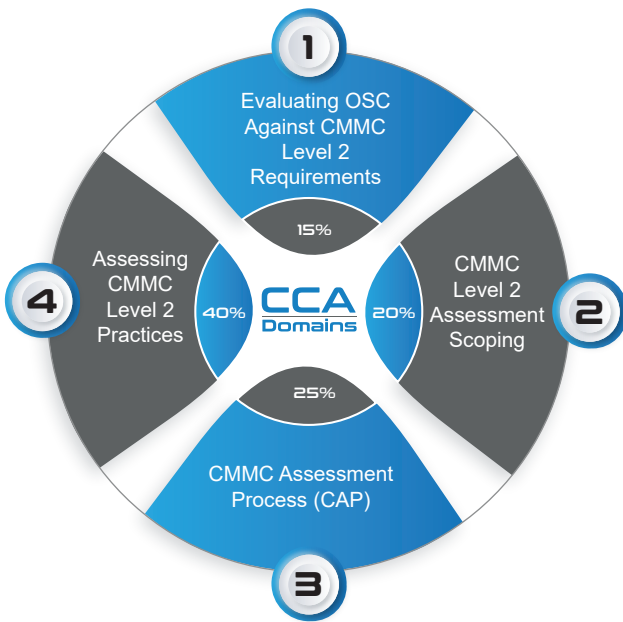


Public | Virtual | On-Site

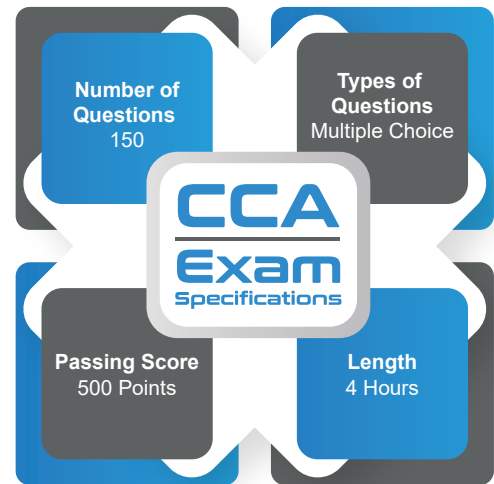
Summary

The CMMC Certified Assessor (CCA) 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 the CCA exam is a prerequisite to a CMMC Lead Assessor designation.

CMMC Certified Assessor (CCA)



CCA Exam Specifications



This is not an open book exam

Domain Exam Weight

Intended Audience

- ◆ CMMC Certified Professional (CCP) seeking to advance to CCA
- ◆ CMMC Certified Instructors who wish to teach the CCA course

Why ecfirst for CCA 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.
- ◆ 25 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!

#	Domain	Exam Weight	CCA Program	36 Hours
1	CCA Pre Program Prep			2 Hours
2	Welcome Introductions, About the Portal and Pre-Quiz		Domain 0, 1, 2 Tuesday, Day 1 8:30 am - 4:30 pm Group Exercises: 8 40 Minutes Offline Prep: 2 Hours	10 Hours
	Introduction			
3	Evaluating OSC Against CMMC Level 2 Requirements Blueprint Domain 1	15%		
4	CMMC Level 2 Assessment Scoping Blueprint Domain 2	20%		
5	CMMC Assessment Process (CAP) Blueprint Domain 3	25%	Domain 3 Wednesday, Day 2 8:30 am - 4:30 pm Group Exercises: 7 35 Minutes Offline Prep: 2 Hours	10 Hours
6	Assessing CMMC Level 2 Practices Blueprint Domain 4	40%	Domain 4 Thursday, Day 3 8:30 am - 4:30 pm Group Exercises: 10 60 Minutes Offline Prep: 2 Hours	10 Hours
7	Practice Exam & Review		Review and Final Quiz Friday, Day 4 8:30 am - 12:30 pm	4 Hours

Blueprint Domain

1

Evaluating OSC Against CMMC Level 2 Requirements

Task 1 Assess the various environmental considerations of OSCs against CMMC Level 2 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 CMMC Level 2 assessment

