

CMMC Solutions

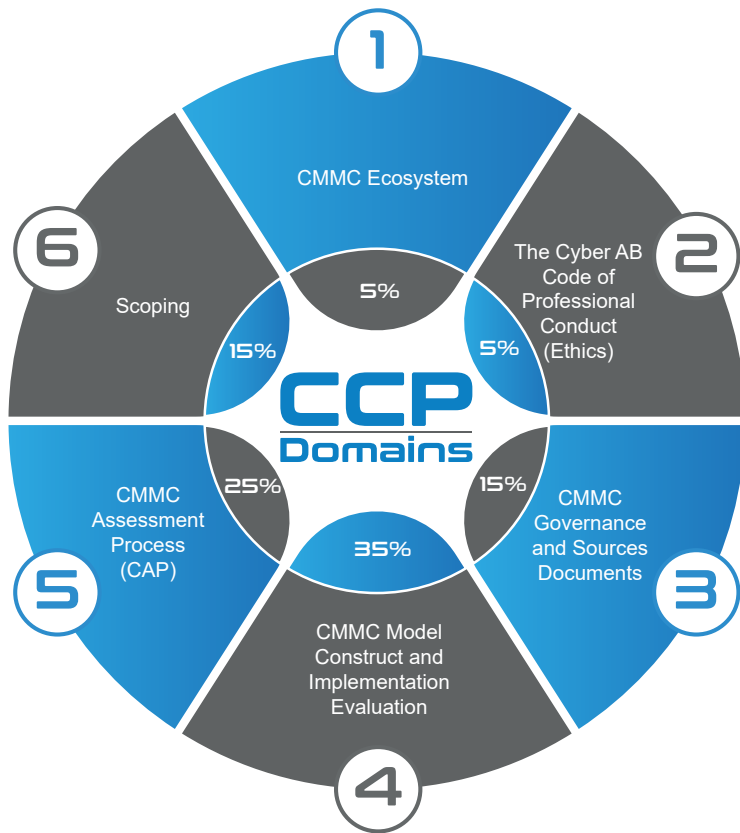


ecfirst CMMC Solutions

1	CCP Training	2
2	CCA Training	3
3	CMMC Level 1 Platform	4
4	CMMC Level 2 Platform	6
5	CMMC Playbook	8
6	CMMC Assessment Playbook	12
7	CMMC Toolkit	13

CMMC CCP

Public | Virtual | On-Site



www.ecfirst.com/CCP



“

I am happy to let you know **I passed the CMMC CCP exam** on my **first attempt**. The **CCP prep** process was **easier** than I expected - thanks to the **fantastic training class** and **study materials** from the **ecfirst CCP Academy**! I appreciated **my ecfirst** experience.

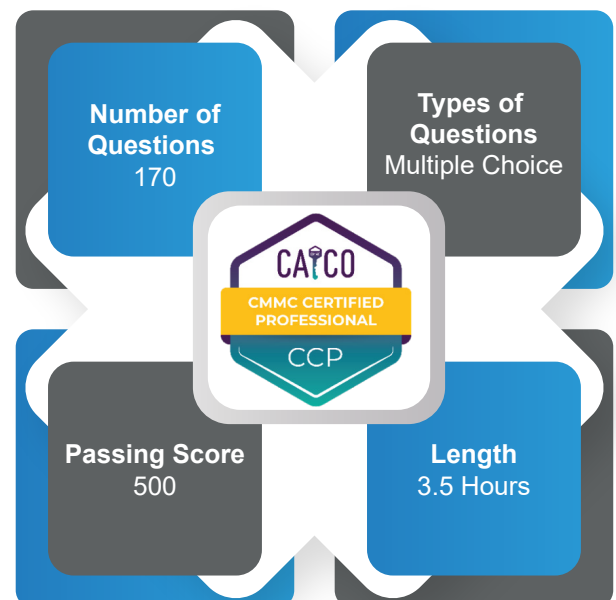
”

