infor

HOW-TO GUIDE

Your guide to CMMC 2.0 compliance requirements

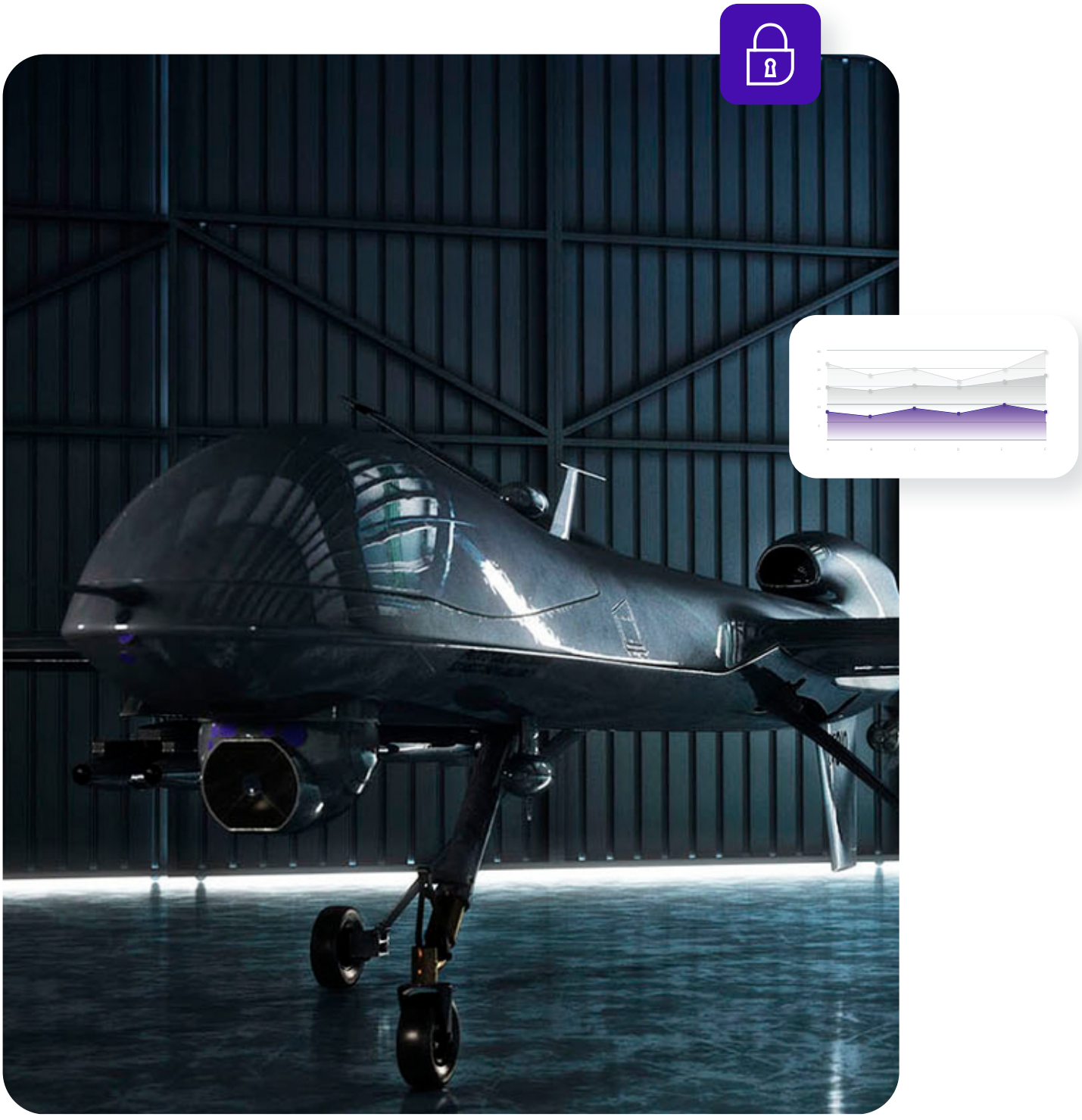

Table of contents

Introduction

The Department of Defense (DoD) developed the Cybersecurity Maturity Model Certification (CMMC) framework to protect the Defense Industrial Base (DIB) from adversarial intelligence collection efforts and corporate proprietary data theft that could compromise US national security. The framework is designed to ensure that defense contractors can meet the cybersecurity requirements built on the National Institute of Standards and Technology (NIST) 800-171 standards.

