CYBERSHEATH

CMMC 2.0 Guide

Discover Requirements, Best Practices & the Assessment Process for Cybersecurity Maturity Model Certification

In order to be able to meet CMMC 2.0 (Cybersecurity Maturity Model Certification) requirements and continue to bid on and secure federal contracts with the Department of Defense (DOD), it's critical that your organization have a thorough understanding of the mandate.

This CMMC 2.0 Guide provides basic knowledge about the purpose and structure of CMMC 2.0. It also includes implementation support, best practice recommendations, answers to frequently asked questions, and more.

CMMC 2.0 Explained

CMMC is a framework established by the DOD to ensure that defense contractors and subcontractors implement adequate cybersecurity practices to protect sensitive information and avoid data breaches. Organizations in the defense industrial base (DIB) that handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) are under its purview.

This mandate outlines how the defense supply chain should protect sensitive defense information. It standardizes cybersecurity requirements across the DIB and establishes a verification process. Compliance is mandatory for companies seeking to participate in DOD contracts.

CMMC 2.0 incorporates various aspects of cybersecurity including technical measures as well as legal, governance, and broader business considerations.

CMMC 2.0 History & Evolution

Before CMMC, contractors self-attested to implementing required security measures under NIST SP 800-171. Multiple high-profile cyber incidents revealed that this system was not effective in protecting CUI. The DOD initially developed CMMC in response to these growing cybersecurity threats targeting contractors in the defense industry supply chain.

CMMC 1.0 was published in September 2020 as a five-level certification model. After receiving industry feedback, the DOD revised the framework and CMMC 2.0 was launched in November 2021. The new version simplified the model to three levels and aligned it more closely with NIST standards.

The program continues to evolve with ongoing implementation efforts. Organizations are adapting their cybersecurity practices to meet these new requirements.

CMMC 2.0 Levels

After you've familiarized yourself with CMMC, it's time to dive in and get started. One of the first steps is to determine which level of the mandate applies to your organization. When considering certification, it's important to align with the level that matches your organizational intent and the sensitivity of the information you handle. For instance, if your organization anticipates engaging with Controlled Unclassified Information (CUI) datasets, then it is prudent to aim for CMMC Level 2 certification. Although the contract may dictate the necessary level, aligning your cybersecurity posture with your operational intentions ensures robust protection and compliance.
Simply stated, your contract dictates which CMMC level you need to meet.

A review of the three tiers shows that each level builds upon the security requirements of the previous level and assessment requirements become progressively more stringent as you advance from Level 1 to Level 3. Different levels allow your organization to meet security requirements based on the sensitivity of information you handle.

	Overview	**Assessment Requirements**
Level 1: Foundational *Purpose:* Protection of FCI *Focus:* Basic cyber hygiene practices	This entry-level certification is required for all companies that handle FCI. This level outlines 17 cybersecurity practices drawn from the FAR 52.204-21 and NIST SP 800-171. Basic access controls, identity authentication, physical controls, and anti-malware are key components of Level 1 protections.	Requires annual self-assessment
Level 2: Advanced *Purpose:* Protection of FCI and CUI *Focus:* Intermediate cyber hygiene aligned with NIST SP 800-171	This level includes 110 security requirements within 14 control families and 320 assessment objectives aligned with NIST SP 800-171. These practices include System Security Plan (SSP) development, access control implementation, and regular cybersecurity best practice training for employees. The certification process involves a review by a CMMC Certified Assessment Organization (C3PAO), who will verify that the company has implemented the required cybersecurity practices. Level 2 requires a lot of documentation - and it includes technical and administrative controls.	Requires third-party assessment
Level 3: Expert	This highest level is required for companies that handle CUI deemed the highest priority by the DOD. It builds upon the	

Purpose: Protection of FCI and CUI *Focus:* Controls commensurate with the highest level of security	110 security requirements from Level 2 and incorporates additional protections from NIST SP 800-172 to defend against advanced persistent threats (APTs).	Requires government-led assessment

How to Implement CMMC 2.0 Controls

As you work to continue toward achieving compliance with NIST 800-171 and meeting CMMC 2.0 requirements, there are tools and approaches that support your journey. Compliance with CMMC is required today, so it's important that your company take action now.

