



Cybersecurity Maturity Model Certification (CMMC)

The final rule is here



The long-awaited **final rule** (32 CFR Part 170) for the CMMC program was published in the Federal Register on October 15, 2024, and will become effective December 16, 2024.¹ With this publication, organizations have accelerated their timelines for CMMC compliance and shifted resources and investment to uplifting their security posture in a short amount of time. The finalized rule introduced some slight changes that may impact how your organization prioritizes CMMC compliance initiatives.

NOTABLE TAKEAWAYS

- 1 Asset categories are assessed differently at Level 3 vs. Level 2**
For Level 3 assessments, contractor risk managed assets (CRMAs) are classified as Controlled Unclassified Information (CUI) assets and are assessed against the relevant security requirements.
- 2 Clarification around Level 3 control requirements**
Identified the 24 NIST SP 800-172 controls required for Level 3 certification (in addition to the 110 Level 2 controls). The DoD has also indicated that additional requirements may be added on a contract-by-contract basis.
Organization defined parameters (ODPs) requirements have been defined by the DoD to address the risk of inconsistencies across various DoD programs.
- 3 Not all requirements must initially be met for a contractor to be eligible for contract award**
If certain critical requirements are met and the minimum required score (80%) is achieved, a conditional status will be granted for a limited period.
Requirements scored as "Not Met" during an assessment must be placed on the POA&M and remediated within 180 days of the organization seeking assessment (OSA) receiving their Conditional CMMC Status. Proper closure must be validated during a second assessment ("POA&M Closeout Assessment").
- 4 External service providers (ESP)**
Contractors using an ESP (e.g., Cloud Service Provider (CSP) that handles CUI must confirm that the ESP meets the FEDRAMP Moderate Baseline or equivalent requirements.
- 5 Subcontractor flow-down requirements**
Clarification provided regarding minimum subcontractor flow-down requirements (e.g., a subcontractor supporting a prime contractor with a Level 2 (CMMC Third-Party Assessor Organization or "C3PAO") requirement also has a Level 2 (C3PAO) requirement.

Click [here](#) to learn more about our **CMMC services**.

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
kthompson@deloitte.com

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

¹Federal Register, [Cybersecurity Maturity Model Certification \(CMMC\) Program](#), October 15, 2024

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2024 Deloitte Development LLC. All rights reserved.