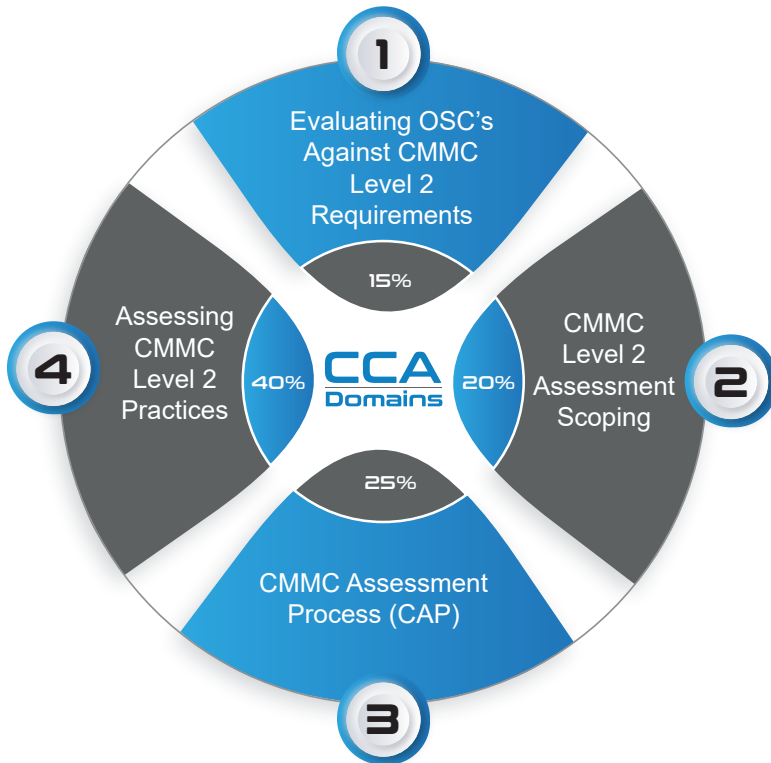
Exam Prerequisites

- 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.

<https://www.dodcui.mil/Training/DoD-Training/>

CCP Exam Specifications





“The **ecfirst CCA Program** was extensive with excellent assessment resources.

Practical, real-world CMMC assessment scenarios presented, including insight on a credible SSP.”

www.ecfirst.com/CCA



Why ecfirst?

Our auditors are our trainers!

ecfirst is all in for CMMC (RPO, APP, ATP & Authorized C3PAO).

20+ years of privacy and security compliance training experience.

20+ years of compliance audit/assessment experience (HIPAA, PCI DSS, HITRUST, GDPR, NIST SP 800-171, multiple state regulations).

ecfirst's Academy Portal gives students access to all training materials, resource documents, study guides, and quizzes to solidify learning in one location.

One of the first organizations to take the training to market!

CCA Exam Specifications

Number of Questions
150

Types of Questions
Multiple Choice

Passing Score
500+

Length
4 Hours





Home / Assessment / CMMC Level 1 Self-Assessment

Back

Phase
1
Planning

Phase
2
Self- Assessment

Phase
3
Verification

Phase
4
Generate Report

Reference

Dashboard

Policy Template



Phase 1 Planning



Home / Assessment / CMMC Level 1 Self-Assessment / Phase 1: Planning

Back

Phase
1
Planning

Phase
2
Self-Assessment

Phase
3
Verification

Phase
4
Generate Report

Reference

Dashboard

Policy Template

Self-Assessment Questionnaire

DTB

CORP

CMMC 2.0 Assessment Questionnaire

Back

Home / CMMC 2.0 Level 1 Engagement / Phase 1 Planning / CMMC 2.0 Assessment Questionnaire

AC.L1-3.1.1

AC.L1-3.1.2

AC.L1-3.1.20

AC.L1-3.1.22

IA.L1-3.5.1

IA.L1-3.5.2

MPL1-3.8.3

PE.L1-3.10.1

PE.L1-3.10.3

PE.L1-3.10.4

PE.L1-3.10.5

SC.L1-3.13.1

IA.L1-3.5.1

Identify information system users, processes acting on behalf of users, or devices.

1/3

System users are identified [a]

Are system users identified?

Policy Implementation Status

Yes

No

Not Applicable (N/A)

Policy Reference

Upload

Map Files

Procedure Implementation Status

Yes

No

Not Applicable (N/A)

