Deloitte.

Cybersecurity Maturity Model Certification (CMMC)

CMMC is here: What contractors should know and do to prepare

Effective November 10, 2025[1], the long-awaited final rule (48 Code of Federal Regulation "CFR") for the CMMC program kicked off the official phased roll-out of CMMC which consists of four phases over a three-year period. This structured approach culminates in the full implementation of CMMC requirements, with CMMC provisions included in all contracts by Phase 4 (begins 36 months after the start of Phase 1).

CMMC brings both changes and challenges to contractors and subcontractors across the defense industrial base (DIB). As CMMC will be a requirement to do business with Department of Defense (DoD), it is critical for contractors and subcontractors to understand what CMMC means for their organizations and begin preparing now.

Click here to learn more about CMMC and our CMMC services

CMMC Phased Rollout Timeline[2]

2025

Nov 2025
Phase 1
- 48 CFR Effective
- Level 1 and 2 Self-Assessments requirements in solicitations, where applicable

2026

Nov 2026
Phase 2
- Begins 12 months after start of Phase 1
- Level 2 Certification requirement in solicitations, where applicable

2027

Nov 2027
Phase 3
- Begins 24 months after start of Phase 1
- Level 3 Certification requirement in solicitations, where applicable

2028

Nov 2028
Phase 4
- Begins 36 months after start of Phase 1
- Applicable CMMC Level requirements included in all solications and contracts

5 Things You Should Know		5 Actions You Should Take
Which CMMC level is applicable to you	1	If you are serving the DoD in any capacity (prime or sub-contractor), FCI and/or CUI likely exists within your environment which means you must address relevant CMMC requirements. Work with relevant stakeholders within your organization to determine which requirements are applicable (e.g., Level 1, Level 2)
You must have your CMMC Assessment Scope defined	2	Perform CUI Discovery, evaluate results, and categorize assets using the CMMC Assessment Guide (e.g., CUI Asset, Security Protection Asset (SPA), Contractor Risk Managed Asset (CRMA)).
What your current state of compliance is	3	Perform an assessment against the applicable requirements (e.g., 110 NIST SP 800-171 controls) to identify compliance gaps and improvement opportunities.
Which Plan of Action & Milestone (POA&M) requirements are applicable to you	4	Understand the POA&M requirements based on your respective CMMC level and address them as applicable. For example, at Level 1 POA&Ms are not permitted. For CMMC Levels 2 and 3 only, a conditional CMMC status may be granted for 180 days in accordance with 32 CFR 170.21[3], and award can be granted with a conditional CMMC level, however, closeout of POA&Ms is needed for final CMMC status.
Assessment results must be uploaded to Supplier Performance Risk System (SPRS)	5	Once you complete your assessment, upload your results into SPRS and communicate this to your relevant customers (e.g., DoD, prime contractors that you support as a subcontractor for a DoD contract)

CONTACT US

Alan Faver
Partner
Deloitte & Touche LLP
afaver@deloitte.com

Charan Ahluwalia
Principal
Deloitte & Touche LLP
cahluwalia@deloitte.com

Keith Thompson
Managing Director
Deloitte & Touche LLP
keithompson@deloitte.com

Mika Alexoudis
Senior Manager
Deloitte & Touche LLP
malexoudis@deloitte.com

[1]Federal Register, Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity, September 10, 2025

[2]US Department of Defense (DoD) Chief Information Officer (CIO), "About CMMC," accessed October 13, 2025

[3]Code of Federal Regulations, "Plan of Action and Milestones requirements," accessed October 13, 2025

How Deloitte has helped

CUI discovery

Deloitte conducts systematic CUI data discovery to identify, classify, and document CUI data across organizational systems, resulting in a clear CUI scope, asset inventory, and boundary identification, which directly informs the SSP and streamlines CMMC compliance.

CUI protection

Deloitte designs and implements automated data labeling and data loss prevention solutions to identify, classify, and safeguard CUI in alignment with CMMC requirements.

Gap assessments & readiness

Deloitte conducts gap assessments and readiness reviews that deliver clear remediation roadmaps, Supplier Performance Risk System (SPRS) score, helping organizations efficiently prepare for a successful CMMC assessment. While we are not a Certified Third-Party Assessment Organization (C3PAO), our services are designed to position you for success.

Policy, procedure, and system security plan development

Deloitte assists in developing and operationalizing cybersecurity policies, procedures, and SSPs. Leveraging standardized templates and collaborative workshops, helping organizations establish clear, actionable, and sustainable documentation aligned to CMMC controls.

FedRAMP-authorized cloud migration

Deloitte facilitates migration to FedRAMP authorized cloud environments through planning, architecture design, migration execution, and ongoing management, enabling a smooth transition that minimizes operational risk and accelerates adoption of secure, modern cloud infrastructure.

A broad approach to CMMC