



YOUR CMMC PARTNER



WHAT YOU NEED TO KNOW ABOUT CMMC



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 & CMMC

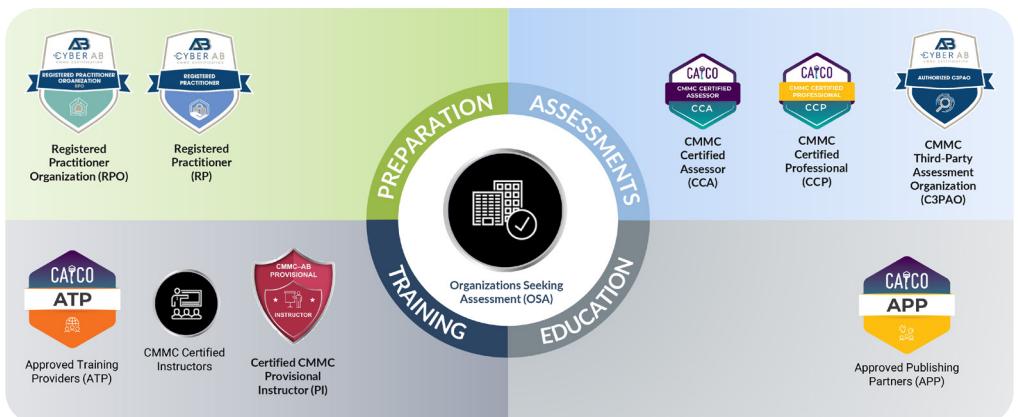
We partner with organizations to provide the expertise needed to prepare for and comply with CMMC. **WE DO NOT COMPETE WITH CONSULTANTS, IMPLEMENTERS, OR MSPs.** Our goal-oriented Plans of Action meet CMMC requirements while supporting business outcomes.

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

Currently we support **Organizations Seeking Assessment (OSAs)**, also referred to as **Organizations Seeking Certification (OSCs)**, through our role as a **Registered Practitioner Organization (RPO)** and as an **Authorized CMMC Third-Party Assessment Organization (C3PAO)**, by providing CMMC preparation, gap assessments, consulting, and remediation support.

As an **Authorized Publishing Partner (APP)**, we developed the curricula to train the assessment community, and as an **Authorized Training Provider (ATP)**, our consultants deliver training classes.

ORGANIZATIONS



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

134 Requirements
(110 from NIST SP
800-171 r2 plus 24
from 800-172)

- DIBCAC assessment every 3 years
- Annual Affirmation

Level 2 Advanced

110 Requirements
aligned with NIST SP
800-171 r2

- C3PAO assessment every 3 years, or
- Self-assessment every 3 years for select programs
- Annual Affirmation

