ENS
Innovate. Protect. Deliver

ControlCase

WEBINAR

CMMC COMPLIANCE

Your IT Compliance Partner – Go Beyond the Checklist

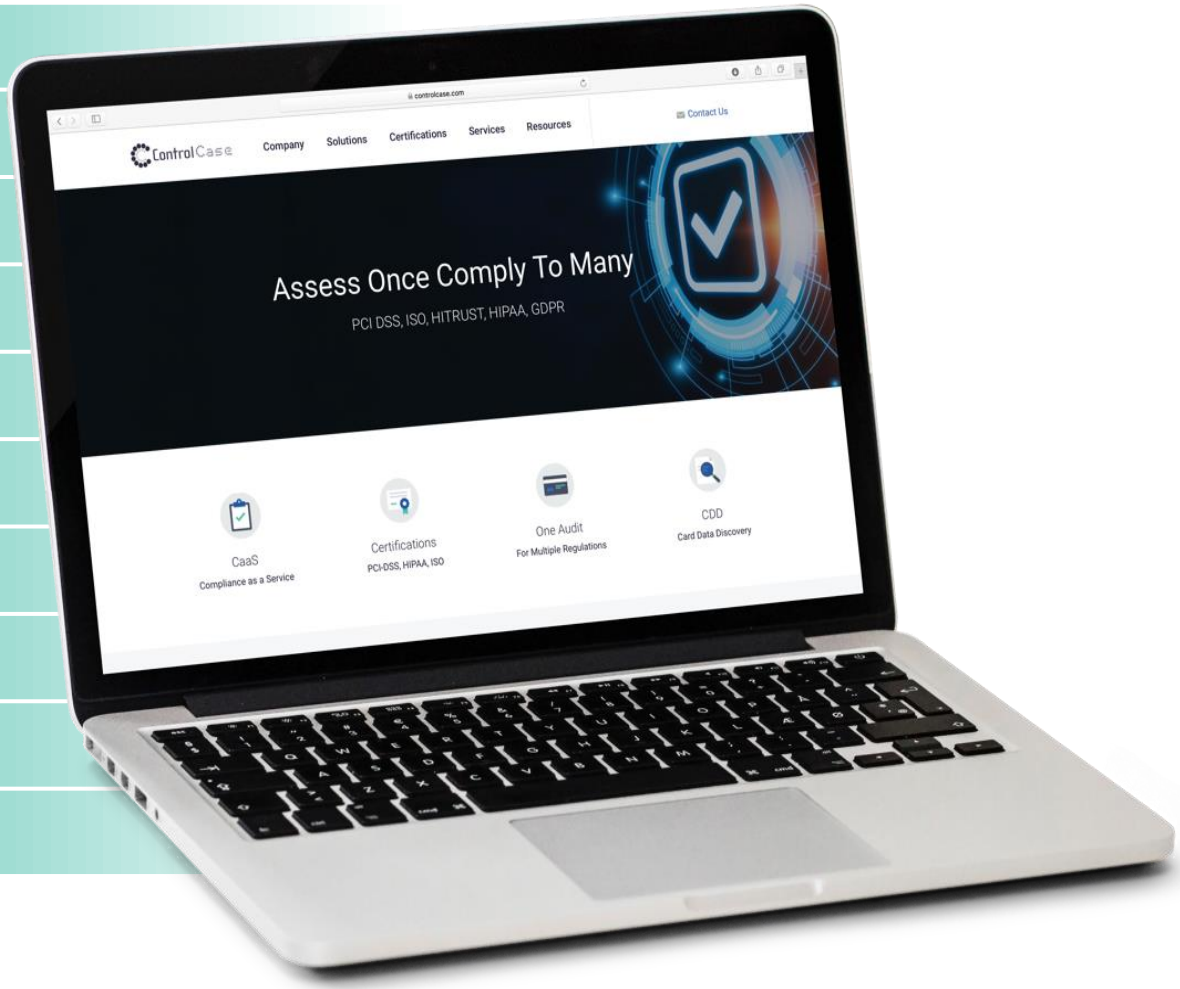
Download CMMC Compliance Checklist

CMMC Compliance Blog

Schedule a Discussion

Agenda

1. ControlCase Introduction
2. What is CMMC?
3. Who does CMMC apply to?
4. What is the CMMC accreditation body (CMMC-AB)?
5. What are the CMMC certification levels?
6. What is a CMMC Registered Provider Organization (RPO)?
7. What is a CMMC Third-Party Organization (C3PAO)?
8. CMMC and NIST
9. What is the CMMC Assessment process
10. Why ControlCase?