Prev

1

2

3

Next

Dashboard

DTB

CORP

Home / Assessment / CMMC Level 1 Self-Assessment / Level 1 Dashboard

Back

Intake Form

100%

Assessment

75%

Roles

50%

SSP

40%

General

84%

Policy

25%

Procedure

67%

Evidence

100%

Subscribe to CMMC Level 1 Platform

© ecfirst. All Rights Reserved. 2025

Page 5

DTB

CORP

Home / Assessment / CMMC Level 2 Engagement

Back

Phase 1

Planning

Phase 2

Assessor Review of Phase 1

Phase 3

Assessment

Phase 4

Report

Phase 5

POA&M

Client Phase

ecfirst | Assessor Phase

SSP Documents

CMMC Reference

Readiness Portal

Policy Template



Phase 1

Planning

DTB

CORP

Home / Assessment / CMMC Level 2 Readiness Portal / Phase 1: Planning

Back

Intake Form

100.0%

Assessment Information

96.8%

Roles

62.5%

Assessment Questionnaire

© ecfirst. All Rights Reserved. 2025

Page 6

Assessment Questionnaire

DTB CORP

CMMC 2.0 Assessment Questionnaire

Home / CMMC 2.0 Level 2 Engagement / Phase 1 Planning / CMMC 2.0 Assessment Questionnaire

AC.L1-3.1.1

AC.L1-3.1.2

AC.L1-3.1.20

AC.L1-3.1.22

AC.L2-3.1.3

AC.L2-3.1.4

AC.L2-3.1.5

AC.L2-3.1.6

AC.L2-3.1.7

AC.L2-3.1.8

AC.L2-3.1.9

AC.L2-3.1.10

AC.L1-3.1.1

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Authorized users are identified [a]

Are authorized users identified as part of the system access control process?

Policy Implementation Status

Yes No Not Applicable (N/A)

Policy Reference

logo_tracer (2).png

Upload

Map Files

ok

Prev 1 2 3 4 5 6 Next

Assessment Documents and Templates

DTB CORP

Home / Assessment / CMMC Level 2 Readiness Portal / Organize and Prepare Assessment Documents and Templates

#	File Name	Format	Download	Upload
1	CMMC Assessment In-Brief	PowerPoint	View Download	View Upload
2	CMMC Pre-Assessment Template	Checkist	View Download	View Upload
3	CMMC Daily Checkpoint	Excel	View Download	View Upload
4	CMMC Assessment Findings Brief Template	Excel	View Download	View Upload
5	OSC Self-Assessment Practice Deficiency Tracker	PowerPoint	View Download	View Upload
6	CMMC Scoring with DoD Assessment Scoring Methodology	PowerPoint	View Download	View Upload
7	CMMC Assessment Quality Review Checklist	Excel	View Download	View Upload
8	CMMC Assessor Waiver Process	PDF	View Download	View Upload
9	High Level Scoping	PDF	View Download	View Upload

Subscribe to CMMC Level 2 Platform

CMMC Playbook



Quick Links

[Home](#)
[CMMC Final Rule](#)
[CMMC Level](#)
[CMMC Domains](#)
[Domains/Roles/Topics](#)
[CMMC Training](#)
[Source Documents](#)
[Getting Started with CMMC](#)
[DoD CJM Mandatory Training](#)
[CMMC Ecosystem](#)
[CMMC News](#)
[System Security Plan](#)

CMMC Playbook

NEW

CMMC Final Rule

DoD PR

Source

CMMC IOI Brief

SELECT CMMC Level

Level 1

Level 2

Level 3

CMMC Source Documents

Download All

CMMC Model Overview

Level 2 Scoping Guide

Level 2 Assessment Guide

CMMC Hashing Guide

CMMC Glossary

CMMC Domains

Domain 1

Access Control (AC)

Domain 2

Awareness & Training (AT)

Domain 3

Audit and Accountability (AU)

Domain 4

Configuration Management (CM)

Domain 5

Identification & Authentication (IA)

Domain 6

Incident Response (IR)

Domain 7

Maintenance (MA)

Domain 8

Media Protection (MP)

Domain 9

Personnel Security (PS)

Domain 10

Physical Protection (PP)

Domain 11

Risk Assessment (RA)

Domain 12

Security Assessment (SA)

Domain 13

System & Communications Protection (SC)

Domain 14

System & Information Integrity (SI)

Subscribe to CMMC Playbook

© ecfirst. All Rights Reserved. 2025

Page 8

CMMC


Level 1 Playbook

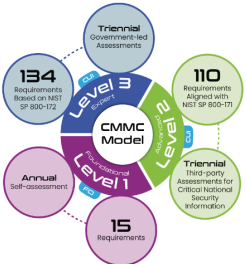


Quick Links

[Home](#)
[CMMC Final Rule](#)
[CMMC Domains](#)
[Domains/Roles/Topics](#)
[CMMC Training](#)
[Source Documents](#)
[Getting Started with CMMC](#)
[DoD CUI Mandatory Training](#)
[CMMC Ecosystem](#)
[CMMC News](#)

