CMMC Certification Training

Virtual | Public | Private

Cybersecurity Maturity Model Certification

Program Guide

THE CYBER AB CMMC CERTIFICATION
REGISTERED PRACTITIONER
CAICO LPP
CAICO CERTIFIED CMMC ASSESSOR
THE CYBER AB CMMC CERTIFICATION
REGISTERED PRACTITIONER ORGANIZATION RPO
THE CYBER AB CMMC CERTIFICATION
AUTHORIZED C3PAO
CAICO LTP
THE CYBER AB CMMC CERTIFICATION
REGISTERED PRACTITIONER ADVANCED
CAICO CERTIFIED CMMC PROFESSIONAL

ecfirst | AI Defense, *Beyond Cyber*

Table of Contents

DoD's - CMMC 2.0

Ali Pabrai
Chief Executive
Global Cyber Defense
Thought Leader

Cybersecurity is only as good as an organization's weakest link. Increasingly, the weakest link is the cyber supply chain. Third-party vendors and business associates such as CSPs or technology firms have long struggled to establish a credible cyber defense to protect sensitive and confidential information they process for their clients.

To aid with this and to ensure cyber resilience in its supply chain, the U.S. DoD introduced the CMMC framework in 2020. The latest version of this standard is CMMC.

The CMMC framework is of relevance not only to the DoD but other federal and state government agencies, and organizations that provide services to government agencies. CMMC is built on the NIST family of standards. CMMC establishes cybersecurity certification requirements, so achieving CMMC Certification brings credibility to any organization wanting to do business with the federal government. Senior executives will benefit from studying CMMC standard and considering raising the bar of their NIST-based program by achieving CMMC Certification.

The latest version of CMMC framework, CMMC, is a comprehensive framework that includes cyber protection standards that aim to protect the DIB from being damaged by APTs.

CSPs
Cloud Service Providers

NIST
National Institute of Standards and Technology

DIB
Defense Industrial Base

APTs
Advanced Persistent Threats

CMMC 2.0 framework includes several updates to CMMC 1.0 model. Both models address the following topics:

- Safeguarding sensitive information such as FCI and CUI
- Enhancing accountability while minimizing barriersto comply with DoD requirements
- Dynamically enhancing DIB cybersecurity to meet evolving threats

By incorporating CMMC standards into acquisition programs, the DoD ensures that contractors and subcontractors will meet its cybersecurity requirements.

The DIB is the target of increasingly frequent and complex cyberattacks by adversaries and non-state actors. Made up of hundreds of thousands of small, medium, and large organizations, the DIB exists globally. It is a top priority of the DoD to dynamically enhance DIB cybersecurity requirements to protect against these evolving threats and safeguard the information that supports and enables U.S. military services and operations such as the exchange of sensitive information. CMMC is a key component of the DoD's expansive DIB cybersecurity effort.

> It is a top priority of the DoD to dynamically enhance DIB cybersecurity requirements to protect against evolving. Evolving threats and safeguard the information that supports and enables U.S. military services and operations such as the exchange of sensitive information.

"CMMC will dramatically strengthen the cybersecurity of the Defense Industrial Base," said Jesse Salazar, U.S. Deputy Assistant Secretary of Defense for Industrial Policy. "By establishing a more collaborative relationship with industry, these updates will support businesses in adopting the practices they need to thwart cyberthreats while minimizing barriers to compliance with DoD requirements."

The changes reflected in CMMC will be implemented through CMMC rulemaking process. Enterprises will be required to comply once the forthcoming rules go into effect. The DoD intends to pursue rulemaking in both Part 32 of the CFR and the DFARS in Part 48 of the CFR.

FCI
Federal Contract Information

CUI
Controlled Unclassified Information

DoD
Department of Defense

CFR
Code of Federal Regulations

DFARS
Defense Federal Acquisition Regulation Supplement

The DoD is exploring opportunities to provide incentives for contractors who voluntarily obtain a CMMC Certification in the interim period.

FCI and CUI Are a CMMC Priority

FCI is defined as information not intended for public release; that is, information that is provided by or generated for the government under a contract to develop or deliver a product or service to the government, but not provided by the government to the public (such as that which exists on public websites). Simple transactional information such as that necessary to process payments is also defined as FCI.

CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

The DoD's intent under CMMC is that if a DIB enterprise does not process, store or transmit CUI on its unclassified network, but does process, store or handle FCI, then it must perform a CMMC Level 1 Self-Assessment and submit the results with an annual affirmation by a senior enterprise official.

> The CMMC model is designed to protect FCI and CUI that are shared with contractors and subcontractors of the DoD to support contract acquisition and performance.

CMMC only applies to DIB contractors' unclassified networks that process, store or transmit FCI or CUI.

The Structure of CMMC

CMMC is aligned with U.S. NIST standards, specifically NIST SP SP 800-171 Rev 2, Protecting CUI in Nonfederal Systems and Organizations, and NIST SP 800-172, Enhanced Security Requirements for Protecting CUI. The DoD's requirements will continue to evolve as changes are made to the underlying NIST SP 800-171 and NIST SP 800-172 requirements.

SP
Special Publication

CMMC standard is organized into 3 specific levels:

1. **Level 1 Foundational** - Represents the entry level for CMMC 2.0 framework and includes 17 practices.
2. **Level 2 Advanced** - Includes 110 practices aligned with NIST SP 800-171 Rev 2. Level 2 may include:
   - CUI (non-prioritized acquisitions)
   - CUI (prioritized acquisitions)

3. Level 3 Expert - Includes more than 110 practices based on NIST SP 800-172 and is the highest level.

Level 1 applies to organizations that process FCI but not CUI. Level 2 organizations process both FCI and CUI and require the implementation of additional cybersecurity capabilities. In addition, Level 2 organizations must meet all security requirements specified in NIST SP 800-171 Rev 2.

CMMC Assessment and Certification

DIB organizations are fully responsible for obtaining the necessary CMMC Certification, including coordinating and planning their participation in CMMC assessment.

Level 1 and a subset of organizations at Level 2 can demonstrate compliance with CMMC requirements through Self-Assessments. Self-Assessments associated with Level 1 and a subset of Level 2 programs (e.g., CUI, nonprioritized acquisitions) will be required on an annual basis.

Third-party and government-led assessments, associated with some Level 2 (e.g., CUI, prioritized acquisitions) and all Level 3 programs, will be required on a triennial basis. The assessment requirements will be applicable to the impacted organizations and their associated contractors.

Once CMMC is fully implemented, the DoD will only accept CMMC assessments that are provided by an authorized and accredited C3PAO and conducted by certified CMMC Assessors. Under certain circumstances, the DoD allows enterprises to make POA&Ms to earn their CMMC Certifications.

After completion of CMMC assessment, the C3PAO will provide an assessment report to the DoD. As part of the CMMC implementation, the DoD will approve all CMMC AB conflict-ofinterest-related policies that apply to CMMC ecosystem.