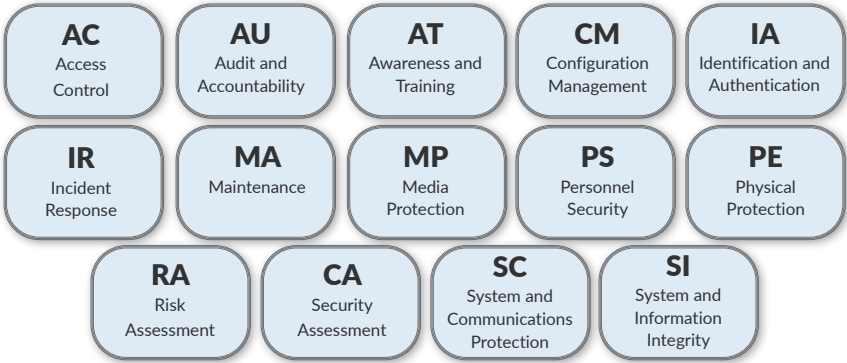
Level 1 Foundational

15 Requirements
aligned with FAR
52.204-21

- Annual Self-assessment
- Annual Affirmation

CMMC DOMAINS

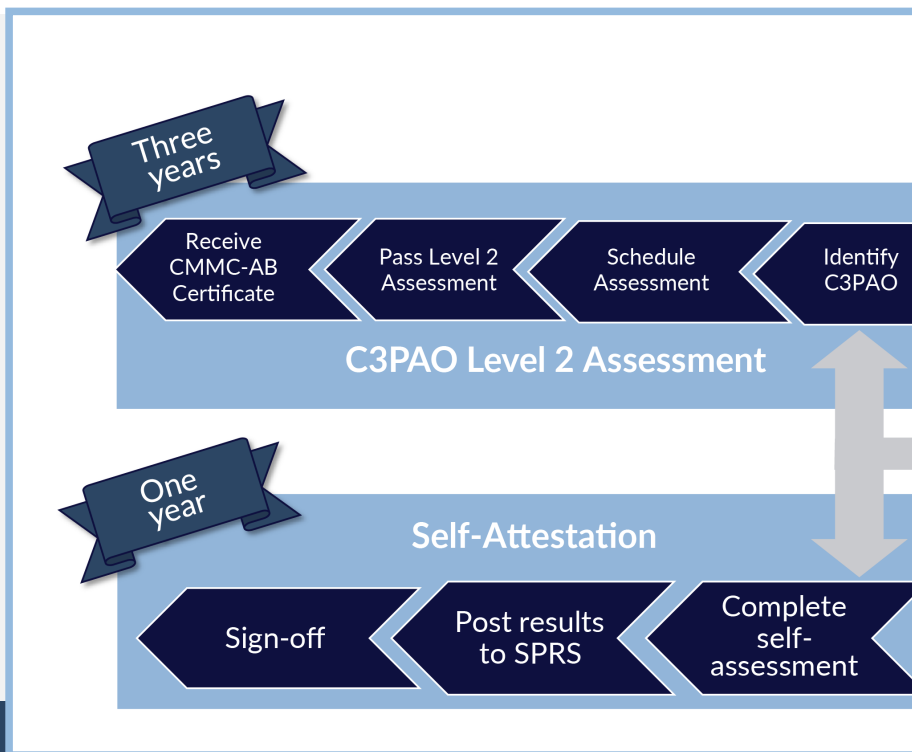
The CMMC model framework organizes processes and cybersecurity best practices into a set of 14 domains. These domains are broken down into supporting requirements, and further broken down into objectives.



REQUIREMENTS

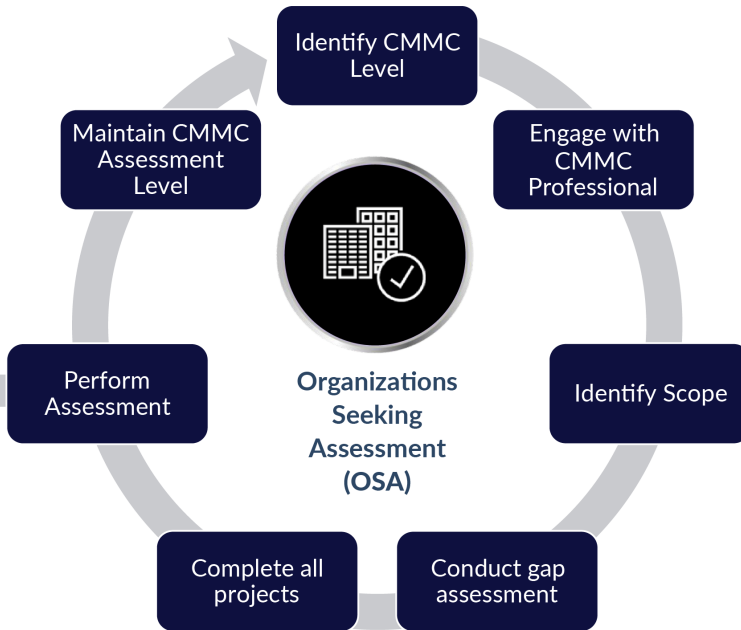
DOMAIN	LEVEL 1	LEVEL 2	LEVEL 3
Access Control	4	22	24
Audit & Accountability		9	9
Awareness & Training		3	5
Configuration Management		9	12
Identification & Authentication	2	11	13
Incident Response		3	5
Maintenance		6	6
Media Protection	1	9	9
Personnel Security		2	3
Physical Protection	2	6	6
Risk Assessment		3	10
Security Assessment		4	5
System & Communications Protection	2	16	17
System & Information Integrity	4	7	10
ALL DOMAINS	15	110	134

CMMC CONFORMITY **LIFECYCLE**



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 OSA possesses/develops.
2. **Engage with The Cyber AB trained professionals for guidance** – This may be a C3PAO, CCA, CCP, RP, or trained individual/team within the OSA. The key is that they should be trained to understand what the assessors will be looking for.
3. **Identify the assessment scope and categorize assets** – Identify the type and flow of CUI and FCI, as well as which systems, personnel, and services are in scope. Determine asset categorization to ensure the appropriate security protections are applied.
4. **Conduct a gap assessment** – Complete all projects associated with any identified gaps.