The DoD issued a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to mandate compliance with CMMC 2.0. As of November 10, 2025, CMMC requirements are included as award criteria in new contracts as well as when exercising option years for existing contracts.

Use the following guide to understand the key components of CMMC 2.0 and answer frequently asked questions about the CMMC 2.0 compliance requirements.

What is CMMC 2.0

The CMMC framework was created to protect the availability, confidentiality, and integrity of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) throughout the DoD's extensive contractor supply chain.

CMMC 2.0—an advancement of CMMC 1.0 based on input from stakeholders—was released in October 2024. The revised framework streamlines and simplifies the original one with the goal of increasing the accountability and uniformity of cybersecurity procedures for contractors operating within the DIB.

With the introduction of CMMC 2.0, the DoD is pursuing three objectives:

- Guaranteeing that suitable cybersecurity controls and procedures are in place
- Streamlining certification
- Lowering compliance obstacles and costs for smaller organizations

Effective since December 2024 (32 CFR Final Rule), the revised CMMC Program is characterized by a tiered model and its assessment requirements aligned to NIST SP 800-171, a set of cybersecurity requirements published by NIST, and a phased rollout.

Tiered Model: Businesses entrusted with FCI and CUI are required to implement the progressive cybersecurity standards mandated by CMMC. The program also explains the process for mandating information that is flowed down to subcontractors to be protected.

- The new model has been simplified to three maturity levels instead of the previous five.

Assessment Requirement: The DoD can confirm the use of precise cybersecurity standards through CMMC evaluations.

- Self-evaluation is sufficient for Level 1, but third-party assessment is required for Level 2, and the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessment is required for Level 3.

Phased Implementation: Certain DoD contractors handling FCI and CUI will need to reach a specific CMMC level as a requirement of contract award once CMMC regulations go into effect.

- CMMC 2.0 has a well-defined implementation schedule; the new requirements will be put into effect over a three-year period, utilizing a four-phase implementation plan.

Standard Alignment:

- Unlike the earlier program, CMMC 2.0 fully aligns with the controls set out in NIST SP 800-171 Revision 2.

Who needs CMMC

To be awarded contracts and for the continuance of contracts, all DoD contractors and subcontractors must have a current CMMC record in the DoD Supplier Performance Risk System (SPRS) for all information systems that process, store, or transmit FCI or CUI during contract performance.

DFARS mandates contractor compliance with the CMMC requirements at the specified level for contract award. Depending on the kind and level of sensitivity of the data that companies may receive, retain, and transmit, the DoD will determine which CMMC level will be applicable to a contract.

As CMMC 2.0 seeks to secure the entire defense supply chain, via the “flow-down” principle, DFARS clauses also apply to subcontractors, making contractors responsible for their enforcement.

- Prime contractors are companies that work directly with the DoD on defense-related contracts.
- Subcontractors are third-party businesses that supply prime contractors with goods or services.

Contractors and subcontractors must submit a current assessment of their compliance with SPRS prior to contract award.

Which CMMC level is relevant to your organization: Understanding FCI and CUI

CUI is information that needs to be protected and may also be subject to dissemination regulations, whereas FCI is any information that is “not intended for public release.” Title 32 CFR Part 2002 defines CUI, while FAR clause 52.204-21 defines FCI.

Federal Contract Information:

- Is provided by or generated for the US Government under a contract to develop or deliver a product or service to the Government
- Is not marked as public or for public release
- Examples of FCI can include communication and representation of knowledge, such as facts, data, or opinions in text, numerical, graphical, or audiovisual format

Controlled Unclassified Information:

- Is created or owned by the US Government or its partners
- Can be critical (CUI with prioritized acquisitions) or non-critical (CUI with non-prioritized acquisitions)—it depends on the specific information’s content, its relation to national security, economic interests, or individual privacy, and requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government policies to protect national security
- Is not classified under Executive Order 13526 or the Atomic Energy Act
- Is marked as CUI
- Examples of CUI include DoD personnel identifiable information, technical specifications for military equipment, critical infrastructure information, and contract performance data

What are the new CMMC levels in the revised CMMC 2.0 framework

The revised CMMC framework includes three levels for a progressive and simplified journey to cybersecurity maturity.

Each level is characterized by a set of cybersecurity best practices, standards, and processes as defined in NIST SP 800-171 Revision 2.

