CMMC 2.0 At a Glance

Cybersecurity Maturity Model Certification (CMMC) is a cybersecurity program managed by the U.S. Department of Defense (DoD) Chief Information Officer (CIO).
With the CMMC program, the DoD will seeks to improve security and resilience around Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) entrusted to Defense Industrial Base (DIB) contractors.

3 Tiers/Levels
Different levels of compliance that consider the information handled and security needs.

Implementation through contracts
Contracts issued by the DoD will require CMMC compliance.

Required assessments
Certification of compliance by either third-party assessors or government partners.

CMMC Implements Requirements Across 14 Domains:
Access Control, Awareness & Training, Audit & Accountability, Configuration & Management, Identification & Authentication, Incident Response, Maintenance, Media Protection, Personnel Security, Physical Protection, Risk Assessment, Security Assessment, System & Communication Protection, System & Information Integrity.

Why is CMMC Important?

80% of critical infrastructure organizations will migrate from siloed security solutions to hyperconverged solutions that bridge cyber-physical and IT risks by 2024

– Gartner

~$6 trillion Global Cost of Cybercrime 2021, expected to grow to $10 trillion by 2025 – World Economic Forum

300,000+ DIB companies supporting

CMMC Levels

Foundational: 1

Aligns with 15 controls from FAR 52.204-21 “basic” controls to protect FCI. Annual certifications and self-assessments are reported by company leadership in DoD Supplier Performance Risk System (SPRS).

Advanced: 2

Aligns with 110 controls in NIST SP 800-171. Triennial assessments by Certified Third-Party Assessment Organizations (C3PAO).

Expert: 3

Requires 110 controls stipulated in Level 2 as well as controls from NIST SP 800-172. Triennial, government-led assessments. (This level of certification will not be required for most DIB contractors.)

Framework for CMMC

Federal Acquisition Regulation (FAR) 52.204-21
Contractors are mandated to protect systems with the requisite 15 basic cybersecurity requirements to secure FCI.

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012
All government contractors and subcontractors must comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 to secure CUI.

DFARS 252.204-7019
Requires contractors and subcontractors to upload their summary level score for their NIST SP 800-171 DoD assessment (Basic, Medium, or High) to the DoD Supplier Performance Risk System (SPRS).

DFARS 252.204-7020
Establishes the right of the government to audit companies; audits will be carried out by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). Companies must provide the government with access to their systems and facilities and verify that subcontractors are compliant.

DFARS 252.204-7021
CMMC compliance will be required by contract award after rollout (Oct 1, 2025). Prior to rollout, the OUSD(A&S) must approve inclusion of CMMC in new acquisitions. The level of mandated CMMC certification must be maintained throughout the contract award period.

How FileCloud Can Help

FileCloud is a hyper-secure content collaboration platform (CCP) that provides compliance support via powerful governance, security, and access controls.

- **Integrations: AD, LDAP, SSO & NTFS**
- **Remote Device Management**
- **Role-Based Access Controls (RBAC)**
- **Endpoint Backup**
- **Workflow Automation**
- **FIPS-enabled Encryption (At Rest & In Transit)**
- **Two-Factor Authentication (2FA)**
- **Comprehensive Audit Logs**
- **Content Classification Engine**
- **SIEM Integration**
- **Data Leak Prevention (DLP)**
- **Granular File/Folder Permissions**

*FileCloud maintains and secures the platform infrastructure. The client is responsible for configuring the platform to meet CMMC requirements and secure data within and outside the FileCloud environment.