© 2021 ControlCase. All Rights Reserved.

CONTROLCASE INTRODUCTION

© ControlCase. All Rights Reserved.

ControlCase Snapshot

CERTIFICATION AND CONTINUOUS COMPLIANCE SERVICES

Go beyond the auditor's checklist to:

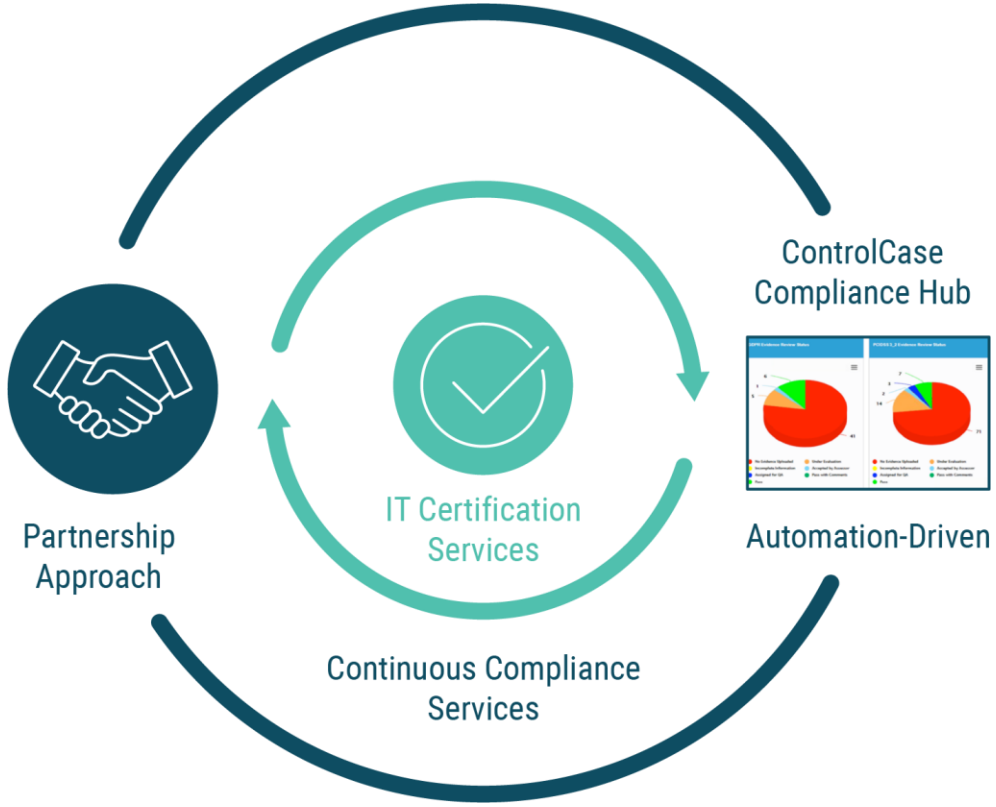
Dramatically cut the time, cost and burden from becoming certified and maintaining IT compliance.

- Demonstrate compliance more efficiently and cost effectively (cost certainty)
- Improve efficiencies
  - Do more with less resources and gain compliance peace of mind
- Free up your internal resources to focus on their priorities
- Offload much of the compliance burden to a trusted compliance partner

© ControlCase. All Rights Reserved.