REQUIREMENTS



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 OSA preparations)
 - Pass the Level 2 assessment
 - Receive the Certificate of CMMC Status from C3PAO; valid for three years

6. Maintain the approved CMMC Assessment level status for all components of the assessment status and re-assess

- 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 applications that falls under CUI protections and is subject to access, use, reproduction, modification, performance, display, release, or disclosure controls per government regulations.

CLASSIFIED INFORMATION IS OUTSIDE THE SCOPE OF CMMC

“

Edwards instructors are top notch educators who bring a tremendous amount of experience to the classroom. I was 100% ready to pass my CCP exam immediately after completing the course. I absolutely intend to return to sit in the CCA training.

LOGAN THERRIEN | Operations Manager, Kieri Solutions

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 Deeter (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, 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

”

DIVING IN: GAP ASSESSMENTS

Gap assessments identify vulnerabilities in your cybersecurity program, comparing the organization's security practices against a set of security standards or regulations, like **NIST**, **HIPAA**, **ISO**, **HITRUST**, or **CMMC**, to determine areas where improvements are needed.



WHY DO I NEED A GAP ASSESSMENT?

Conducting a gap assessment is an essential step in achieving compliance with industry regulations and improving the overall security posture of your organization.

Non-compliance may result in penalties or lost business opportunities, so it's important to stay ahead of the game.

Assessment reports provide a:

- Detailed analysis of your gaps
- Prioritized remediation efforts
- Plan of Action and Milestones (**POA&Ms**) based on your business objectives, allowing you to improve your organization's security posture over time

THE EDWARDS DIFFERENCE

We provide non-biased consulting and remain product agnostic. Our experienced assessors navigate the practices and objectives of industry standards, delivering the expertise needed to achieve compliance.

- Documentation and Governance support
- Compliance support for multiple frameworks
- Data Flow Diagramming
- Trace Matrix development and support
- SSP development and support
- Penetration Testing and Vulnerability Scanning
- vCISO services

EDWARDS ASSESSMENTS

Simple Approach; Comprehensive Results. Our targeted yet simple approach delivers big results that respect your budget and timeline – all while keeping key stakeholders informed.



PRE-ASSESSMENT SUPPORT

Edwards conducts tailored interviews to learn about your entire ecosystem and target our engagement to your business needs.



DATA FLOW DIAGRAMMING

We identify and document the flow of FCI and CUI throughout your organization and between you and your external partners – providing the foundation for scoping your CMMC environment.



SCOPING

We determine if the assessment scope is at the enterprise, department, enclave, or service level. Asset categorization ensures CUI/FCI locations, data flow, and protections are properly mapped.



FULL-SCALE GAP ASSESSMENT

We review your systems, assess your processes, identify gaps, and ensure existing practices are fully implemented.



REMEDATION PLANNING & ROADMAPPING

We provide an actionable compliance roadmap to address remediation items, as well as outline business risk, priorities, and investments that result from identified gaps.



REMEDATION SUPPORT

We provide project and technical support to remediate your POA&Ms – helping your teams, practices, and processes become CMMC compliant.

EDWARDS CMMC TRAINING: CCP & CCA

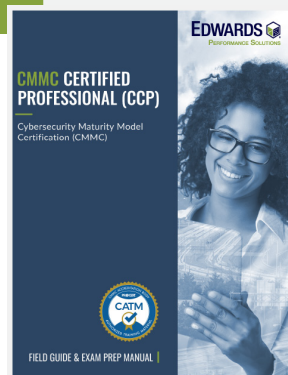
Edwards offers CAICO-approved training material (CATM) courses designed, built, and delivered by leading experts in the field.

