EDWARDS
PERFORMANCE SOLUTIONS

YOUR CMMC PARTNER

CYBER AB CMMC CERTIFICATION
AUTHORIZED C3PAO

CYBER AB CMMC CERTIFICATION
REGISTERED PRACTITIONER ORGANIZATION
RPO

CAICO
LPP

CAICO
LTP

WHAT YOU NEED TO KNOW ABOUT CMMC

300,000+

CONTRACTORS, SUBCONTRACTORS, SUPPLIERS, AND SUPPORTING ORGANIZATIONS

CMMC IS DESIGNED TO

- Safeguard sensitive information to enable and protect the warfighter
- Dynamically enhance DIB cybersecurity to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Contribute towards instilling a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

ALL DoD Contractors and Subcontractors must comply with CMMC to achieve these goals

EDWARDS & THE CMMC

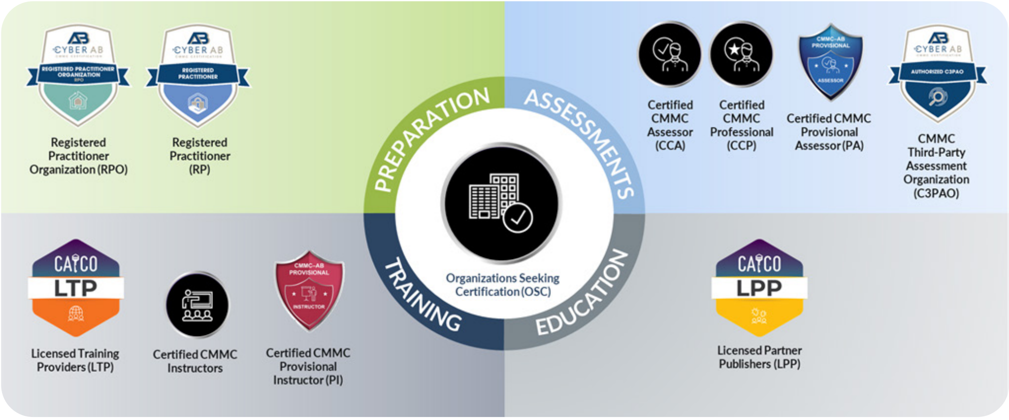
We partner with organizations to provide the knowledge and expertise needed to prepare for and comply with CMMC; **WE DO NOT COMPETE WITH CONSULTANTS, IMPLEMENTERS, OR MSPs**. We develop goal-oriented, impactful plans of action to both meet the requirements of CMMC and support your desired business outcomes.

Edwards plays a role in nearly every aspect of the CMMC ecosystem — training, education, consulting, and assessments.

Currently, we support Organizations Seeking Certification (OSC) as a Registered Practitioner Organization (RPO) and Authorized CMMC Third-Party Assessment Organization (C3PAO), providing CMMC preparation/gap assessments, consulting, and remediation support.

As a Licensed Partner Publisher (LPP) Edwards developed the curriculum to train the assessment community as a Licensed Training Provider (LTP) our consultants are also conducting the training classes.

ORGANIZATIONS


Registered Practitioner Organization (RPO)
Registered Practitioner (RP)
PREPARATION
ASSESSMENTS
Certified CMMC Assessor (CCA)
Certified CMMC Professional (CCP)
Certified CMMC Provisional Assessor (PA)
CMMC Third-Party Assessment Organization (C3PAO)
Organizations Seeking Certification (OSC)
TRAINING
EDUCATION
Licensed Training Providers (LTP)
Certified CMMC Instructors
Certified CMMC Provisional Instructor (PI)
Licensed Partner Publishers (LPP)

CMMC MODEL

The level of certification an organization requires is largely dependent on the type of information they handle and the work they may be bidding.

Level 3 Expert	110+ requirements based on NIST SP 800-171 & 800-172	Triennial government-led assessment & annual affirmation
Level 2 Advanced	110 requirements aligned with NIST SP 800-171	Triennial third-party assessment & annual affirmation; annual self-assessment & annual affirmationfor select programs
Level 1 Foundational	15 requirements	Annual self-assessment & annual affirmation

