

CMMC Compliance Checklist

7 questions to Guide Your Journey

What is CMMC?

The cybersecurity maturity model certification (CMMC) was created to strengthen cybersecurity within the defense industrial base (DIB). It focuses on security controls for sensitive information in nonfederal systems processing Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Defense Industrial Base (DIB) contractors and subcontractors are required to achieve CMMC compliance.

The required CMMC compliance level (1,2 or 3) depends on the type of sensitive information handled, such FCI or CUI. Higher CMMC levels impose stricter cybersecurity controls, ensuring enhanced protection against cyber threats. CMMC compliance is required for maintaining Department of Defense (DoD) contract eligibility. CMMC 2.0 was finalized with the 32 CFR final rule becoming effective on December 16, 2024.



7 questions to guide your journey

While CMMC is not new, now that the final rule has been published, it has hit the radar of many organizations in the DIB. Maintaining eligibility for DoD contracts or pursuing new contracts is a critical business requirement. While CMMC details are spelled out well, you probably have questions about the process and the milestones along the way. The questions below will help guide and prepare you for the CMMC process from getting started through your certification by a certified third-party assessor organization (C3PAO) authorized by the Cyber-AB (Cybersecurity Maturity Model Certification Accreditation Body).



1. Do we need CMMC compliance and at what level?

DIB contractors and subcontractors that handle CUI will be required to meet the CMMC compliance requirements at one of three levels. Depending on the information that your organization handles, you may not be required to achieve CMMC compliance. If your firm handles FCI and non-critical CUI, you are only required to meet CMMC Level 1, foundational, requiring 15 requirements. If your organization is handling CUI, then CMMC level 2 - advanced is required. CMMC level 2 requires 110 requirements aligned with NIST SP 800-171. For organizations that handle highly sensitive DoD data, CMMC required level 3 -expert is needed. CMMC level 3 requires requirements based on NIST SP 800-171 and NIST SP 800-172 for advanced security.

If you are uncertain what type of information that your organization is handling, advisory firms can assist you with the early stages of determining what is required and a strategy for achieving CMMC compliance.

2. Do all our systems have to meet CMMC compliance requirements?

CMMC is intended to strengthen and ensure protection of DOD information handled by your organization. Since not all systems within your organization handle CUI, it is important to identify and document in scope and out of scope assets. This is a critical step to being determining what will fall under the CMMC requirements. Once this step is completed, determine the CUI dataflows and assets identified in your discovery to minimize the footprint that falls under CMMC requirements. This will not only ensure segmentation to protect DoD information, but also help you limit the scope of systems that must meet CMMC requirements. It is also important to review contracts and agreements with third party vendors to ensure any requirements for their control environments are also compliant.

If you are uncertain of the data flows handling CUI or system segmentation, advisory firms can assist you with analyzing the data flows and systems that would fall under CMMC compliance requirements.

3. What controls must our systems have in place for CMMC compliance?

Since CMMC Level 1 applies to organizations handling only FCI, the control requirements are less. The three key controls required are:

1. Implement the 17 basic cybersecurity practices based on FAR 52.204-21,
2. implement firewalls, strong passwords, and access controls, and
3. train employees on cybersecurity best practices.

CMMC Level 2 compliance is has more stringent controls due to the handling of CUI. Your organization will need to validate compliance with the level 2 requirements against your CUI boundary that you have identified. These requirements are 1) evaluate implementation of all 110 controls from NIST SP 800-171 and 320 assessment objectives identified in NIST SP 800-171, encrypt CUI data in storage and transit, restrict access to CUI using multi-factor authentication (MFA), and regularly audit security logs and incident response procedures.

If CMMC level 3 applies to your organization you are also required to 1) follow NIST SP 800-172 advanced security measures, implement continuous monitoring and risk mitigation strategies, and ensure proactive threat detection and response capabilities.

Firms with experience building systems for FedRAMP, NIST, and other compliance environments can help advise you on the controls required and necessary changes to your environment to prepare for CMMC compliance.

4. How will we know that we are ready to meet CMMC requirements?

Once your organization has taken the steps required to determine the appropriate CMMC level, identify CUI assets and data flow, and determined the scope for systems, a mock assessment will help determine if your organization's preparations are sufficient to meet the CMMC compliance requirements that will be required for CMMC certification. Firms with experience with CMMC certification experience can perform a mock assessment to help ensure that your preparation is complete and likely to result in a successful CMMC certification.

5. If we have shortcomings, do we start over? How do we proceed?

Achieving CMMC compliance is a journey. A mock assessment will help you identify gaps in your environment that require further changes. While some of these gaps may be simple and easily remediated, you should develop timelines and budgets for addressing more complex gaps such as replacing non-compliant 3rd party vendors. You should create plans of actions and milestones (POAMs) for anything in your environment that is not compliant and requires remediation. CMMC level 2 allows 180 days to address gaps. POAMs cannot be used for "high-weighted" security requirements—meaning some gaps must be remediated before certification.

6. How do we get officially certified for CMMC compliance?

CMMC level 1 only requires a self-assessment that your organization can perform without a third-party assessor. Your organization will attest to its compliance initially for level 1 and recertify annually. CMMC level 2 requires a third-party triennial assessment by a C3PAO and annual affirmation. CMMC level 3 requires a triennial government-led assessment with an annual affirmation.

7. When must we have CMMC certification?

The DoD released the CMMC final rule on December 16, 2024, making CMMC now enforceable. DoD will be requiring CMMC compliance in new and renewing contracts in 2025 with full implementation in 2026. To minimize jeopardizing new and existing DoD contracts, you should get started now on your efforts to develop a CMMC compliance plan, from early scoping efforts through certification by a C3PAO.



Whether you are just getting started on your CMMC journey or ready for certification and looking for a C3PAO, Coalfire can help. Coalfire provides CMMC compliance services to help your organization achieve certification, strengthen cybersecurity, and meet federal compliance standards. Our team ensures that you are fully prepared for CMMC assessments by guiding you through every step of the process.

With a proven track record in cybersecurity compliance and government security frameworks, Coalfire is your trusted partner for expert CMMC consulting and preparation, end-to-end guidance through certification, and building secure, compliant environments to support DoD contracts. Visit <https://coalfire.com/cmmc-certification> to get started.