Blueprint Domain

2

CMMC Level 2 Assessment 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. CUI Assets
 - i. Process, store, and transmit CUI
 - b. Security Protection Assets
 - i. Assets that provide security functions and capabilities to a contractor's CMMC Assessment Scope
 - c. Contractor Risk Managed Assets
 - i. Assets that can, but are not intended to, process, store, and transmit CUI because of security policy, procedures, and practices in place
 - d. Specialized Assets
 - i. Assets that may/may not process, store, and transmit CUI
 - ii. Assets include government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and test equipment
 - e. Out-of-Scope Assets
 - i. 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 Risk Managed Assets
 - d. Specialized Assets
2. CMMC Assessment Asset Categories (Out-of-scope)
3. Separation Techniques
 - a. Logical separation
 - i. Firewalls
 - ii. Virtual Local Area Network (VLANs)
 - b. Physical separation
 - i. Gates
 - ii. Locks
 - iii. Badge Access
 - iv. 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 Service Providers
 - a. Evaluation of responsibility matrix
 - b. Non-Duplication
 - c. Agreements, Service-Level Agreements (SLAs)

Blueprint Domain 3 CMMC Assessment Process (CAP)

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

Blueprint Domain 4 CMMC Level 2 Practices

Task 1 Identify evidence verification/validation methods and objects for Practices based on the CMMC Level 2 Assessment Guide and 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
 - i. Policy
 - ii. Plan
 - iii. Resourcing
 - iv. Communication
 - v. Training
 - c. Characterization of evidence
 - i. Validate that evidence effectively meets intent of standard
 - ii. 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 an minimum the practices listed below must be evaluated for CCA candidates)
 - a. Access Control (AC)
 - i. AC.L2-3.1.3 - Control CUI Flow
 - ii. AC.L2-3.1.4 - Separation of Duties
 - iii. AC.L2-3.1.5 - Least Privilege

- iv. AC.L2-3.1.6 - Non-Privileged Account Use
- v. AC.L2-3.1.7 - Privileged Functions
- vi. AC.L2-3.1.8 - Unsuccessful Logon Attempts
- vii. AC.L2-3.1.9 - Privacy & Security Notices
- viii. AC.L2-3.1.10 - Session Lock
- ix. AC.L2-3.1.11 - Session Termination
- x. AC.L2-3.1.12 - Control Remote Access
- xi. AC.L2-3.1.13 - Remote Access Confidentiality
- xii. AC.L2-3.1.14 - Remote Access Routing
- xiii. AC.L2-3.1.15 - Privileged Remote Access
- xiv. AC.L2-3.1.16 - Wireless Access Authorization
- xv. AC.L2-3.1.17 - Wireless Access Protection
- xvi. AC.L2-3.1.18 - Mobile Device Connection
- xvii. AC.L2-3.1.19 - Encrypt CUI on Mobile
- xviii. AC.L2-3.1.21 - Portable Storage Use

b. Awareness & Training (AT)

- i. AT.L2-3.2.1 - Role-Based Risk Awareness
- ii. AT.L2-3.2.2 - Role-Based Training
- iii. AT.L2-3.2.3 - Insider Threat Awareness

c. Audit & Accountability (AU)

- i. AU.L2-3.3.1 - System Auditing
- ii. AU.L2-3.3.2 - User Accountability
- iii. AU.L2-3.3.3 - Event Review
- iv. AU.L2-3.3.4 - Audit Failure Alerting
- v. AU.L2-3.3.5 - Audit Correlation
- vi. AU.L2-3.3.6 - Reduction & Reporting
- vii. AU.L2-3.3.7 - Authoritative Time Source
- viii. AU.L2-3.3.8 - Audit Protection
- ix. AU.L2-3.3.9 - Audit Management

Blueprint Domain **4** CMMC Level 2 Practices (Cont'd...)