CMMC DOMAINS

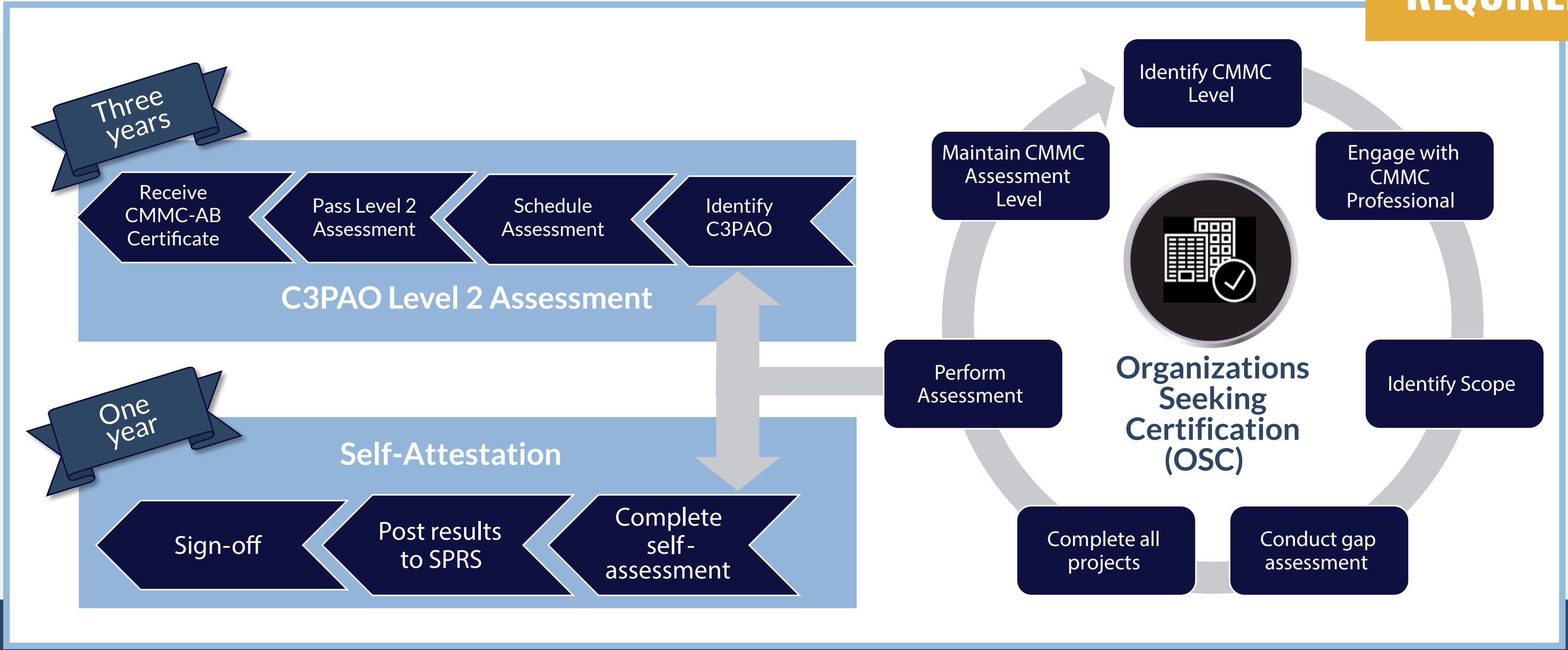
The CMMC model framework organizes processes and cybersecurity best practices into a set of 14 domains. These domains are broken down into capabilities, and further broken down into practices.

AC Access Control	**AU** Audit and Accontability	**AT** Awareness and Training	**CM** Configuration Management	**IA** Identification and Authentication
IR Incident Response	**MA** Maintenance	**MP** Media Protection	**PS** Personnel Security	**PE** Physical Protection
RA Risk Assessment	**CA** Security Assessment	**SC** System and Communications Protection	**SI** System and Information Integrity	

DOMAIN	LEVEL 1 PRACTICES	LEVEL 2 PRACTICES	GRAND TOTAL
Access Control	4	18	22
Audit & Accountability		9	9
Awareness & Training		3	3
Configuration Management		9	9
Identification & Authentication	2	9	11
Incident Response		3	3
Maintenance		6	6
Media Protection	1	8	9
Personnel Security		2	2
Physical Protection	4	2	6
Risk Assessment		3	3
Security Assessment		4	4
System & Communications Protection	2	14	16
System & Information Integrity	4	3	7
ALL DOMAINS	**17**	**93**	**110**

CMMC CONFORMITY LIFECYCLE

REQUIREMENTS



1. **Identify the desired CMMC Level –** This may be driven by existing contracts, the desire to bid on contracts requiring a particular level of compliance, or the type of information the OSC possesses/develops.

2. **Engage with The Cyber AB trained professionals for guidance –** This may be a Certified CMMC Professional (CCP), C3PAO, or trained individual/ team within the OSC. The key is that they should be trained to understand what the assessors will be looking for.

3. **Identify the assessment scope –** Identify the flow of CUI and FCI; determine the in and out of scope systems, and their related protections.

4. **Conduct a gap assessment –** Complete all projects associated with any identified gaps.

5. **Perform the assessment**
   - Self-Attestation: complete the self-assessment and posting the results in the SPRS system, signed off by a company official.
   - C3PAO Level 2 assessment:
     - Identify a C3PAO in the CMMC Marketplace
     - Schedule an assessment with the C3PAO (cannot be individuals or a C3PAO who may have helped with the OSC preparations)
     - Pass the Level 2 assessment
     - Receive The Cyber AB Certificate; valid for three years

6. **Maintaining the approved CMMC Assessment level status for all components of the assessment status and re-assessing**
   - One year (if self-assessment)
   - Three years (if Level 2 formal assessment)

SENSITIVE INFORMATION CLASSIFICATION

Within the CMMC Model, there are three classifications for sensitive information. These classifications inform what maturity levels are necessary when achieving CMMC certification.