C3PAO
CMMC Third-Party Assessor Organization

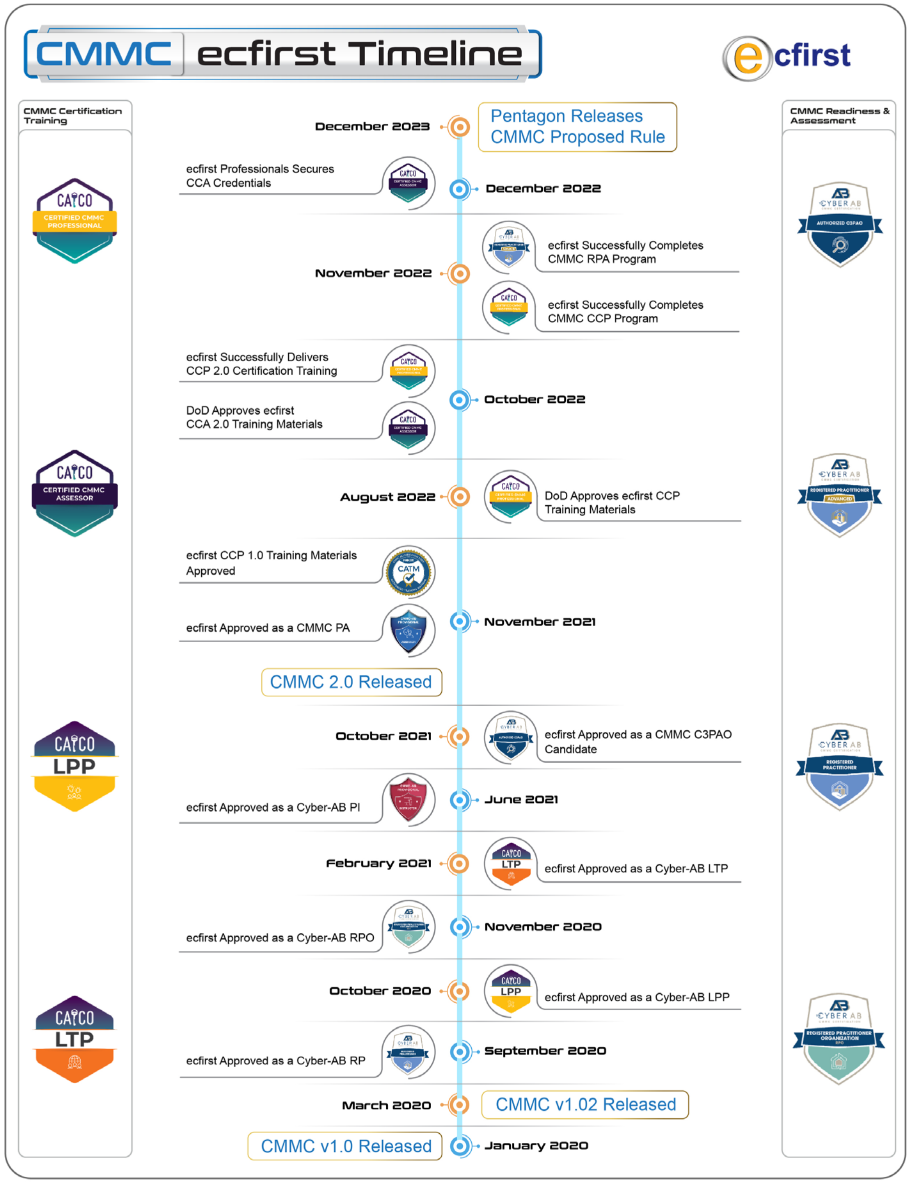
POA&Ms
Plans of Action and Milestones

Conclusion

CMMC is organized into 3 levels. Level 2 (advanced) will be equivalent to NIST SP 800-171. Level 3 (expert) will be based on a subset of NIST SP 800-172 requirements.

Cybersecurity professionals and senior executives across industries should take note of CMMC framework. This is the cybersecurity standard for this decade and beyond. Organizations across industries can leverage CMMC requirements to improve their cyberdefense posture and establish a more credible, evidence-based security program.

The future demands active cyber defense. The threats faced by enterprises will require leaders to rethink and reimagine cybersecurity. Forward-thinking organizations should target CMMC Certification at the appropriate level based on the risk to their businesses and associated assets.



CMMC ecfirst Timeline

CMMC Certification Training
CATCO CERTIFIED CMMC PROFESSIONAL
CATCO CERTIFIED CMMC ASSESSOR
CATCO LPP
CATCO LTP
CMMC Readiness & Assessment
CYBER AB AUTHORIZED C3PAO
CYBER AB REGISTERED PRACTITIONER ADVANCED
CYBER AB REGISTERED PRACTITIONER
CYBER AB REGISTERED PRACTITIONER ORGANIZATION RPO

December 2023 – Pentagon Releases CMMC Proposed Rule

December 2022 – ecfirst Professionals Secures CCA Credentials

November 2022 – ecfirst Successfully Completes CMMC RPA Program; ecfirst Successfully Completes CMMC CCP Program

October 2022 – ecfirst Successfully Delivers CCP 2.0 Certification Training; DoD Approves ecfirst CCA 2.0 Training Materials

August 2022 – DoD Approves ecfirst CCP Training Materials

November 2021 – ecfirst CCP 1.0 Training Materials Approved; ecfirst Approved as a CMMC PA

CMMC 2.0 Released

October 2021 – ecfirst Approved as a CMMC C3PAO Candidate

June 2021 – ecfirst Approved as a Cyber-AB PI

February 2021 – ecfirst Approved as a Cyber-AB LTP

November 2020 – ecfirst Approved as a Cyber-AB RPO

October 2020 – ecfirst Approved as a Cyber-AB LPP

September 2020 – ecfirst Approved as a Cyber-AB RP

March 2020 – CMMC v1.02 Released

January 2020 – CMMC v1.0 Released

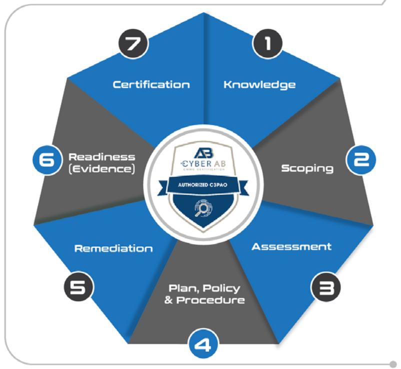
Organizations Seeking Certification OSC

Cybersecurity Maturity Model Certification (CMMC)