Solution

Certification and Continuous Compliance Services



I've worked on both sides of auditing. ***I have not seen any other firm deliver the same product and service with the same value****. No other firm provides that continuous improvement and the level of detail and responsiveness.*

— Security and Compliance Manager,
Data Center

© ControlCase. All Rights Reserved.

Certification Services

One Audit™

Assess Once. Comply to Many.

> *You have 27 seconds to make a first impression. And after our initial meeting,* ***it became clear that they were more interested in helping our business and building a relationship, not just getting the business****.*
>
> — Sr. Director, Information Risk & Compliance, Large Merchant

© ControlCase. All Rights Reserved.

WHAT IS CMMC?

© ControlCase. All Rights Reserved.

What is CMMC?

Cybersecurity Maturity Model Certification (CMMC)

CMMC is a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB).

CMMC 1.0 Released by the US Department of Defense (DoD) and became effective November, 2020.

CMMC 2.0 Released November 2021

CMMC ensures that DIB companies implement appropriate cybersecurity practices and processes to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their unclassified networks.

© ControlCase. All Rights Reserved.

What is Federal Contract Information (FCI)?

FCI refers to Information that is collected, created or received pursuant to a government contract.	
The information is not marked as "public" or "for public release“.	Could be information used to develop a product or service.

© ControlCase. All Rights Reserved.

What is Controlled Unclassified Information (CUI)?

CUI refers to sensitive information that laws, Federal regulations, or Government-wide policies require or permit executive branch agencies to protect.

Information the Government creates or possesses.	Information an entity creates or possesses for or on behalf of the Government.

© ControlCase. All Rights Reserved.

WHO DOES CMMC APPLY TO?

© ControlCase. All Rights Reserved.

Who Does CMMC Apply To?

Defense Industrial Base (DIB) contractors whose unclassified networks possess, store, or transmit Controlled Unclassified Information (CUI).

Defense Industrial Base (DIB) contractors whose unclassified networks possess Federal Contract Information (FCI).

© ControlCase. All Rights Reserved.

WHAT IS THE CMMC ACCREDITATION BODY (CMMC-AB)?

© ControlCase. All Rights Reserved.

What is CMMC Accreditation Body (CMMC-AB)?

Independent organization authorized to operationalize CMMC in accordance with the US Department of Defense requirements.

Authorizes and Accredits CMMC Registered Provider Organizations (RPO) and Third Party Assessment Organizations (C3PAOs).

Authorizes and Accredits CMMC Assessors and Instructors Certification Organizations (CAICO).

© ControlCase. All Rights Reserved.

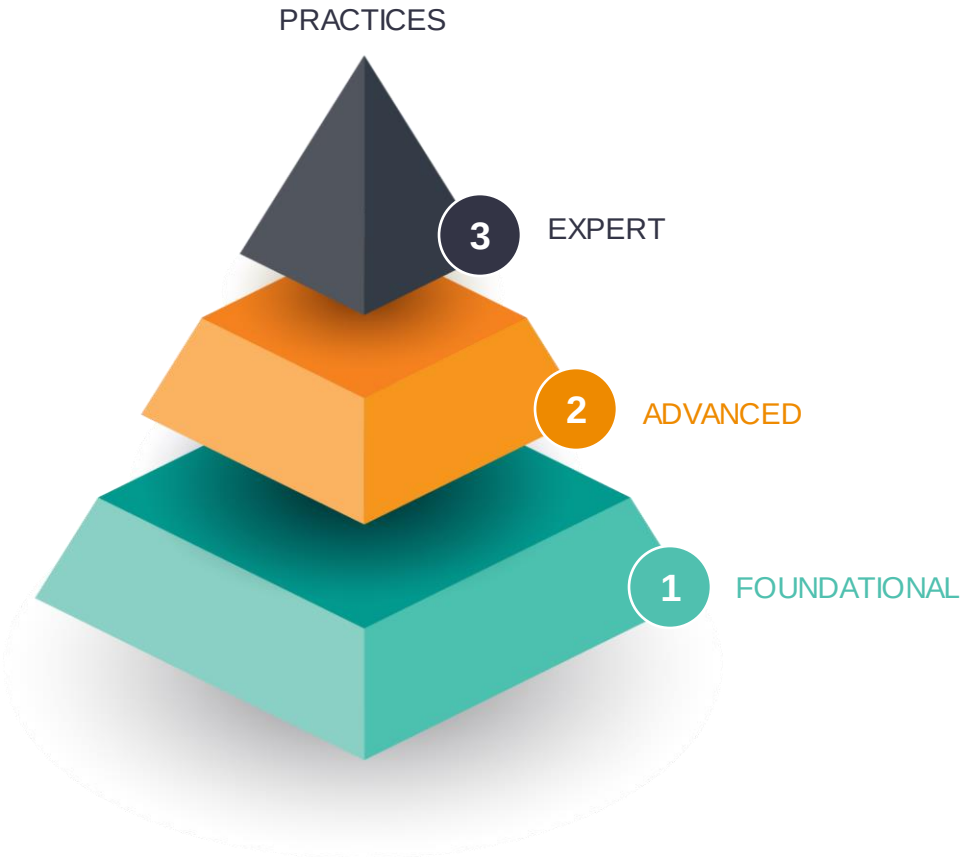
WHAT ARE THE CMMC CERTIFICATION LEVELS?

