# CMMC 2.0: What You Need to Know and How It Compares to Your Current Practices

On October 15, 2024, the CMMC Final Rule was published in the Federal Register, effectively making CMMC 2.0 the law. While requirements for CMMC certification will not show up in federal contracts until early 2025, the preparation for and successfully completing an audit could take companies many months to complete.

Not sure if the rule applies to your business? Here's a guide to understanding how CMMC applies to companies, what compliance entails, and what steps (if anything) you need to take right now.

## WHY THE SHIFT TO CMMC 2.0?

The Cybersecurity Maturity Model Certification (CMMC) was developed to help contractors working with the Department of Defense (DOD) effectively safeguard Federal Contact Information (FCI) and Controlled Unclassified Information (CUI).

CMMC 2.0 aims to streamline this process. For example, while CMMC 1.0 had five maturity levels, CMMC 2.0 has just three. Additionally, the new iteration aligns with well-known security standards published by the National Institute of Standards and Technology (NIST), such as NIST Special Publication (SP) 800-171 and NIST SP 800-172.

## WHO NEEDS TO COMPLY WITH CMMC 2.0?

Any company that works with the DOD and handles FCI or CUI must comply with CMMC 2.0. Understanding whether these requirements apply to your organization involves assessing a few key criteria.

### HANDLING FCI

According to the National Archives and Records Administration (NARA) Information Security Oversight Office (ISOO), FCI is any information not intended for public release that is provided by or generated for the government to develop a product or deliver a service.

For example, if your company manufactures airplane fuselages and receives specifications from the DOD or develops specifications for a government project, this data is classified as FCI, and you must achieve at least CMMC Level 1 certification.

### HANDLING CUI

CUI includes any information that the government creates or possesses or that an entity creates or possesses for the government, which is governed by law or regulation that requires the use of security controls.

Examples of CUI include technical specifications, personnel data, or protected health information. If your business handles CUI as part of a DOD contract, CMMC 2.0 requires you to achieve Level 2 or Level 3 certification, depending on the sensitivity of the data.

## WHEN WILL CMMC 2.0 COME INTO FORCE?

The CMMC 2.0 final rule was published on October 15, 2024, effectively making CMMC the law regarding protecting of the information communicated or stored in relation to DOD contracts. The next step is the publishing of the acquisition rule, also known as the DFARS rule. Comments closed on the DFARS rule on October 15, 2024, and it is estimated that it will be published in the first half of 2025. This marks the beginning of a phased implementation. Here's what you need to know about the timeline:

1

**PHASE 1**
*begins 60 days after publishing of the DFARS final rule*

All new solicitations for DOD contracts will require either Level 1 or Level 2 self-assessments.

2

**PHASE 2**
*12 months later*
All applicable contract solicitations will require Level 2 certification.

3

**PHASE 3**
*24 months later*
All applicable contract solicitations will need to include Level 3 certification.

4

**PHASE 4**
*36 months later*
At this stage, all solicitations and contracts must provide evidence of the appropriate CMMC level for handling FCI or CUI.

While this means that three years will pass before CMMC 2.0 regulations are fully in effect, it's wise for businesses that handle FCI or CUI (or plan to bid on any future DOD contracts) to prepare for CMMC compliance now. This early-adopter approach offers several benefits:

- **Demonstrate industry leadership:** Proactively achieving compliance can boost credibility and attract new business opportunities.
- **Reduce stress closer to deadlines:** By getting ahead of the curve, companies can avoid last-minute scrambles as each phase takes effect.
- **Adapt to CMMC updates:** Early adopters can adjust more smoothly to any changes or updates to CMMC 2.0 as they arise.


## WHAT ARE THE CMMC 2.0 CORE REQUIREMENTS?

As noted above, CMMC 2.0 consists of three levels, each with specific requirements based on the type of information handled:

**Level 1** *Foundational*
Required for DOD contracts that involve the use of or access to FCI.

**Level 2** *Advanced*
Required for DOD contracts that handle CUI.

**Level 3** *Expert*
Required for DOD contracts that handle sensitive or critical CUI.

## HOW DO YOU ENSURE YOU'RE READY FOR CMMC 2.0?

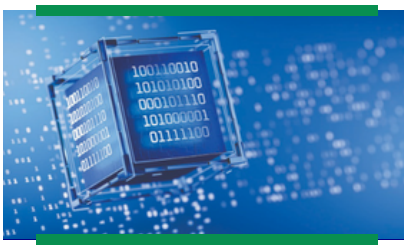
Getting ready for CMMC 2.0 starts with assessing how your existing cybersecurity practices stack up against CMMC 2.0 requirements. While many companies already implement basic cybersecurity measures, like regular software updates and data encryption, CMMC 2.0 introduces more structured and rigorous expectations.


### LEVEL ONE

This level involves basic cybersecurity practices, such as patching and updating security tools, ensuring that passwords are regularly changed, and encrypting sensitive data.

### LEVEL TWO

Meeting this level means implementing more sophisticated solutions, such as access control and incident response. In practice, this might entail deploying zero- trust network access (ZTNA) policies and creating well-documented and regularly updated incident response plans.



### LEVEL THREE

This level involves advanced strategies like data recovery planning and system hardening. This may take the form of cloud-based backups and the use of behavior-based cybersecurity solutions capable of detecting suspicious behavior and taking prescriptive action.

## IDENTIFYING GAPS IN YOUR CYBERSECURITY

While many companies might already have strong cybersecurity foundations, gaps often exist in the details. For example:

- **Access control:** Companies may limit access to sensitive information, but they may lack granular tools capable of permitting access on a per-user and per-use-case basis.
- **Credential management:** While user passwords may be regularly updated, companies may overlook the credentials for connected devices like routers and IoT sensors, which often go unchang from factory settings, putting them at risk of compromise.

To make sure you're ready for CMMC 2.0, consider conducting an in-house or third-party security audit. The more you know about your current security posture, the better prepared you are to make changes that align with NIST security guidelines—and, in turn, meet CMMC 2.0 standards.

## MAKING THE MOVE TO CMMC 2.0

If your company does business or plans to do business with the DOD, CMMC 2.0 compliance is a must. The best approach? Don't panic. Instead, use the established security guidelines of NIST SP 800-171 and NIST SP 800-172 as a roadmap for meeting CMMC compliance requirements.

Need help streamlining the compliance process and positioning your business for future contract solicitations?

Contact AB Advisory Dynamics today for expert guidance.