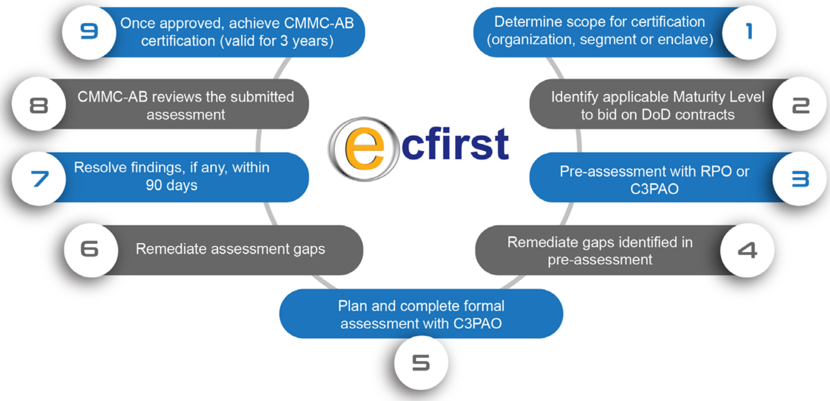
OSC

- OSCs are organizations with the intent to have the maturity of their cybersecurity program(s) certified under CMMC.
- Initially, CMMC-AB will focus on DoD contractors who need certification to respond to an active DoD solicitation.
- CMMC is currently expected to be required at contract award, not at proposal submission.
- Registered Provider Organizations (RPOs) and Certified 3rd Party Assessment Organizations (C3PAOs) assist OSC to create cybersecurity programs that will meet/exceed CMMC requirements and to prepare for an assessment.
- May grow to include other federal agencies in the near future.

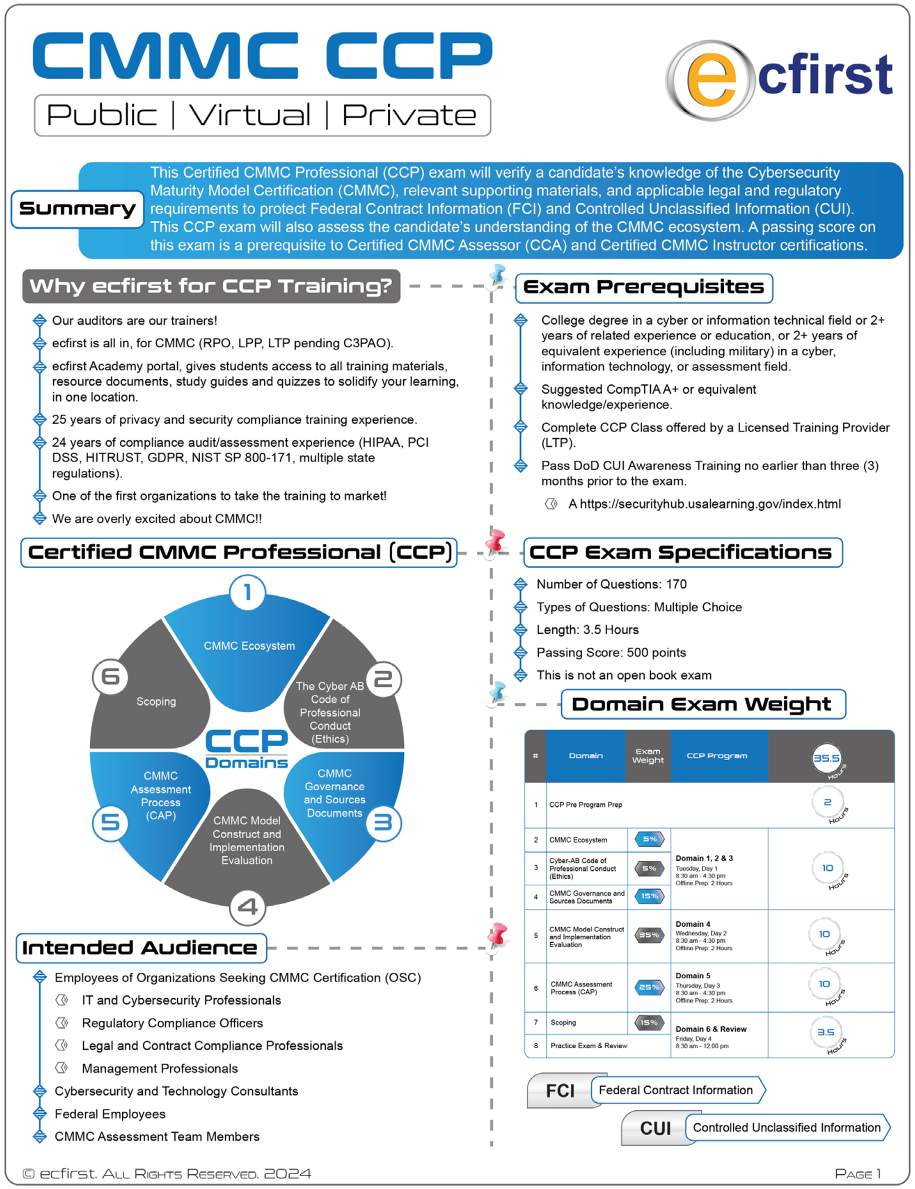
Signature Methodology



CMMC-AB Certification | Key Steps



1. Determine scope for certification (organization, segment or enclave)
2. Identify applicable Maturity Level to bid on DoD contracts
3. Pre-assessment with RPO or C3PAO
4. Remediate gaps identified in pre-assessment
5. Plan and complete formal assessment with C3PAO
6. Remediate assessment gaps
7. Resolve findings, if any, within 90 days
8. CMMC-AB reviews the submitted assessment
9. Once approved, achieve CMMC-AB certification (valid for 3 years)



CMMC CCP

Public | Virtual | Private

ecfirst

Summary

This Certified CMMC Professional (CCP) 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). This CCP 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 (CCA) and Certified CMMC Instructor certifications.

Why ecfirst for CCP Training?

- Our auditors are our trainers!
- ecfirst is all in, for CMMC (RPO, LPP, LTP pending C3PAO).
- ecfirst Academy portal, gives students access to all training materials, resource documents, study guides and quizzes to solidify your 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!
- We are overly excited about CMMC!!