© ControlCase. All Rights Reserved.

Overview of CMMC 2.0 Levels

Cybersecurity Maturity Model Certification (CMMC)

There are 3 levels, each with associated controls and processes.	The level of the CMMC certificate is dependent upon the type and nature of information flowed down from your prime contractor.	The DoD will specify the required CMMC level in Requests for Information (RFIs) and Requests for Proposals (RFPs).



© ControlCase. All Rights Reserved.

What CMMC Level Are You?

You have FCI (Federal Contract Info) Only	You have CUI (Controlled Unclassified Information) (in addition to FCI)
Level 1	Level 2 or 3

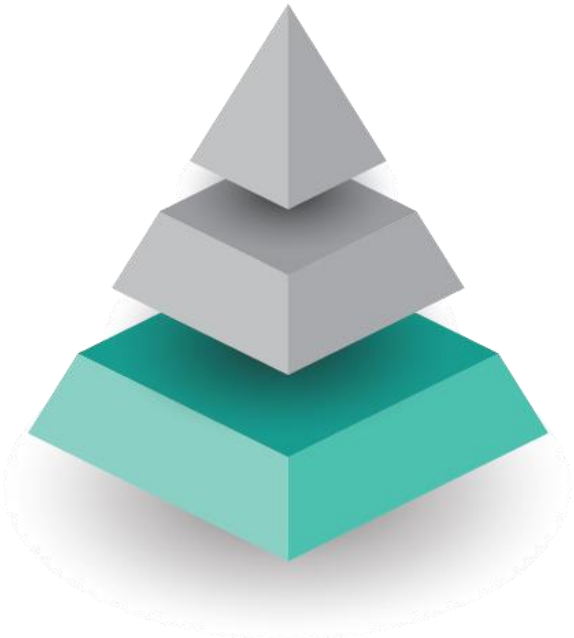
WHAT YOU NEED TO DO	
Level 1	**Self Assessment (optionally assisted by ControlCase)**
Level 2a	Your CUI is not critical to national security AND the information originated within the company) - **Self Assessment (optionally assisted by ControlCase)**
Level 2b	Your CUI is not critical to national security AND it originates within the US Government — **C3PAO assessment (C3PAO assessment once every three years)**
Level 3	Your CUI is critical to national security — **Government conducts an audit (Once every three years)**

© ControlCase. All Rights Reserved.

CMMC Level 1

(“Foundational”)

- **For Entities with Federal Contract Information (FCI) only.**
  - No Controlled Unclassified Information (CUI)
  - CMMC Self Assessment Required Annually.
  - Optionally assisted by ControlCase RPO.



© ControlCase. All Rights Reserved.