FCI

FEDERAL CONTRACT INFORMATION

is not intended for public release, provided by, or generated for the Government under a contract to develop or deliver a product or service to the government.

CUI

CONTROLLED UNCLASSIFIED INFORMATION

is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies.

CTI

CONTROLLED TECHNICAL INFORMATION

means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, or disclosure.

CLASSIFIED INFORMATION IS OUTSIDE THE SCOPE OF CMMC

> “I enjoyed piecing together all the resources available to assist the community in understanding CMMC. The commentary and context from all the instructors was amazing compared to just reading the slides.
>
> TRAVIS BRITTAIN | Director Product Enablement
> Blackpoint (Cybersecurity Vendor)

> I really enjoyed the flow of the class - it was great to hear the background of CMMC and then move into the meat of actual assessment content. Going through the framework and hearing the thoughts of the presenters on each was very helpful and informative.
>
> JESSIE SANDELL | CISA, IT Audit & Advisory Manager
> Frazier Deeeter (CMMC-AB RPO, SOC2 Specialists)

> It was very useful to have the different objectives explained in detail as part of the process. Hugely valuable source of reference material and insight to the process and how the DOD approaches compliance. Not having a huge Government background, this was very helpful for me as a security specialist from the private sector.
>
> DAVID GROOT | President, Windstar Technologies
> (MSP, CMMC-AB RP)

> The instructors and participants shared a lot of real-world experience throughout the course, which was extremely valuable. The sharing of links and other sources of information by instructors and participants was also very valuable.
>
> RUTH BARRA | CISA, QSA, CISSP, CDPSE
> Senior Consultant, Cybersecurity
> Sikich LLP (CMMC-AB C3PAO Candidate)”

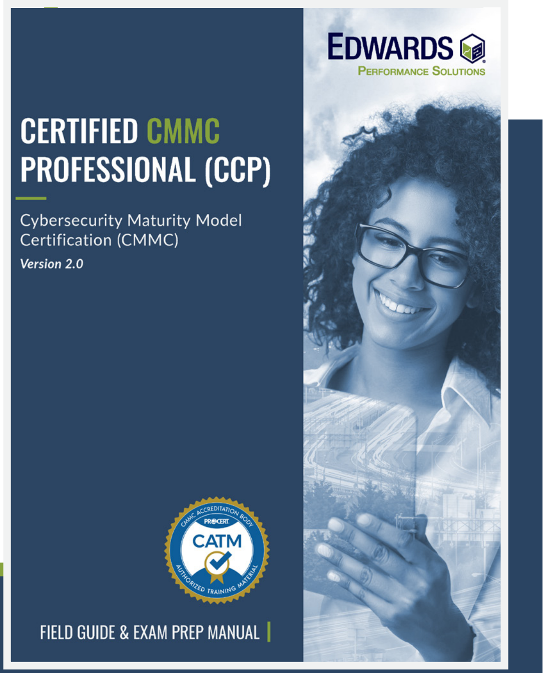
PATH TO BECOMMING A CERTIFIED CMMC PROFESSIONAL (CCP)

Edwards offers CAICO approved (CATM) CMMC classes and other materials designed, built, and delivered by leading experts in the field.

Becoming a Certified CMMC Professional (CCP) offers immense value to an OSC and Edwards team is ready to help.

SYLLABUS

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 based on 110 controls through Level 2
5. CMMC Assessment Process (CAP)
6. Scoping through Level 2



EDWARDS
PERFORMANCE SOLUTIONS

CERTIFIED CMMC PROFESSIONAL (CCP)

Cybersecurity Maturity Model Certification (CMMC)

Version 2.0

CATM

FIELD GUIDE & EXAM PREP MANUAL

EDWARDS SUPPORTS YOUR CMMC JOURNEY

PREPARATION – Edwards is a Registered Provider Organization (RPO), but more importantly we also employ CMMC Provisional Assessors (PAs). In fact, many of our consultants teach the CCP and Certified CMMC Assessor (CCA) classes and developed the curriculum to do so.

ASSESSMENTS – Edwards is a Authorized Certified Third-Party Assessment Organization (C3PAO) with multiple Provisional Assessors on staff. We are ready to support your or your clients' formal assessment process.

TRAINING AND EDUCATION – OSCs and the ecosystem of businesses/individuals supporting them need to know they are preparing the OSC for success – we train your team, consultants, supporting organizations (e.g., MSPs), and of course the assessors themselves.

We designed our curriculum to prepare individuals to do the job an OSC expects when they hire a CMMC Professional. As a Licensed Partner Publisher (LPP), Edwards develops curriculum to train the assessment community and as a Licensed Training Provider (LTP), we also facilitate training classes with a dynamic team of Provisional Instructors (PIs), with real-world experience.

LET'S TALK!

Info@EdwPS.com
www.EdwPS.com

Follow us for more CMMC &
cybersecurity thought leadership