CMMC Level 1 (Foundational)

This level prioritizes safeguarding FCI. It mandates that an organization's systems and procedures adhere to 15 fundamental cybersecurity practices specified under 48 CFR 52.204-21, also known as the FAR clause. (See FAQ)

This level may be applicable to a subset of programs that need to meet CMMC Level 2 requirements, if CUI is not involved; however, it is only applicable when the organization does not receive or hold Controlled Unclassified Information.

CMMC Level 1 Assessment

A self-assessment conducted once a year is sufficient at Level 1. Organizations must score their assessment against DoD requirements and report the results to SPRS for the assessment to be considered valid.

The yearly submission of self-assessment results serves as an affirmation of continuous compliance.

CMMC Level 2 (Advanced)

The protection of CUI is the main focus of this level. At this level, organizations need to document their processes to guide their compliance efforts and follow them as prescribed.

CMMC Level 2 is often referred to as “advanced cyber-hygiene.” It requires the implementation of 110 practices, under the 14 domains (see FAQ), specified in NIST SP 800-171 Revision 2.

CMMC Level 2 (Advanced) Assessment

CMMC Level 2 requires certification and, therefore, third-party assessment, which must be carried out by Certified Third-Party Assessment Organizations (C3PAOs).

After initial certification, affirmation of continuous compliance must be made yearly by an organization official and posted to SPRS.

Three years after initial certification, a full reassessment must be carried out by a C3PAO.

Note: As of November 10, 2025, as part of the CMMC 2.0 rollout phase, new Level 2 contracts and option years now require self-assessments. Starting in November 2026, third-party assessments will be required.

CMMC Level 3 (Expert)

Concerned with protecting CUI from advanced persistent threats (APTs), this CUI level is also described as “High Value Assets.” CMMC Level 3 requires the implementation of 24 additional controls from NIST SP 800-172 enhanced standards related to greater cybersecurity risk management.

CMMC Level 3 Assessment

The certification is only conducted by the DoD via DIBCAC every three years.

As a prerequisite for this level, organizations must already be holding a valid Level 2 certification.

After initial certification, organizations certified at this level should follow the same process for affirmation of continuous compliance and reassessment as CMMC Level 2 certified organizations.

Note: Prime contractors and subcontractors may require different degrees of certification depending on their activities and the sensitivity of the information (flow down).

Once certified at a given NIST revision, organizations remain locked to that revision for the three-year certification cycle. Transition to future revisions (e.g., NIST 800-171 Revision 3) will require new rulemaking, and likely fresh Class deviations for both DFARS 7012 and the 32 CFR CMMC program.

The CMMC accreditation body is Cyber AB.

How to achieve CMMC 2.0 compliance

Achieving CMMC compliance and certification, especially Levels 2 and 3, takes significant time and resources and is a project that involves the entire organization.

Here is an overview of the steps that you need to follow:

1

Determine your organization's certification level

The certification level you need is driven by the type of information you handle—FCI or CUI.

2

Perform a gap analysis

Analyze your current cybersecurity procedures and compare them to the certification level requirements. What are the areas that need improvement to meet the requirements of the CMMC level you are aiming for?

3

Put the necessary procedures into action

To improve your cybersecurity posture, implement the procedures described in FAR 52.204-21 (Level 1) and NIST SP 800-171 (Level 2), or NIST SP 800-172 (Level 3).

4

Select a CMMC-certified C3PAO

To get Level 2 and Level 3 certifications, work with certified third-party assessment organizations (C3PAOs) or with government-led assessors (DIBCAC).

5

Maintain continuous improvement

Continuous cybersecurity excellence is emphasized in CMMC 2.0. To handle new risks, make sure you update and enhance your procedures on a regular basis.

If you are a contractor working with subcontractors, make sure you select subcontractors with a valid SPRS record and check their scores.

6

Conditional certification

Under the CMMC 2.0 final rule, and only in specific cases, organizations may achieve "conditional certification." In this scenario, CMMC Level 2 and CMMC Level 3 assessments identify the gaps preventing full certification. The corrective actions needed and the road map to close and achieve certification are formally outlined in a POA&M document.

Organizations must successfully implement the corrective action plan within 180 days to transition to full certification.

Cost and time

Achieving certification should typically take 6–18 months.

However, costs and time to achieve this vary depending on scope—i.e., volume of CUI and assets that store CUI, the CMMC Level aimed for, and an organization's cybersecurity maturity at the start of the process.

To enhance readiness and prepare your organization for certification, you can work with a CMMC Registered Provider Organization (RPO), authorized by the Cyber AB, or a C3PAO (which, in this case, cannot also be your certifying entity).