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 Licensed Training Provider (LTP).
- Pass DoD CUI Awareness Training no earlier than three (3) months prior to the exam.
  - A https://securityhub.usalearning.gov/index.html

Certified CMMC Professional (CCP)

CCP Domains

1 CMMC Ecosystem

2 The Cyber AB Code of Professional Conduct (Ethics)

3 CMMC Governance and Sources Documents

4 CMMC Model Construct and Implementation Evaluation

5 CMMC Assessment Process (CAP)

6 Scoping

CCP Exam Specifications

- Number of Questions: 170
- Types of Questions: Multiple Choice
- Length: 3.5 Hours
- Passing Score: 500 points
- This is not an open book exam

Domain Exam Weight

#	Domain	Exam Weight	CCP Program	35.5 Hours
1	CCP Pre Program Prep			2 Hours
2	CMMC Ecosystem	5%	**Domain 1, 2 & 3** Tuesday, Day 1 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
3	Cyber-AB Code of Professional Conduct (Ethics)	5%		
4	CMMC Governance and Sources Documents	15%		
5	CMMC Model Construct and Implementation Evaluation	35%	**Domain 4** Wednesday, Day 2 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
6	CMMC Assessment Process (CAP)	25%	**Domain 5** Thursday, Day 3 8:30 am - 4:30 pm Offline Prep: 2 Hours	10 Hours
7	Scoping	15%	**Domain 6 & Review** Friday, Day 4 8:30 am - 12:00 pm	3.5 Hours
8	Practice Exam & Review			

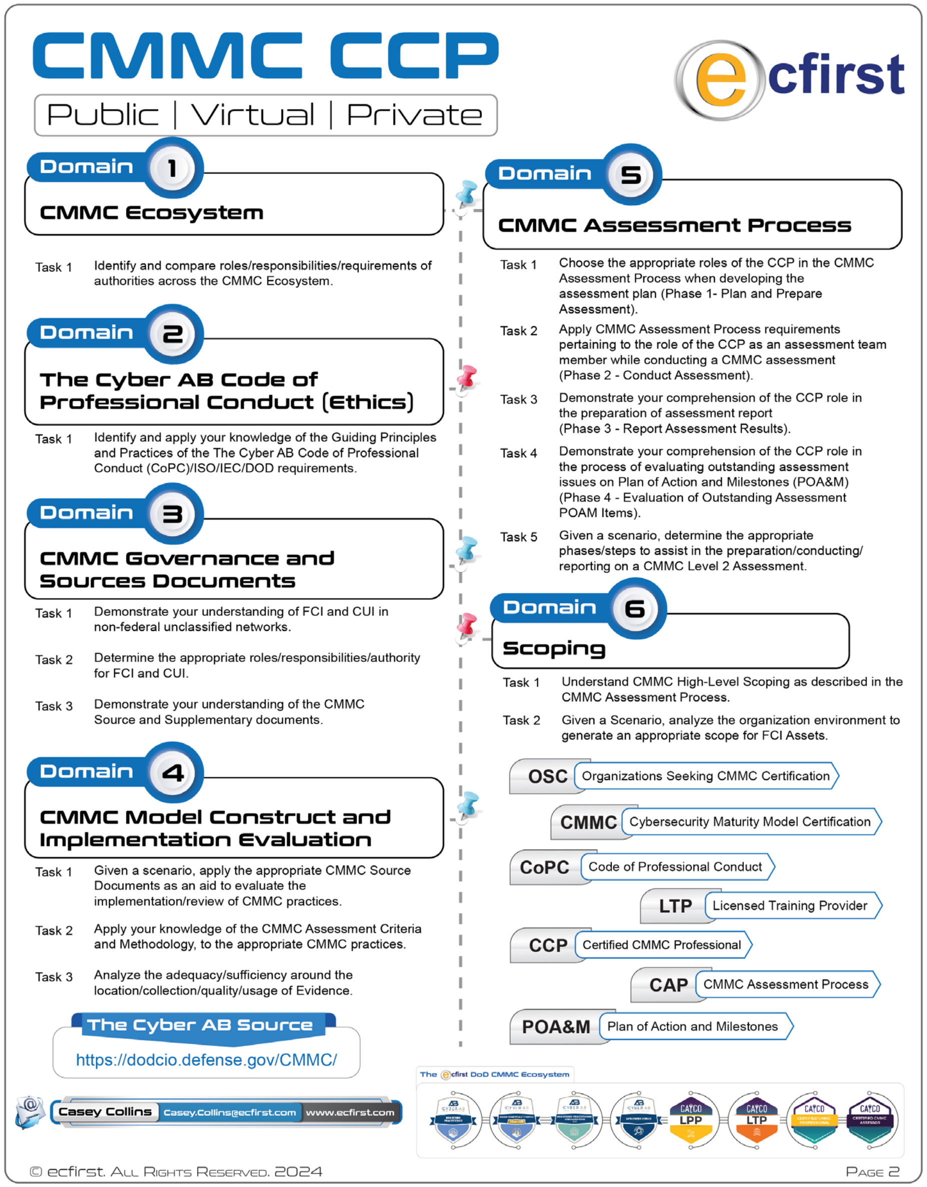
FCI Federal Contract Information

CUI Controlled Unclassified Information

Intended Audience

- Employees of Organizations Seeking CMMC 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

© ecfirst. All Rights Reserved. 2024 Page 1



CMMC CCP

Public | Virtual | Private

ecfirst

Domain 1 CMMC Ecosystem

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

Domain 2 The Cyber AB Code of Professional Conduct (Ethics)

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

Domain 3 CMMC Governance and Sources Documents

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

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

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

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.

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

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

The Cyber AB Source

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

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).

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).

Task 3 Demonstrate your comprehension of the CCP role in the preparation of assessment report (Phase 3 - Report Assessment Results).

Task 4 Demonstrate your 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 POAM Items).