CMMC Level 2 (CUI not critical to national security)

Level 2a (“Advanced”)

- **For Entities with Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their unclassified networks**.
  - CUI is not critical to national security.
  - The information originated within the company.
  - Level 2 CMMC Self Assessment Required Annually.
  - Optionally assisted by ControlCase (an RPO).

Level 2b (“Advanced”)

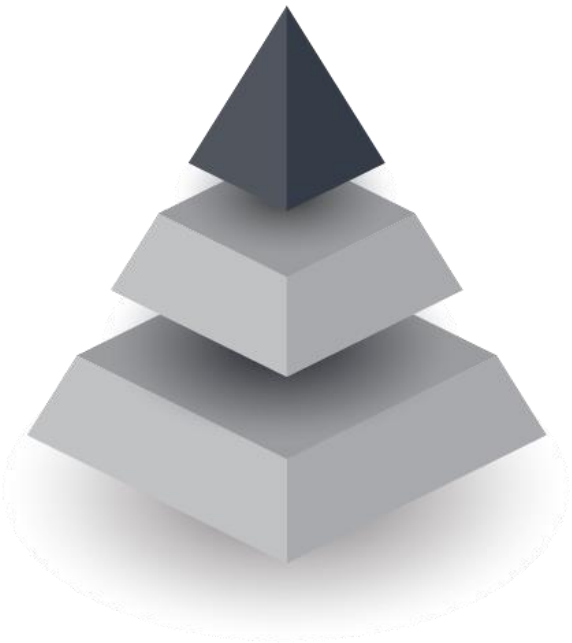
- **For Entities with Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their unclassified networks.**
  - CUI is not critical to national security.
  - The information originated within the US Government.
  - Level 2 CMMC C3PAO Assessment.
  - Completed by an approved C3PAO every 3 years.

© ControlCase. All Rights Reserved.

CMMC Level 3 (CUI critical to national security)

Level 3 (“Expert”)

- **For Entities with Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their unclassified networks.**
  - Involves CUI critical to national security.
  - Government conducts assessment every 3 years.



© ControlCase. All Rights Reserved.

WHAT IS A CMMC REGISTERED PROVIDER ORGANIZATION (RPO)?

© ControlCase. All Rights Reserved.

What is a CMMC Registered Provider Organization (RPO)

Provide “Registered Practitioners” (RPs) for advice, consulting and recommendations for companies required to comply with CMMC.

They are approved by the CMMC-AB.

Can assist with Level 1 and a subset of Level 2 (level 2a)

ControlCase is a Registered Provider Organization (RPO)

© ControlCase. All Rights Reserved.

WHAT IS A CMMC THIRD-PARTY ORGANIZATION (C3PAO)?

© ControlCase. All Rights Reserved.

What is a CMMC Third-Party Organization (C3PAO)?

Conduct CMMC Level 2 (2b) assessments and issue CMMC certificates based on the results of the assessments.

Accredited C3PAOs must meet all DoD requirements and achieve full compliance with ISO/IEC 17020.

© ControlCase. All Rights Reserved.

CMMC AND NIST

© ControlCase. All Rights Reserved.

CMMC and NIST

CMMC Level 2 includes the 110 security requirements specified in NIST SP 800-171.

The CMMC Model also incorporates additional practices and processes from other standards;

- NIST SP 800-53
- Aerospace Industries Association (AIA)
- National Aerospace Standard (NAS) 9933 “Critical Security Controls for Effective Capability in Cyber Defense”, and
- Computer Emergency Response Team (CERT)
- Resilience Management Model (RMM)

© ControlCase. All Rights Reserved.

NIST 800-171 Control Domains

110 security requirements broken down into 14 control families taken from FIPS 200 and NIST 800-53:

Access Control	Identification & Authentication	Physical Protection	Security Assessment
Audit & Accountability	Incident Response	Personnel Security	System & Communications Protection
Awareness & Training	Maintenance	Risk Assessment	Systems & Information Integrity
Configuration Management	Media Protection		

© ControlCase. All Rights Reserved.

