Deloitte.

Cybersecurity Maturity Model Certification (CMMC)

CMMC Toolkit for Organizations Seeking Assessment (OSA)

Navigating CMMC can be daunting. This toolkit brings information and resources together in one place to simplify your CMMC journey.

CMMC Status	# of Requirements & Sources	Assessment Requirements	Affirmation Requirements
Level 1 (Self)	• 15 (FAR 52.204-21)	• Conducted by Organization Seeking Assessment (OSA) annually	• After each assessment, results entered in the Supplier Performance Risk System (SPRS)
Level 2 (Self)	• 110 NIST SP 800-171 R2 (DFARS 252.204-7012)	• Conducted by OSA every 3 years • CMMC Status valid for 3 years (§ 170.4)	• After each assessment and annually thereafter; results entered in SPRS
Level 3 (C3PAO)	• 110 NIST SP 800-171 R2 (DFARS 252.204-7012)	• Conducted by C3PAO every 3 years; *results entered in CMMC Enterprise Mission Assurance Support Service (eMASS)* • CMMC Status valid for 3 years (§ 170.4)	• After each assessment and annually thereafter; results entered in SPRS
Level 3 (DIBCAC)	• 110 NIST SP 800-171 R2 (DFARS 252.204-7012) • 24 selected from NIST SP 800-172 Feb2021; table 1 to § 170.14(c)(4)	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 assessment • Conducted by DIBCAC every 3 years; results entered in CMMC eMASS • CMMC Status valid for 3 years (§ 170.4)	• After each assessment and annually thereafter; results entered in SPRS • Level 2 (C3PAO) affirmation must also continue to be completed annually

Note: Click here for the complete table

Levels & and requirements[1]

CMMC levels come with distinct requirements—knowing which apply to you is a vital step toward compliance.

Resources for OSAs[1]

While the path to CMMC can be challenging, various resources are available to help guide OSAs through the process. Access them here.

POA&M considerations[1]

POA&M requirements differ by level, so be sure to understand which are applicable to you.

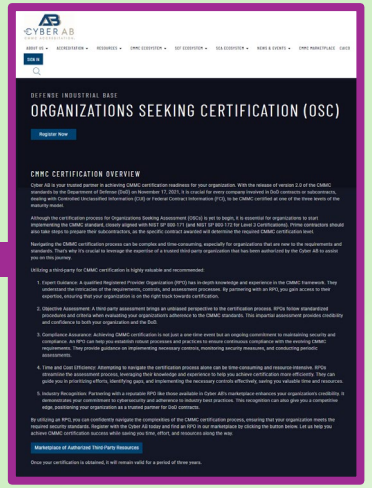
CMMC Status	Plan of Action & Milestones (POA&M) Requirements
Level 1 (Self)	• Not permitted
Level 2 (Self)	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for 3 years from the Conditional CMMC Status Date
Level 3 (C3PAO)	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for 3 years from the Conditional CMMC Status Date
Level 3 (DIBCAC)	• Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days • Final CMMC Status will be valid for 3 years from the Conditional CMMC Status Date

Supplier Performance Risk System (SPRS)[1]

SPRS is used to track contractor compliance—knowing how to use it is essential. Click here for a step-by-step guide.

Scheduling your C3PAO[2]

You're ready for an official C3PAO assessment. Now what? Click here for next steps.



Click here to learn more about CMMC and our CMMC services

CONTACT US

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

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

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

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

[1]DOD CIO – About CMMC, CIO - Cybersecurity Maturity Model Certification, October 9, 2025
[2]The Cyber AB – CMMC Ecosystem, Organizations Seeking Certification (OSC), October 9, 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