FAQ

What are the FAR 52.204-21 15 fundamental cybersecurity practices?

1. **Limit access to authorized users:** Only designated and authorized individuals should have access to information systems.
2. **Authenticate users:** Require users to prove their identity before granting access to systems.
3. **Limit connections:** Restrict connections to external information systems.
4. **Monitor system use:** Audit and log user and system activities to detect suspicious behavior.
5. **Limit physical access:** Secure access to the physical equipment, facilities, and operating environments of information systems.
6. **Escort visitors:** Supervise and monitor any non-employees within secure areas.
7. **Sanitize media:** Ensure media containing FCI is properly wiped or destroyed before disposal.
8. **Update software:** Install necessary patches and updates to protect against vulnerabilities.
9. **Whitelist software:** Control and restrict which software applications are allowed to run on the system.
10. **Scan for malware:** Use antivirus or endpoint detection and response (EDR) tools to scan systems for malicious code.
11. **Restrict information flow:** Prevent the unauthorized transfer of information from the system.
12. **Monitor communications:** Control and protect communications at the boundaries of the information systems.
13. **Dispose of devices properly:** Ensure media with FCI is destroyed correctly before being disposed of.
14. **Limit portable storage:** Restrict the use of portable storage devices like Universal Serial Buses (USBs) to prevent data loss and malware.
15. **Train staff:** Provide training to employees on handling FCI and following cybersecurity best practices.

What are the 14 domains of cybersecurity practices in the CMMC 2.0 framework?

NIST SP 800-171 Revision 2 establishes comprehensive guidelines for implementing and managing cybersecurity practices across an organization, organized in 14 domains, also referred to as the control families.

1. **Access Control (AC)**
   a. Limits and manages information systems access to authorized users
2. **Audit and Accountability (AU)**
   a. Ensures the availability and protection of systems audit information
3. **Awareness and Training (AT)**
   a. Mandates security awareness and training to respond to threats
4. **Configuration Management (CM)**
   a. Establishes, documents, and enforces processes and activities to configure and maintain organizational systems, including hardware, software, firmware, and documentation
5. **Identification and Authentication (IA)**
   a. Ensures appropriate and authorized access to an organization's systems and data
6. **Incident Response (IR)**
   a. Prepares for cybersecurity incidents, ensuring adequate response and effective mitigation
7. **Maintenance (MA)**
   a. Maintains systems securely
8. **Media Protection (MP)**
   a. Ensures information stored physically or digitally is protected from unauthorized access and exposure
9. **Personnel Security (PS)**
   a. Manages security risk linked to personnel
10. **Physical Protection (PE)**
    a. Protects physical locations and systems
11. **Risk Assessment (RA)**
    a. Assesses risks to systems, operations, and assets and determines how to remediate
12. **Security Assessment (CA)**
    a. Evaluates security controls and identifies vulnerabilities
13. **System and Communication Protection (SC)**
    a. Secures communications and data transmission from unauthorized access
14. **System and Information Integrity (SI)**
    a. Monitors and maintains systems to protect their integrity

What is the timeline for CMMC 2.0 implementation?

The DoD has outlined a clear timeline for the implementation of CMMC 2.0:

- **November 2021:** Announcement of CMMC 2.0.
- **2022–2023:** Rulemaking process and stakeholder consultations.
- **2024:** The 32 CFR CMMC final rule was officially published on October 15, 2024, thereby making the revised CMMC a binding federal regulation. The final rule defines the program, as well as the ecosystem of third-party assessment organizations (C3PAOs), their credentialing authority (Cyber AB), and the certification assessment process (CAP). The 32 CFR CMMC was approved by Congress on December 16, 2024.
- **2025** Full transition—the 48 CFR CMMC final rule was published on September 10 in the US Federal Register, amending DFARS, to mandate compliance with the final CMMC 2.0 requirements program rule as a prerequisite to DoD contracts' eligibility.
- **A four-phase implementation of the program is planned over 36 months.**

Organizations should use this timeline to prepare for compliance, ensuring that necessary cybersecurity measures are in place before the final rollout.

About Infor

Infor is a global leader in business cloud software products for companies in industry-specific markets. Infor builds complete industry suites in the cloud and efficiently deploys technology that puts the user experience first, leverages data science, and integrates easily into existing systems. Over 67,000 organizations worldwide rely on Infor to help overcome market disruptions and achieve business-wide digital transformation.

infor.com

Support business transformation and compliance requirements in a CMMC 2.0-ready environment

LEARN MORE

infor