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

Domain 6 Scoping

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

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

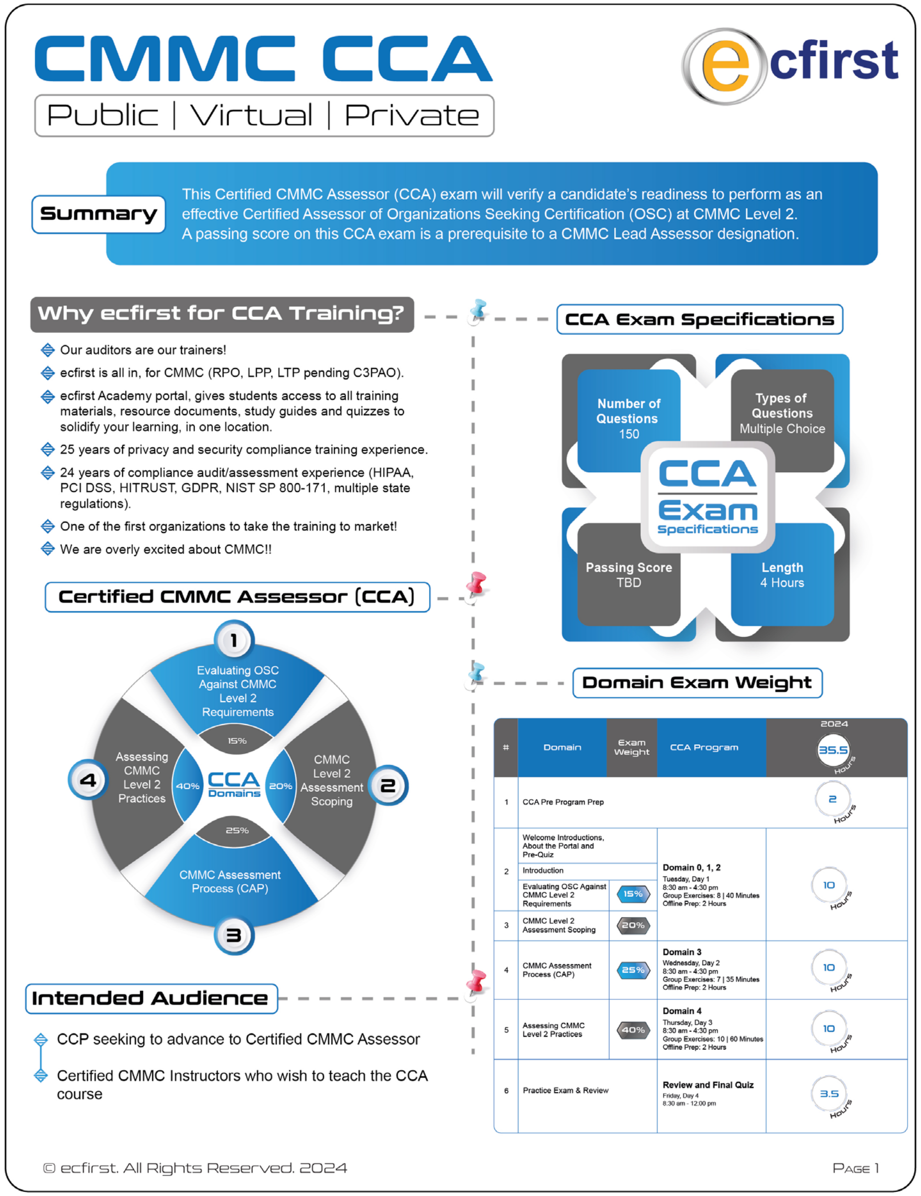
OSC	Organizations Seeking CMMC Certification
CMMC	Cybersecurity Maturity Model Certification
CoPC	Code of Professional Conduct
LTP	Licensed Training Provider
CCP	Certified CMMC Professional
CAP	CMMC Assessment Process
POA&M	Plan of Action and Milestones

Casey Collins Casey.Collins@ecfirst.com www.ecfirst.com

The ecfirst DoD CMMC Ecosystem

CYBER AB
CYBER AB
CYBER AB
CYBER AB
CAICO LPP
CAICO LTP
CAICO CERTIFIED CMMC PROFESSIONAL
CAICO CERTIFIED CMMC ASSESSOR

© ecfirst. All Rights Reserved. 2024 Page 2



CMMC CCA

Public | Virtual | Private

ecfirst

Summary

This Certified CMMC 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 this CCA exam is a prerequisite to a CMMC Lead Assessor designation.

Why ecfirst for CCA Training?

- Our auditors are our trainers!
- ecfirst is all in, for CMMC (RPO, LPP, LTP pending C3PAO).
- ecfirst Academy portal, gives students access to all training materials, resource documents, study guides and quizzes to solidify your 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!
- We are overly excited about CMMC!!

CCA Exam Specifications

CCA Exam Specifications

Number of Questions
150

Types of Questions
Multiple Choice

Passing Score
TBD

Length
4 Hours

Certified CMMC Assessor (CCA)

CCA Domains
1 Evaluating OSC Against CMMC Level 2 Requirements 15%
2 CMMC Level 2 Assessment Scoping 20%
3 CMMC Assessment Process (CAP) 25%
4 Assessing CMMC Level 2 Practices 40%

Domain Exam Weight

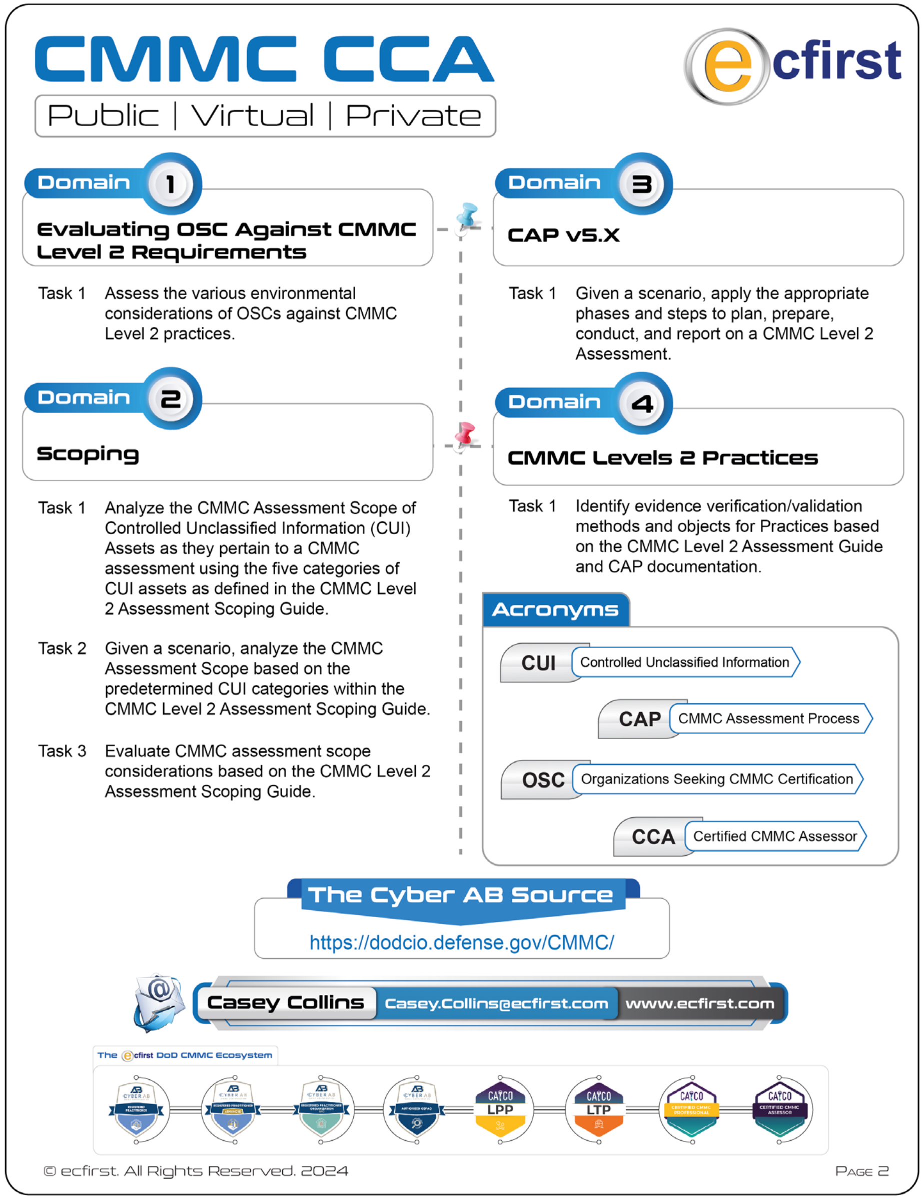
#	Domain	Exam Weight	CCA Program	2024 35.5 Hours
1	CCA Pre Program Prep			2 Hours
2	Welcome Introductions, About the Portal and Pre-Quiz		**Domain 0, 1, 2** Tuesday, Day 1 8:30 am - 4:30 pm Group Exercises: 8 | 40 Minutes Offline Prep: 2 Hours	10 Hours
	Introduction			
	Evaluating OSC Against CMMC Level 2 Requirements	15%		
3	CMMC Level 2 Assessment Scoping	20%		
4	CMMC Assessment Process (CAP)	25%	**Domain 3** Wednesday, Day 2 8:30 am - 4:30 pm Group Exercises: 7 | 35 Minutes Offline Prep: 2 Hours	10 Hours
5	Assessing CMMC Level 2 Practices	40%	**Domain 4** Thursday, Day 3 8:30 am - 4:30 pm Group Exercises: 10 | 60 Minutes Offline Prep: 2 Hours	10 Hours
6	Practice Exam & Review		**Review and Final Quiz** Friday, Day 4 8:30 am - 12:00 pm	3.5 Hours

