3.7.1 – Perform Maintenance
   (2) MA.L2-3.7.2 – System Maintenance Control
   (3) MA.L2-3.7.3 – Equipment Sanitization
   (4) MA.L2-3.7.4 – Media Inspection
   (5) MA.L2-3.7.5 – Nonlocal Maintenance
   (6) MA.L2-3.7.6 – Maintenance Personnel

H. Media Protection (MP)
   (1) MP.L2-3.8.1 – Media Protection
   (2) MP.L2-3.8.2 – Media Access
   (3) MP.L2-3.8.4 – Media Markings
   (4) MP.L2-3.8.5 – Media Accountability
   (5) MP.L2-3.8.6 – Portable Storage Encryption
   (6) MP.L2-3.8.7 – Removeable Media
   (7) MP.L2-3.8.8 – Shared Media
   (8) MP.L2-3.8.9 – Protect Backups

I. Personnel Security (PS)
   (1) PS.L2-3.9.1 – Screen Individuals
   (2) PS.L2-3.9.2 – Personnel Actions

J. Physical Protection (PE)
   (1) PE.L2-3.10.2 – Monitor Facility
   (2) PE.L2-3.10.6 – Alternative Work Sites

K. Risk Assessment (RA)
   (1) RA.L2-3.11.1 – Risk Assessments
   (2) RA.L2-3.11.2 – Vulnerability Scan
   (3) RA.L2-3.11.3 – Vulnerability Remediation

L. Security Assessment (CA)
   (1) CA.L2-3.12.1 – Security Control Assessment
   (2) CA.L2-3.12.2 – Plan of Action
   (3) CA.L2-3.12.3 – Security Control Monitoring
   (4) CA.L2-3.12.4 – System Security Plan

M. System & Communications Protection (SC)

   (1) SC.L2-3.13.2 – Security Engineering
   (2) SC.L2-3.13.3 – Role Separation
   (3) SC.L2-3.13.4 – Shared Resource Control
   (4) SC.L2-3.13.6 – Network Communication by Exception
   (5) SC.L2-3.13.7 – Split Tunneling
   (6) SC.L2-3.13.8 – Data in Transit
   (7) SC.L2-3.13.9 – Connections Termination
   (8) SC.L2-3.13.10 – Key Management
   (9) SC.L2-3.13.11 – CUI Encryption
   (10) SC.L2-3.13.12 – Collaborative Device Control
   (11) SC.L2-3.13.13 – Mobile Code
   (12) SC.L2-3.13.14 – Voice over Internet Protocol
   (13) SC.L2-3.13.15 – Communications Authenticity
   (14) SC.L2-3.13.16 – Data at Rest

N. System & Information Integrity (SI)

   (1) SI.L2-3.14.3 – Security Alerts & Advisories
   (2) SI.L2-3.14.6 – Monitor Communications for Attacks
   (3) SI.L2-3.14.7 – Identify Unauthorized Use

Revision History:

Version Number	**Change criteria**	**Date**
1.0	Initial document draft	10/29/2021
2.0	Update Blueprint to CMMC Framework v2.0; removed outdated content based on new framework.	01/09/2022
2.7	Updated Blueprint based on meetings with the PMO. This is considered the final objectives blueprint for CCA.	01/21/2022
2.8	Updated by Scantron editorial	01/22/2022
2.9	LTP/LPP Review and update	02/15/2022
3.0	Final public draft	04/05/2022
3.1	Updated Public Draft	06/20/2022
3.2	Exam Specifications Updated	10/26/2022
3.3	Exam Specifications Updated	12/14/2022