Becoming a CMMC Certified Professional (CCP) offers immense value, providing a comprehensive CMMC foundation for CMMC implementers, consultants, or members of the assessment team.

Our CMMC Certified Assessor (CCA) course continues your education, allowing you to play a critical role in compliance, including conducting assessments or assessment preparation.

CCP SYLLABUS

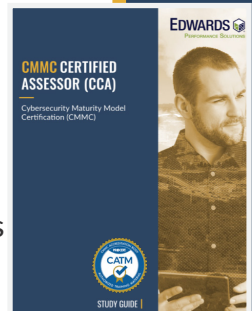
1. CMMC Ecosystem
2. The Cyber AB Code of Professional Conduct (Ethics)
3. CMMC Governance and Source Documents
4. CMMC Model Construct and Implementation Evaluation (110 controls)
5. CMMC Assessment Process (CAP)
6. Scoping through Level 2



CCA COURSE TAKEAWAYS

Building on the CCP syllabus, our CCA course provides The Cyber AB assessor perspective.

- ✓ Learn to score assessment objectives
- ✓ Explore multiple environments varying in size, locations, and on-prem vs. hybrid systems



EDWARDS SUPPORTS YOUR CMMC JOURNEY

ASSESSMENTS – Edwards is an Authorized CMMC Third-Party Assessment Organization (C3PAO) with multiple CCPs and CCAs on staff. We are ready to support your or your clients' formal assessment process.

PREPARATION – Edwards is a Registered Practitioner Organization (RPO) and employs CMMC Certified Professionals (CCPs) and CMMC Certified Assessors (CCAs) to support preparation. In fact, many of our consultants developed the CCP & CCA curricula and teach the classes.

TRAINING AND EDUCATION – Organizations Seeking Assessment (OSAs) along with the businesses and individuals supporting them, must understand what's required for a successful assessment – we train your team, consultants, supporting organizations (e.g., MSPs), and of course the assessors themselves.

We designed our curriculum to prepare individuals to meet OSA expectations when hiring a CMMC Professional. As an **Authorized Publishing Partner (APP)**, Edwards develops curriculum to train the assessment community. As an **Authorized Training Provider (ATP)**, we also facilitate training classes with a dynamic team of **Provisional Instructors (PIs)** with real-world experience.



WHO WE ARE

EDWARDS PERFORMANCE SOLUTIONS

Founded in 1997, Edwards is an innovative and respected leader in Performance Management, Organizational Resilience, Training & Development, and Cybersecurity consulting and services – ensuring operational excellence for both commercial and government entities.

We believe solutions based on proven process and procedures result in higher quality deliverables. Edwards is appraised at CMMI Level 3 for Services (CMMI SVC) and ISO 9001:2015 certified, as well as a long-time Microsoft® Silver Partner and Enterprise Solutions Provider for Microsoft® Project Professional and Project Server.

In addition to our CMMC accreditations, we are also an Authorized Training Partner (ATP) through the Project Management Institute (PMI®), with team members holding multiple PMI certifications (e.g., PMP, PMI-ACP, PMI-RMP).

These certifications indicate well-defined processes, the infrastructure to improve service delivery, and ensure a consistent level of quality on our team.

Our expansive CMMC services tap into Edwards lengthy consulting and program management history, more than two decades of successful training and facilitation, and a diverse range of cybersecurity expertise in assessing and interpreting standards – providing you top notch training and assessment preparation.

The evolving marketplace demands innovation to grow. Our dynamic approach, coupled with the real-world experience of our team, provides you the best solutions available.

We are committed to your success, providing solutions focused on people, processes, technology, and outcomes.

**WE TAKE YOUR SECURITY SERIOUSLY; AND,
HELP SMART PEOPLE DO BIG THINGS.**

LET'S TALK...

- Compliance Assessments
- Security Awareness Training
- Documentation Creation/Support
- Penetration Testing
- Vulnerability Scanning
- Organizational Resilience
- vCISO services



443.561.1334 | info@edwps.com
www.edwps.com



LET'S TALK!

info@edwps.com
www.edwps.com



Follow us for more CMMC &
cybersecurity thought leadership