Intended Audience

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

© ecfirst. All Rights Reserved. 2024

Page 1



CMMC CCA

Public | Virtual | Private

ecfirst

Domain 1

Evaluating OSC Against CMMC Level 2 Requirements

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

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.

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

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

Domain 3

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.

Domain 4

CMMC Levels 2 Practices

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

Acronyms

CUI	Controlled Unclassified Information
CAP	CMMC Assessment Process
OSC	Organizations Seeking CMMC Certification
CCA	Certified CMMC Assessor

The Cyber AB Source

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

Casey Collins | Casey.Collins@ecfirst.com | www.ecfirst.com

The ecfirst DoD CMMC Ecosystem

© ecfirst. All Rights Reserved. 2024

Page 2

An Infographic

CMMC Fast Facts

Cybersecurity Maturity Model Certification | CMMC

CMMC Highlights

- With the implementation of CMMC, the Department (DoD) is introducing several key changes that build on and refine the original program requirements.
  - Focused on the most critical requirements
  - Aligned with widely accepted standards
  - Reduced assessment costs
  - Higher accountability
  - Spirit of collaboration
  - Added flexibility and speed

CMMC Model Overview

- CMMC is the next iteration of the DoD's CMMC cybersecurity model.
- It streamlines requirements to three levels of cybersecurity.
- Aligns the requirements at each level with well-known and widely accepted NIST cybersecurity standards.

CMMC Source

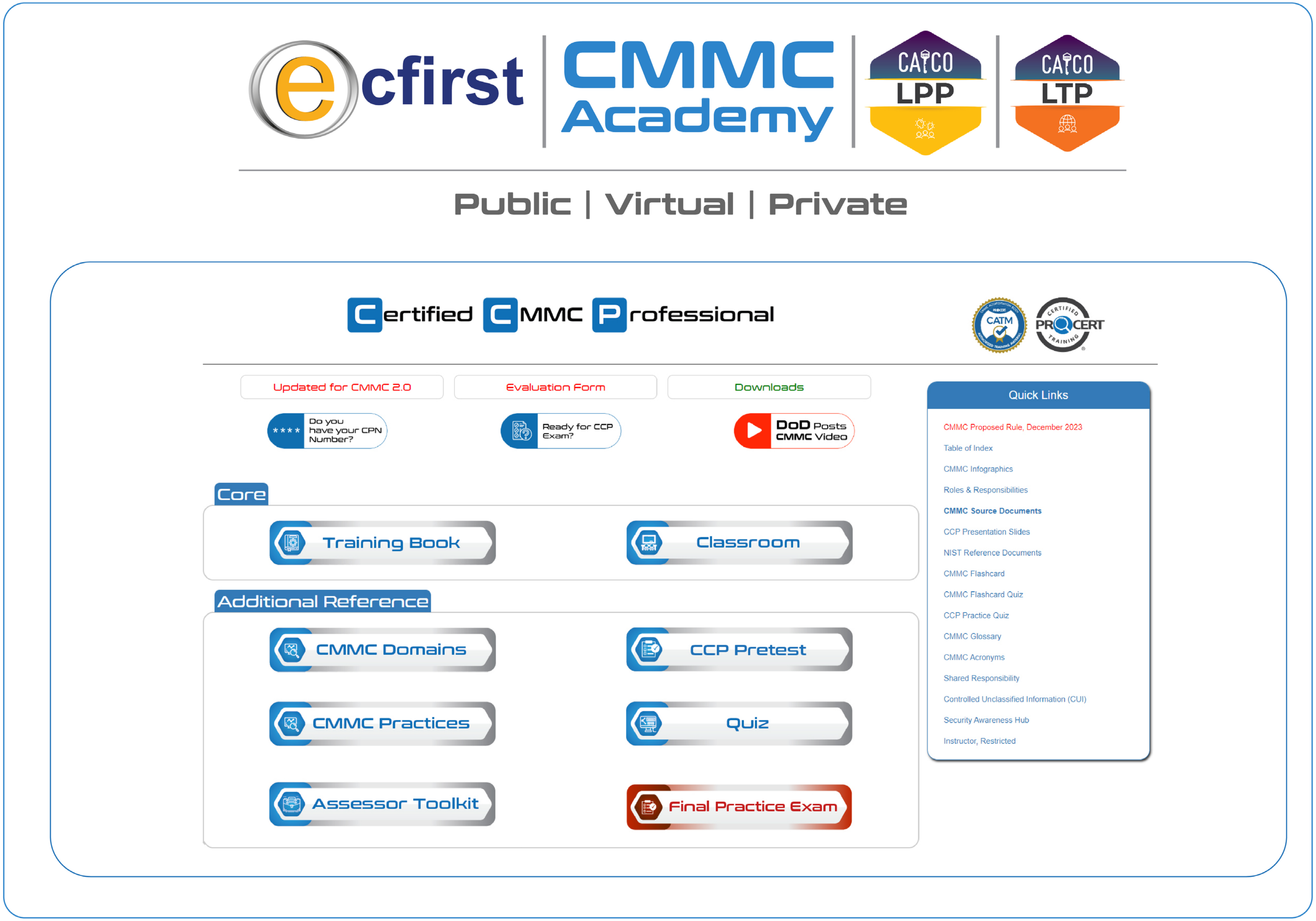
https://dodcio.defense.gov/CMMC/

CMMC Key Features

CMMC Model	Model	Assessment
LEVEL 3	110+ Requirements based on NIST SP 800-171 & 800-172	Triennial government-led assessment & annual affirmation
LEVEL 2	110 Requirements aligned with NIST SP 800-171	Triennial third-party assessment & annual affirmation; Triennial self-assessment & annual affirmation for select programs
LEVEL 1	15 Requirements	Annual self-assessment & annual affirmation

AI Defense, *Beyond Cyber*

Global AI Cyber Defense Thought Leader



ecfirst | CMMC Academy | CAICO LPP | CAICO LTP

Public | Virtual | Private

Certified CMMC Professional

Updated for CMMC 2.0

Evaluation Form

Downloads

Do you have your CPN Number?