At CyberSheath we have developed the AIM approach to assess your current state and tailor a solution to help you gain full compliance.

Assess current operations for compliance

Start with a gap assessment of your current people, process, and technology against compliance with NIST 800-171. When done correctly, an assessment will directly link to Control 3.12.1 of NIST 800-171 which requires that you "periodically assess the security controls in organizational systems to determine if the controls are effective in their application." It also gives you a clear view of your current compliance with all 110 requirements and lays the foundation for you to generate an SSP and associated Plans of Action and Milestones (POA&M), both of which are NIST 800-171 requirements.

Implement the required controls

Your POA&Ms are your path to compliance. Executing them will probably be a full-time effort. Bear in mind that implementing the requirements will likely be the most resource intensive phase as it is a hands-on technical effort. We advise dedicating a team to the effort and having a project manager track progress. Don't forget that you must flow DFARS/NIST 800-171 down to your subcontractors.

Manage compliance

Once you have implemented all of the controls, you need to plan for ongoing compliance in a way that meets the requirements as your business grows. Be sure to document and automate reporting and plan for ongoing operational expenses related to maintaining compliance. Modify existing managed services contracts to reflect compliance requirements and update your SSP, periodically, as required.

Keep in mind that full compliance is documented, repeatable, and scalable, and it incorporates shared responsibility, continuous compliance, and integrated people,

processes, and technology. As your company pursues its compliance goals, remember that NIST and CMMC compliance can be pursued in parallel for protecting CUI. Use our AIM process to bring order to the chaos. Following a documented, scalable, and repeatable process grounded in actual requirements will guide you to compliance.

CMMC 2.0 Best Practices

Here are recommended actions to take as you work toward CMMC compliance.

Know the controls.

NIST 800-171 provides the framework for securing CUI within non-federal systems and organizations. It includes 14 control families with a total of 110 requirements and 320 objectives, addressing both technical and non-technical aspects of security. Meeting these controls requires thorough and precise documentation.

Control Family	Number of Controls
Access Control	22
Awareness and Training	3
Audit and Accountability	9
Configuration Management	9
Identification and Authentication	11
Incident Response	3
Maintenance	6
Media Protection	9
Personnel Security	2
Physical Protection	6
Risk Assessment	3
Security Assessment	4
System and Communications Protection	16
System and Information Integrity	7

Keep in mind that documentation is key.

You need to implement the controls defensibly either with evidence or demonstration that shows that you are truly doing the things that you say you're doing. For the most part, during certification assessors are collecting assertions from practitioners. The people who do the work are showing what they're doing or providing artifacts to confirm compliance.

Use the AIM approach to implement control and maintain compliance.

Assess	Assess existing infrastructure and generate a detailed report of what is needed.	Step 1: Assess for compliance with NIST 800-171.
		Step 2: Generate your SSP.
Implement	Implement all elements - write all policies, plans, and time frames; install all technical controls - required for compliance.	Step 3: Document POA&Ms.
		Step 4: Implement security requirements.
Manage	Continuously collect, review, and preserve evidence of your ongoing compliance. Remediate compliance gaps as you find them.	Step 5: Maintain compliance.

Use a CMMC-certified Managed Service Provider (MSP).

If your service provider is CMMC-certified and you are leveraging those certified managed services, that can help in expediting your assessment because you have a certified entity that is part of your boundary. Be sure to have a shared responsibility matrix in place that accurately reflects what you and your MSP are responsible for. If the service provider is accountable for a particular component of your compliance, they're going to get assessed in some cases as if they were staff.

