

CMMC 2.0 – Level 3 (Expert)

CMMC 2.0 Level 3 sets advanced cybersecurity requirements to protect Controlled Unclassified Information handled by Department of Defense contractors.



What it is

CMMC 2.0 Level 3 is a cybersecurity compliance framework that sets advanced security requirements for organizations handling Controlled Unclassified Information (CUI) within the U.S. Defense Industrial Base. Its primary purpose is to safeguard sensitive government data by mandating comprehensive security controls and robust risk management practices.

Published by the U.S. Department of Defense (DoD), CMMC 2.0 Level 3 is required for contractors and subcontractors working with federal defense agencies. This level integrates practices from NIST SP 800-171 and additional requirements, covering areas such as incident response, access control, system security, and continuous monitoring of cyber risks.

At a glance

PUBLISHER U.S. Department of Defense (DoD)	TYPE Certification / Assurance Program	VERSION 2.0
EFFECTIVE November 4, 2021	DOMAIN Cybersecurity	FAMILY CMMC
REGION United States	INDUSTRY Aerospace & Defense	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY Very High		

Source: <https://dowcio.war.gov/CMMC/About/>

Why it matters

- Strengthen cybersecurity governance** Enables organizations to formalize security roles, responsibilities, and oversight, ensuring consistent management of critical cybersecurity controls.
- Enhance regulatory alignment** Aligns with NIST SP 800-171 and federal requirements, supporting organizations in demonstrating compliance with U.S. Department of Defense mandates.
- Improve incident response capabilities** Mandates robust incident detection, reporting, and recovery plans, allowing organizations to respond quickly and effectively to cyber threats.
- Increase audit readiness** Prepares contractors for mandatory third-party assessments by requiring regular security self-assessments and detailed policy documentation.

How SmartSuite supports CMMC 2.0 Level 3

Advanced Requirement Library Manage Level 3 practices layered on Level 2 with clear ownership and scope.	Threat-Focused Control Validation Track enhanced monitoring and detection validation with supporting evidence.	SSP, POA&M, and Remediation Discipline Maintain advanced evidence trails and retesting proof for closure verification.
Continuous Monitoring and Metrics Schedule high-frequency monitoring tasks and capture metrics that prove maturity.	Supplier and Access Risk Oversight Manage third-party access, dependency risks, and control evidence at scale.	Government Assessment Readiness Produce leadership-ready reporting for assessments, gaps, and risk posture.

Common framework mappings

CIS Controls v8.1

CMMC 2.0

CMMC 2.0 L2

ISO 27001:2022

NIST CSF 2.0

NIST SP 800-161 Rev.1

NIST 800-171 Rev.2

NIST 800-53 Rev.5

Official resources

CMMC 2.0 Level 3 Overview Provides an official overview of the CMMC 2.0 Level 3 cybersecurity framework and its components. acq.osd.mil/cmmc/index.html	CMMC 2.0 Framework Specification Defines requirements and practices necessary for compliance with CMMC 2.0 Level 3. acq.osd.mil/cmmc/docs/current_version.pdf
CMMC 2.0 Assessment Guide Outlines assessment processes for evaluating compliance with CMMC 2.0 Level 3 standards. acq.osd.mil/cmmc/docs/assessment_guide_v2.pdf	CMMC 2.0 Implementation Guidance Provides guidance on implementing and maintaining CMMC 2.0 Level 3 cybersecurity practices. acq.osd.mil/cmmc/implementation_guide.html

Frequently asked questions

- What is CMMC 2.0 Level 3 used for?**

CMMC 2.0 Level 3 is used to ensure that organizations within the U.S. Defense Industrial Base implement advanced cybersecurity controls to protect Controlled Unclassified Information (CUI). It serves as a benchmark for safeguarding sensitive data against sophisticated threats and supporting compliance with Department of Defense (DoD) requirements.
- Is CMMC 2.0 Level 3 certification required?**

Yes, CMMC 2.0 Level 3 certification is mandatory for contractors and subcontractors handling CUI for federal defense programs. Organizations must pass a third-party assessment to demonstrate compliance before being awarded certain DoD contracts.
- What organizations are in scope for CMMC 2.0 Level 3?**

Any organization that processes, stores, or transmits CUI on behalf of the DoD, or provides critical support through the defense supply chain, is within the scope of CMMC 2.0 Level 3. This includes both primary contractors and relevant subcontractors.
- What are the key security requirements of CMMC 2.0 Level 3?**

CMMC 2.0 Level 3 integrates all security practices from NIST SP 800-171 and adds enhanced controls from NIST SP 800-172. Key requirements include risk assessment, incident response, access management, continuous monitoring, supply chain risk management, and robust documentation of policies and procedures.

How does implementation of CMMC 2.0 Level 3 work in practice?

Organizations must map and embed CMMC 2.0 Level 3 controls into their technical, administrative, and physical security processes. This involves documenting security policies, conducting regular risk and gap assessments, training personnel, and preparing for independent third-party audits.

How does CMMC 2.0 Level 3 relate to other cybersecurity frameworks?

CMMC 2.0 Level 3 is based on NIST SP 800-171 and incorporates advanced requirements from NIST SP 800-172. It complements frameworks like ISO 27001 and builds on existing risk management and incident response processes utilized in broader information security programs.

What are the ongoing compliance obligations for CMMC 2.0 Level 3?

Maintaining CMMC 2.0 Level 3 compliance requires continuous monitoring of security controls, regular internal assessments, collection and maintenance of audit evidence, timely remediation of vulnerabilities, and periodic third-party reassessments as dictated by DoD contractual cycles.

How would SmartSuite support US CMMC 2.0 Level 3?

SmartSuite supports CMMC 2.0 Level 3 by enabling organizations to centralize risk tracking, manage and map required controls, and streamline evidence collection for audits. Its compliance tracking and remediation workflows help teams maintain audit readiness, while reporting dashboards deliver insights into compliance status and ongoing security monitoring efforts.

License included / downloadable: Yes CMMC 2.0 model and guidance are published by the U.S. DoD and are publicly available on official DoD websites. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/cmmc-2-0-level-3