Ready for CCP Exam?

DoD Posts CMMC Video

Core

Training Book

Classroom

Additional Reference

CMMC Domains

CCP Pretest

CMMC Practices

Quiz

Assessor Toolkit

Final Practice Exam

Quick Links

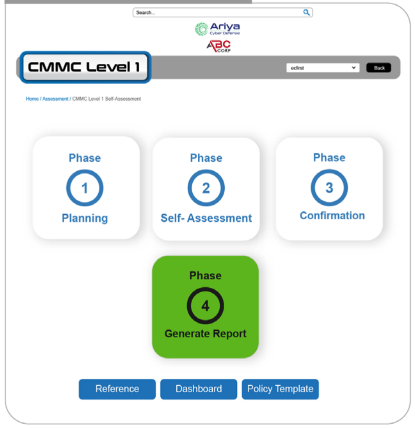
- CMMC Proposed Rule, December 2023
- Table of Index
- CMMC Infographics
- Roles & Responsibilities
- **CMMC Source Documents**
- CCP Presentation Slides
- NIST Reference Documents
- CMMC Flashcard
- CMMC Flashcard Quiz
- CCP Practice Quiz
- CMMC Glossary
- CMMC Acronyms
- Shared Responsibility
- Controlled Unclassified Information (CUI)
- Security Awareness Hub
- Instructor, Restricted

CMMC L1 Self-Assessment Portal

Cybersecurity Maturity Model Certification (CMMC)

Ariya Cyber Defense

CMMC Dashboard



Search...

Ariya Cyber Defense

ABC CORP

CMMC Level 1

ecfirst | Back

Home / Assessment / CMMC Level 1 Self-Assessment

Phase 1 Planning

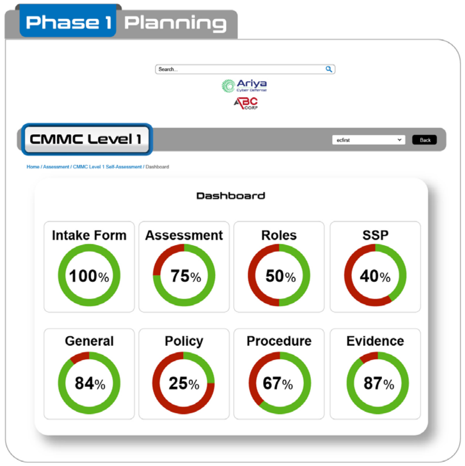
Phase 2 Self- Assessment

Phase 3 Confirmation

Phase 4 Generate Report

Reference | Dashboard | Policy Template

Phase 1 Planning



Search...

Ariya Cyber Defense

ABC CORP

CMMC Level 1

ecfirst | Back

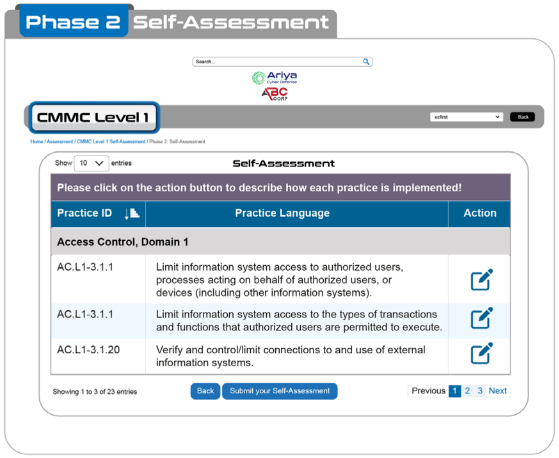
Home / Assessment / CMMC Level 1 Self-Assessment / Dashboard

Dashboard

Intake Form	Assessment	Roles	SSP
100%	75%	50%	40%

General	Policy	Procedure	Evidence
84%	25%	67%	87%

Phase 2 Self-Assessment



Search...

Ariya Cyber Defense

ABC CORP

CMMC Level 1

ecfirst | Back

Home / Assessment / CMMC Level 1 Self-Assessment / Phase 2: Self-Assessment

Self-Assessment

Show 10 entries

Please click on the action button to describe how each practice is implemented!

Practice ID	Practice Language	Action
Access Control, Domain 1		
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).	✎
AC.L1-3.1.1	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	✎
AC.L1-3.1.20	Verify and control/limit connections to and use of external information systems.	✎

Showing 1 to 3 of 23 entries

Back | Submit your Self-Assessment

Previous 1 2 3 Next

Sample CMMC Report

ABC CORP

CMMC Level 1
Self-Assessment Report

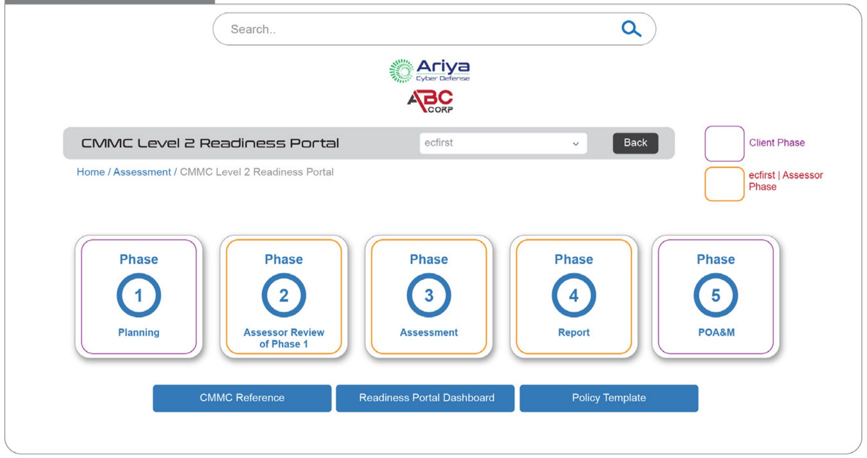
March 2, 2025

CMMC Level 2 Readiness Portal

Cybersecurity Maturity Model Certification (CMMC)

Ariya Cyber Defense

CMMC Dashboard



Search..