CMMC Level 1 Playbook





134 Requirements Based on NET SP 800-172


110 Requirements Aligned with NET SP 800-171

15 Requirements

Triennial Government-led Assessments

Triennial Third-party Assessments for Critical National Security Information

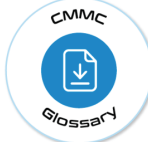




Annual Self-assessment









[DoD PR](#)[Source](#)[CMMC 101 Brief](#)

CMMC Source Documents

[Download All](#)



CMMC Domains



Explore the Playbook

[CMMC Assessment Playbook](#)

Domains

Access Control (AC)

1

Identification and Authentication (IA)

2

Media Protection (MP)

1

Physical Protection (PP)

2

System and Communications Protection (SC)

2

System and Information Integrity (SI)

2

Roles

Personnel installing, configuring, and maintaining the system

1

Personnel with access enforcement responsibilities

1

Personnel with account management responsibilities

2

Personnel with authenticator management responsibilities

1

Personnel with boundary protection responsibilities

2

Personnel with configuration management responsibilities

1

Topics

Access Authorization

2

Access Control

2

Access Enforcement

1

Account Management

1

Authenticator Management

1

Boundary Protection

1

Configuration Management

1

Subscribe to CMMC Level 1 Playbook

© ecfirst. All Rights Reserved. 2025

Page 9

CMMC

Level 2 Playbook



Quick Links

Home

CMMC Final Rule

CMMC Domains

Domains/Roles/Topics

CMMC Training

Source Documents

Getting Started with CMMC

DoD CUI Mandatory Training

CMMC Ecosystem

CMMC News

CMMC Level 2 Playbook

AI-Powered Assistant

Bailey

134 Requirements based on NIST SP 800-122

Level 3

Level 2

Level 1

110 Requirements aligned with NIST SP 800-171

Triennial Government-led Assessments

Triennial Third-party Assessments for Critical National Security Information

Annual Self-assessment

15 Requirements

CMMC Final Rule

DoD PR

Source

CMMC IOI Brief

CMMC Source Documents

Download All

CMMC Model Overview

Level 2 Scoping Guide

Level 2 Assessment Guide

CMMC Hashing Guide

CMMC Glossary

CMMC Domains

CMMC 1 Access Control (AC)

CMMC 2 Awareness & Training (AT)

CMMC 3 Audit and Accountability (AU)

CMMC 4 Configuration Management (CM)

CMMC 5 Identification & Authentication (IA)

CMMC 6 Incident Response (IR)

CMMC 7 Maintenance (MA)

CMMC 8 Media Protection (MP)

CMMC 9 Personnel Security (PS)

CMMC 10 Physical Protection (PP)

CMMC 11 Risk Assessment (RA)

CMMC 12 Security Assessment (SA)

CMMC 13 Systems & Communications Protection (SC)

CMMC 14 Systems & Information Integrity (SI)

Explore the Playbook

CMMC Assessment Playbook

Domains

Access Control (AC)

Awareness and Training (AT)

Audit and Accountability (AU)

Configuration Management (CM)

Identification and Authentication (IA)

Incident Response (IR)

Maintenance (MA)

Roles

Members of change control board or similar

Personnel (authorities) to whom incident information is to be reported

Personnel approving use of alternate work sites

Personnel using alternate work sites

Personnel assessing controls at alternate work sites

Personnel composing the general system user community

Topics

Access Authorization

Access Enforcement

Access Restrictions

Account Management

Alternate Work Site

Alternative Physical Safeguards

Application Partitioning

Subscribe to CMMC Level 2 Playbook

© ecfirst. All Rights Reserved. 2025

Page 10

CMMC

Level 3 Playbook



Quick Links

[Home](#)

[CMMC Final Rule](#)

[CMMC Domains](#)

[Domains/Roles/Topics](#)

[CMMC Training](#)

[Source Documents](#)

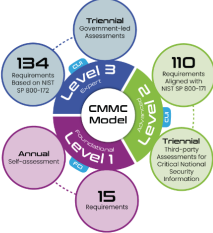

[Getting Started with CMMC](#)


[DoD CUI Mandatory Training](#)

[CMMC Ecosystem](#)

[CMMC News](#)


CMMC Level 3 Playbook





[DoD PR](#)[Source](#)[CMMC IOI Brief](#)


CMMC Source Documents


[Download All](#)

[CMMC Model Overview](#)


[Level 3 Scoping Guide](#)


