ENS
Innovate. Protect. Deliver

ControlCase

CMMC 2.0 COMPLIANCE CHECKLIST

CMMC is a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB). CMMC was released by the US Department of Defense (DoD) and became effective November 30th, 2020. Version 2.0 was released in November 2021.

CMMC aims to standardize and improve cybersecurity practices within the Defense Department and the Defense Industrial Base (DIB) ecosystem. 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.

CMMC enforces the Defense Federal Acquisition Regulation Supplement (DFARS) and National Institute of Standards and Technology (NIST) frameworks by requiring every contractor to be audited by an independent third-party auditor or CMMC Third-Party Assessment Organization (C3PAO).

WHAT IS CUI?

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

WHAT IS THE CMMC ACCREDITATION BODY?

It is a dependent organization authorized to operationalize CMMC in accordance with the US Department of Defense requirements. It authorizes and accredits third-party assessment organizations (C3PAOs), assessors, and instructor certification organizations (CAICO).

WHO DOES CMMC APPLY TO?

CMMC applies to:

1. Defense Industrial Base (DIB) contractors whose unclassified networks possess, store, or transmit CUI.
2. DIB contractors whose unclassified networks possess Federal Contract Information (FCI).

WHAT IS A THIRD-PARTY ORGANIZATION?

A C3PAO conducts CMMC assessments and uses CMMC certificates based on the results of the assessments. Accredited C3PAOs must meet all DOD requirements and fully comply with ISO/IEC 17020.

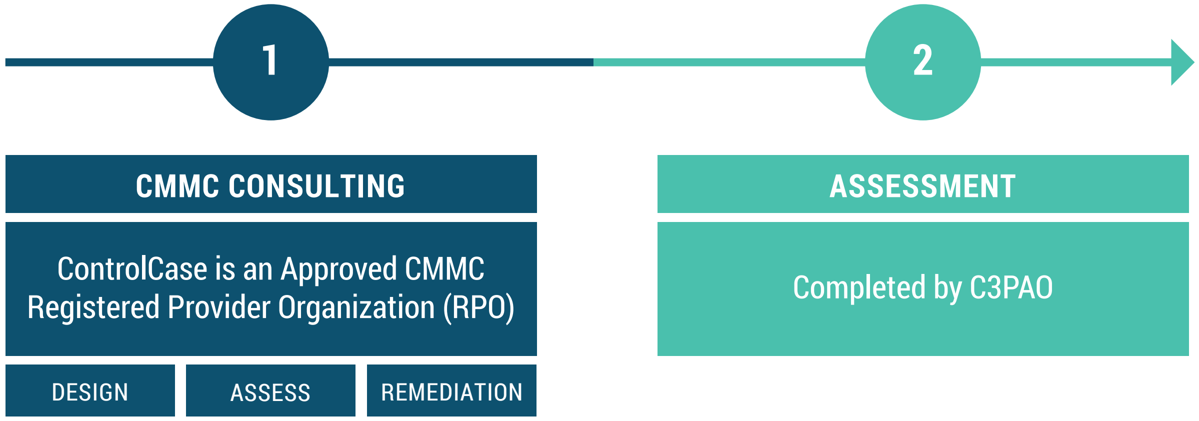
Copyright ©, ControlCase, All rights reserved.

CMMC 2.0 COMPLIACE DOMAINS CHECKILST

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

CMMC CERTIFICATION METHODOLOGY

To achieve CMMC, organizations begin by consulting an RPO to design, assess, and remediate their current cybersecurity posture. Next, they complete an assessment with an approved CMMC C3PAO. See the following graphic for more information:



1

CMMC CONSULTING

ControlCase is an Approved CMMC Registered Provider Organization (RPO)

DESIGN | ASSESS | REMEDIATION

2

ASSESSMENT

Completed by C3PAO

ABOUT CONTROLCASE:

ControlCase is a global provider of certification, cybersecurity, and continuous compliance services. ControlCase is committed to empowering organizations to develop and deploy strategic information security and compliance programs that are simplified, cost-effective, and comprehensive in both on-premises and cloud environments. ControlCase offers certifications and a broad spectrum of cyber security services that meet the needs of companies required to certify to PCI DSS, HITRUST, SOC2, CMMC, ISO 27001, PCI 3DS, PCI PIN, PCI P2PE, PCI TSP, PCI SSF (SSS & SSLC), PCI CPP, CSA STAR, HIPAA, GDPR, SWIFT, and FedRAMP.

Copyright ©, ControlCase, All rights reserved.