- d. Configuration Management (CM)
 - i. CM.L2-3.4.1 - System Baselining
 - ii. CM.L2-3.4.2 - Security Configuration Enforcement
 - iii. CM.L2-3.4.3 - System Change Management
 - iv. CM.L2-3.4.4 - Security Impact Analysis
 - v. CM.L2-3.4.5 - Access Restrictions for Change
 - vi. CM.L2-3.4.6 - Least Functionality
 - vii. CM.L2-3.4.7 - Nonessential Functionality
 - viii. CM.L2-3.4.8 - Application Execution Policy
 - ix. CM.L2-3.4.9 - User-Installed Software
- e. Identification & Authentication (IA)
 - i. IA.L2-3.5.3 - Multifactor Authentication
 - ii. IA.L2-3.5.4 - Replay-Resistant Authentication
 - iii. IA.L2-3.5.5 - Identifier Reuse
 - iv. IA.L2-3.5.6 - Identifier Handling
 - v. IA.L2-3.5.7 - Password Complexity
 - vi. IA.L2-3.5.8 - Password Reuse
 - vii. IA.L2-3.5.9 - Temporary Passwords
 - viii. IA.L2-3.5.10 - Cryptographically-Protected Passwords
 - ix. IA.L2-3.5.11 - Obscure Feedback
- f. Incident Response (IR)
 - i. IR.L2-3.6.1 - Incident Handling
 - ii. IR.L2-3.6.2 - Incident Reporting
 - iii. IR.L2-3.6.3 - Incident Response Testing
- g. Maintenance (MA)
 - i. MA.L2-3.7.1 - Perform Maintenance
 - ii. MA.L2-3.7.2 - System Maintenance Control
 - iii. MA.L2-3.7.3 - Equipment Sanitization
 - iv. MA.L2-3.7.4 - Media Inspection
 - v. MA.L2-3.7.5 - Nonlocal Maintenance
 - vi. MA.L2-3.7.6 - Maintenance Personnel
- h. Media Protection (MP)
 - i. MP.L2-3.8.1 - Media Protection
 - ii. MP.L2-3.8.2 - Media Access
 - iii. MP.L2-3.8.4 - Media Markings
 - iv. MP.L2-3.8.5 - Media Accountability
 - v. MP.L2-3.8.6 - Portable Storage Encryption
 - vi. MP.L2-3.8.7 - Removeable Media
 - vii. MP.L2-3.8.8 - Shared Media
 - viii. MP.L2-3.8.9 - Protect Backups
- i. Personnel Security (PS)
 - i. PS.L2-3.9.1 - Screen Individuals
 - ii. PS.L2-3.9.2 - Personnel Actions
- j. Physical Protection (PE)
 - i. PE.L2-3.10.2 - Monitor Facility
 - ii. PE.L2-3.10.6 - Alternative Work Sites
- k. Risk Assessment (RA)
 - i. RA.L2-3.11.1 - Risk Assessments
 - ii. RA.L2-3.11.2 - Vulnerability Scan
 - iii. RA.L2-3.11.3 - Vulnerability Remediation
- l. Security Assessment (CA)
 - i. CA.L2-3.12.1 - Security Control Assessment
 - ii. CA.L2-3.12.2 - Plan of Action
 - iii. CA.L2-3.12.3 - Security Control Monitoring
 - iv. CA.L2-3.12.4 - System Security Plan
- m. System & Communications Protection (SC)
 - i. SC.L2-3.13.2 - Security Engineering
 - ii. SC.L2-3.13.3 - Role Separation
 - iii. SC.L2-3.13.4 - Shared Resource Control
 - iv. SC.L2-3.13.6 - Network Communication by Exception
 - v. SC.L2-3.13.7 - Split Tunneling
 - vi. SC.L2-3.13.8 - Data in Transit
 - vii. SC.L2-3.13.9 - Connections Termination
 - viii. SC.L2-3.13.10 - Key Management
 - ix. SC.L2-3.13.11 - CUI Encryption
 - x. SC.L2-3.13.12 - Collaborative Device Control
 - xi. SC.L2-3.13.13 - Mobile Code
 - xii. SC.L2-3.13.14 - Voice over Internet Protocol
 - xiii. SC.L2-3.13.15 - Communications Authenticity
 - xiv. SC.L2-3.13.16 - Data at Rest
- n. System & Information Integrity (SI)
 - i. SI.L2-3.14.3 - Security Alerts & Advisories
 - ii. SI.L2-3.14.6 - Monitor Communications for Attacks
 - iii. SI.L2-3.14.7 - Identify Unauthorized Use



Peter Harvey

Peter.Harvey@ecfirst.com

www.ecfirst.com

The ecfirst DoD CMMC Ecosystem



Achieve CMMC Certification