[Level 3 Assessment Guide](#)

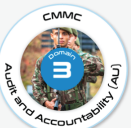
[CMMC Hashing Guide](#)


[CMMC Glossary](#)


CMMC Domains


[1 Access Control \(AC\)](#)

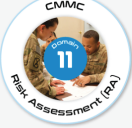
[2 Awareness & Training \(AT\)](#)


[3 Audit and Accountability \(AU\)](#)


[5 Identification & Authentication \(IA\)](#)


[6 Incident Response \(IR\)](#)

[9 Personnel Security \(PS\)](#)

[11 Risk Assessment \(RA\)](#)

[12 Security Assessment \(SA\)](#)

[13 Systems & Communications Protection \(SC\)](#)

[14 System & Information Integrity \(SI\)](#)

Explore the Playbook

[CMMC Assessment Playbook](#)

Domains

[Access Control \(AC\)](#)

[Awareness and Training \(AT\)](#)

[Configuration Management \(CM\)](#)

[Identification and Authentication \(IA\)](#)

[Incident Response \(IR\)](#)

[Personnel Security \(PS\)](#)

[Risk Assessment \(RA\)](#)

Roles

[Enterprise architects](#)

[Members of a change control board or similar roles](#)

[Organizational personnel comprising the general system user community](#)

[Organizational personnel from the incident response team](#)

[Organizational personnel responsible for access enforcement](#)

[Organizational personnel responsible for account](#)

Topics

[Access Authorization](#)

[Access Control](#)

[Advanced Persistent Threat Actors](#)

[Assets](#)

[Baseline Configuration](#)

[BIOS Protection](#)

[Boundary Protection](#)

Access Control (AC)

Organizationally Controlled Assets ACL3-3.1.2e

Definition

Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.

Secured Information Transfer ACL3-3.1.3e

Subscribe to CMMC Level 3 Playbook

© ecfirst. All Rights Reserved. 2025

Page 11

ecfirst Academy

Home Course Access My Dashboard

Quick Links

- Home
- ecfirst CAP Doctrine
- CMMC Glossary
- Assessment Phases
- Phase 1: Preparation
- Phase 2: Conduct Assessment
- Phase 3: Report Results
- Phase 4: POA&M
- CMMC Source Documents
- Assessment Templates

CMMC ASSESSMENT Playbook

ecfirst CAP Doctrine

CAP Flowchart

CAP Playbook

Assessment Phases

0 Preliminary Proceedings

1 Conduct The Pre-Assessment

2 Assess Conformity to Security Requirements

3 Complete & Report Assessment Results

4 Optional Issue Certificate & Close-Out POA&M

Phase 0 Preliminary Proceedings

Summary View Expanded View

1 Initial Engagement

Week 1

2 Preparation

Week 2

OSC

- CAGE Code
- Assessment UID (if applicable)
- Frame the Assessment
- Identify all In-Scope Assets
- Access SSP
- Scope Definition
- Contract Agreement with C3PAO

Phase 0 Checklist

- CMMC Pre-Assessment Form Template
- CA-RR Checklist

C3PAO

- Confirmation of Assessment Scope
- Preliminary Assessment Scope Documentation
- Manage Initial COI
- Propose Lead CCA
- Execute Contractual Agreement
- Identify In-scope ESPs

CMMC Toolkit



Level 1 Toolkit



Policy Template



Procedure Template



**CMMC Playbook
Level 1, 2 & 3**



Mappings

- ✦ CMMC → NIST Cybersecurity Framework
- ✦ CMMC → NIST SP 800-171r2
- ✦ CMMC → NIST SP 800-53r5



Infographics

- ✦ CMMC Ecosystem
- ✦ CMMC Domains
- ✦ CMMC Level 1 Practices
- ✦ CMMC Level 1 Assessment Objectives

Subscribe to CMMC Level 1 Toolkit

Level 2 Toolkit



Policy Template



Procedure Template



**CMMC Playbook
Level 1, 2 & 3**



Mappings

- ✦ CMMC → NIST Cybersecurity Framework
- ✦ CMMC → NIST SP 800-171r2
- ✦ CMMC → NIST SP 800-53r5



Infographics

- ✦ CMMC Ecosystem
- ✦ CMMC Domains
- ✦ CMMC Level 2 Practices
- ✦ CMMC Level 2 Assessment Objectives

Subscribe to CMMC Level 2 Toolkit



Peter Harvey

Peter.Harvey@ecfirst.com

www.ecfirst.com