Ariya Cyber Defense

ABC CORP

CMMC Level 2 Readiness Portal

ecfirst | Back

Home / Assessment / CMMC Level 2 Readiness Portal

□ Client Phase

□ ecfirst | Assessor Phase

Phase 1 Planning

Phase 2 Assessor Review of Phase 1

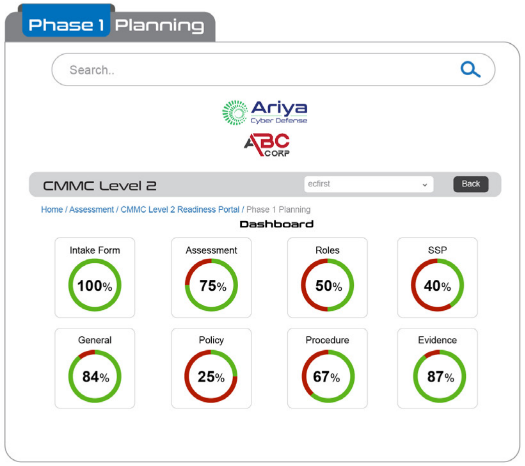
Phase 3 Assessment

Phase 4 Report

Phase 5 POA&M

CMMC Reference | Readiness Portal Dashboard | Policy Template

Phase 1 Planning



Search..

Ariya Cyber Defense

ABC CORP

CMMC Level 2

ecfirst | Back

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

Dashboard

Intake Form	Assessment	Roles	SSP
100%	75%	50%	40%

General	Policy	Procedure	Evidence
84%	25%	67%	87%

Sample CMMC Report

ABC CORP

CMMC Level 2
Readiness Report

March 2, 2025

ecfirst

Consulting Practice

HIPAA™ Academy

TRACER℠ ASSET RISK MANAGEMENT

CYBER AB REGISTERED PRACTITIONER

CYBER AB REGISTERED PRACTITIONER ADVANCED

HITRUST® Authorized External Assessor

Managed Compliance

AI Cyber Defense Academy

CYBER AB AUTHORIZED C3PAO

CYBER AB REGISTERED PRACTITIONER ORGANIZATION

Virtual ISO & InfoSec Staffing

On-Demand Consulting

Med Device Cybersecurity Culinda

NIST

Certification Training

CHP Certified HIPAA Professional HIPAA Academy

CSCS CERTIFIED SECURITY COMPLIANCE SPECIALIST

CCSA℠ Certified Cyber Security Architect

HIMSS APPROVED EDUCATION PARTNER

CAICO LPP

CAICO LTP

ecfirst Academy

CAICO CERTIFIED CMMC PROFESSIONAL

CAICO CERTIFIED CMMC ASSESSOR

AI Defense, *Beyond Cyber*

Ali Pabrai

U.S. Department of Defense CMMC Program

CYBER AB REGISTERED PRACTITIONER

CYBER AB REGISTERED PRACTITIONER ADVANCED

CAICO CERTIFIED CMMC PROFESSIONAL

CAICO CERTIFIED CMMC ASSESSOR

Global AI Cyber Defense Thought Leader

MSEE | CISSP (ISSAP | ISSMP) | CMMC (CCA, CCP, PA, PI, RPA, RP) | HITRUST® CCSFP | Security+

ISACA TOP-RATED SPEAKER ★★★★★

Mr. Ali Pabrai, a global AI cybersecurity & compliance expert, is the chairman & chief executive of ecfirst. A highly sought after professional, he has successfully delivered solutions to U.S. government agencies, IT firms, healthcare systems, legal & other organizations worldwide. His career was launched with the U.S. Department of Energy's nuclear research facility, Fermi National Accelerator Laboratory. He has served as vice chairman and in several senior officer positions with NASDAQ-based firms.

Mr. Pabrai has led numerous engagements worldwide for ISO 27001, PCI DSS, NIST, CMMC, GDPR, CCPA, FERPA, HITRUST CSF and HIPAA/HITECH. Mr. Pabrai served as an Interim CISO for a health system with 40+ locations.

Mr. Pabrai has presented passionate briefs to tens of thousands globally, including the USA, United Kingdom, France, Taiwan, Singapore, Canada, India, UAE, Saudi Arabia, Philippines, Japan, Ireland, Bahrain, Jordan, South Africa, Egypt, Ghana and other countries.

He is a globally renowned speaker who has been featured as a keynote as well as moderated cybersecurity conferences. Mr. Pabrai is the author of several published works. Clients that Mr. Pabrai has delivered to have included the U.S. Defense Intelligence Agency (DIA), and the U.S. Naval Surface Warfare Center.

Mr. Pabrai was appointed and served (2017) as a member of the select HITRUST CSF Assessor Council. Mr. Pabrai is a proud member of the InfraGard (FBI).

> “We have had the true pleasure of working with Ali Pabrai at conferences all over the world during the past few years – with one unanimous word that keeps resounding among audiences and staff alike – *AWESOME!*”
>
> Michael Mach | *Conference Program Manager* | *ISACA*

ISACA® Trust in, and value from, information systems

FBI Conference

INFRAGARD 25 YEARS PARTNERSHIP FOR PROTECTION

> “Pabrai's presentation style is engaging, and he encourages questions and discussions. I would recommend him for future presentations and trainings.”
>
> Josh More | *Cyber Sector Chief* | *Iowa FBI InfraGard*

> “On behalf of the Idaho InfraGard (FBI), I would like to thank Pabrai for presenting at our conference. Pabrai is the kind of speaker you want to bring to executives and staff. He says it in a simple, no nonsense way, in a manner that everyone can understand.”
>
> Rachel Zahn | *President* | *InfraGard (FBI)* | *Idaho Alliance*

> “You delivered a fantastic presentation and we all felt your passion for cyber security.”
>
> James E Lamadrid | *Supervisory Special Agent* | *Federal Bureau of Investigation (FBI)* | *Cyber Task Force*

> “Thank you Pabrai. Your enthusiasm and relevance for the Information Security material you presented at our combined Infragard (FBI) conference in Idaho Falls was very well received and pertinent to both our chapter as an organization and the constituents in attendance.”

> “As a government employee, I appreciated the simplified insight of highlighting the importance of compliance and funding compared to information security success beyond qualitative metrics. I heard many times over that your specific information with measurable results made your material directly relevant to individuals, businesses and organizations. Thanks again and I hope you are able to join us again in the future.”
>
> Clark Harshbarger | *FBI*

Author

Getting Started with HIPAA — First published book on HIPAA

UNIX Internetworking — First book on UNIX & Networks

Internet & TCP/IP Network Security — First book on TCP/IP security

The ecfirst DoD CMMC Ecosystem

CYBER AB REGISTERED PRACTITIONER | CYBER AB REGISTERED PRACTITIONER ADVANCED | CYBER AB REGISTERED PRACTITIONER ORGANIZATION | CYBER AB AUTHORIZED C3PAO | CAICO LPP | CAICO LTP | CAICO CERTIFIED CMMC PROFESSIONAL | CAICO CERTIFIED CMMC ASSESSOR

Achieve CMMC Certification

HITRUST® Authorized External Assessor