WHAT IS THE CMMC ASSESSMENT PROCESS

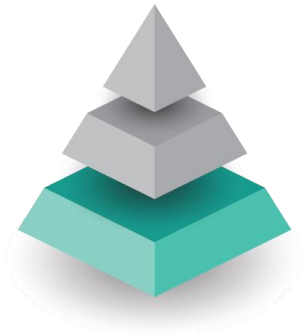
© ControlCase. All Rights Reserved.

ControlCase CMMC Assessment Process

ControlCase is a CMMC Registered Provider Organization (RPO)	ControlCase assists with CMMC Level 1 Compliance and a subset of CMMC Level 2 (2a)

© ControlCase. All Rights Reserved.

ControlCase CMMC Assessment Process



CONTROLCASE CMMC LEVEL 1 ASSESSMENT PROCESS

1. Deploy Compliance Hub with NIST 800-171 controls covering 17 practices
2. Complete Scoping
3. Complete 50% Evidence Review
4. Complete 100% Evidence Review
5. ***Publish Level 1 Self Assessment Report**

.

CONTROLCASE CMMC LEVEL 2A ASSESSMENT PROCESS

A. Deploy Compliance Hub with NIST 800-171 controls covering 110 practices
B. Complete Scoping
C. Complete 50% Evidence Review
D. Complete 100% Evidence Review
E. *Publish Level 2 Self Assessment Report

© ControlCase. All Rights Reserved.

WHY CONTROLCASE?

© ControlCase. All Rights Reserved.

One Audit™

Assess Once. Comply to Many.

CMMC RPO

CCPA

SOC 1,2,3,& Cybersecurity

ISO 27001-2

HIPAA

FedRAMP

PCI DSS

NIST CSF

PCI PIN

PCI PA-DSS

CSA Star

Microsoft SSPA

© ControlCase. All Rights Reserved.

ControlCase Compliance Hub®

Automated Compliance Engine (ACE)	ControlCase Data Discovery (CDD)	Vulnerability Assessment & Penetration Testing (VAPT)	Automated Log Analysis (LOGS)
• Collect evidence such as configurations remotely.	• Scan end user workstations for PII.	• Perform remote vulnerability scans and penetration tests.	• Review log settings and identify missing logs remotely.

© ControlCase. All Rights Reserved.

Continuous Compliance Services

ControlCase Addresses Common non-compliant situations that may leave you vulnerable:

In-scope assets not reporting logs

In-scope assets missed from vulnerability scans

Critical, overlooked vulnerabilities due to volume

Risky firewall rule sets go undetected

Non-compliant user access scenarios not flagged

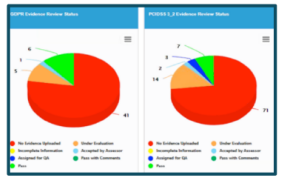
FEATURE:	**Package 1 -** With Cybersecurity Services*	**Package 2 -** Without Cybersecurity Services*
Quarterly Review of 15 to 25 Compliance Questions	✓	✓
Quarterly Review of Scope	✓	✓
Collecting & Analyzing Data through connectors from client systems	—	✓
Vulnerability Assessment	✓	—
Penetration Testing	✓	—
Sensitive Data Discovery	✓	—
Firewall Ruleset Review	✓	—
Security Awareness Training	✓	—
Logging & Automated Alerting	✓	—

* Hybrid package can be selected.

© ControlCase. All Rights Reserved.

Summary – Why ControlCase

Partnership Approach



ControlCase Compliance Hub Automation-Driven

Continuous Compliance Services

> ***They provide excellent service, expertise and technology****. And,* ***the visibility into my compliance throughout the year and during the audit process provide a lot of value to us.***
>
> — Dir. of Compliance, SaaS company

© ControlCase. All Rights Reserved.

ControlCase

THANK YOU FOR THE OPPORTUNITY TO CONTRIBUTE TO YOUR IT COMPLIANCE PROGRAM.

Download CMMC Compliance Checklist

CMMC Compliance Blog

Schedule a Discussion

www.controlcase.com

contact@controlcase.com