Maintain ongoing CMMC 2.0 compliance.

Compliance is not an end-state, and it doesn't end with certification. Regularly manage and monitor your environment to ensure ongoing adherence to CMMC requirements. This includes routine audits, patch management, change control, and operational security. Staying compliant ensures long-term success and audit readiness.

Know and manage your CUI and FCI.

Gain a good handle on what CUI is and how it flows in your organization. Configure strong, defensible CUI flow controls as the assessor will ask how the data flow occurs, how you are engaging with the environment, and if and how users have the ability to move the data.

Be aware that protecting sensitive information starts with understanding the various information categories. The next step is being able to map the information your company holds to the contracting regulations you must adhere to. Information types include:

- FCI - Non-public information associated with a federal contract. CMMC offers this description, “FCI means information provided by or generated for the Government under a contract not intended for public release.”
- CUI - Established by Executive Order 13556 as a way to standardize how to handle sensitive but unclassified information. According to this order, “CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.”

Consider an enclave approach.

When built using CyberSheath’s process, an enclave is a fully NIST/DFARS/CMMC-compliant repository that segregates DOD project data from legacy systems. It acts as a safe deposit box for project-related information that’s secured, managed, and maintained by a U.S.-based managed security service provider (MSSP) 24/7/365.

Any company that is a member of the defense industrial base needs to identify and secure its CUI. An enclave is one way to address this requirement.

Prepare for your assessment—and then prepare more.

Preparation is key in having a good outcome for your C3PAO assessment. Make sure your documentation is complete and uses clear language and that all personnel and partners know their role and responsibilities.

We spend significant time preparing clients for certification, both technically, and administratively with documentation, to ensure clear demonstratable maturity for their C3PAO assessment. In the end, clear, concise, and practical wins to achieve that certifiable score.

Use a customer responsibility matrix.

We’ve found a customer responsibility matrix that defines responsibilities and depicts which party was responsible for each control is an important tool in CMMC assessments. This tool outlines a clear and obvious separation of duties between your company and any services provider you engage with.

CMMC compliance mistakes

Achieving CMMC compliance is a complex and challenging process for many organizations. Despite their best efforts, companies often encounter common pitfalls that hinder their progress. Identifying and understanding these frequent mistakes can help your organization avoid similar issues and streamline your path to certification. Here, we delve into some of the most prevalent CMMC compliance mistakes, starting with documentation issues and moving on to implementation errors and poor process management.

Documentation issues

One of the most common issues companies face is in terms of inadequate documentation of security controls and practices, including not maintaining evidence of control implementation. When we engage with a company to assess their CMMC readiness, what we generally find is most companies have very little documentation around what they're doing and how they're governing their security controls.

Lack of internal resources can make formulating the appropriate documentation a challenge. Often, the hard part is going through your records and aligning policies and procedures with your unique organizational practices. Know that what are considered best practices might not necessarily translate to being applicable to your business. Document your processes and include artifacts underscoring your compliance.

Implementation errors

Many companies also fail to meet all required controls for their designated level with inconsistent application of security practices or perhaps failing to regularly update security measures.

Two areas of particular concern include lack of multi-factor authentication (MFA) and shared accounts. We've discovered that many companies either have MFA partially applied or not applied at all. Meaning maybe these entities are using Microsoft 365 and have activated MFA for when they're logging into that environment. That is not sufficient. Part of the requirement is you need to have multifactor turned on even when you are logging on locally.

In terms of shared accounts, perhaps your IT group has one generic, admin user ID with a shared password. While this ID is only assigned to IT, it could be leveraged by multiple people. This practice creates an accountability issue because it becomes difficult to identify exact users. It's also relatively common for companies to mistakenly or intentionally provision users accounts that grant individual workers outside of management with admin access.

Poor process management

These types of compliance mistakes can be related to poor preparation for a company's third-party assessment for CMMC 2.0 Level 2 compliance, lack of staff training on cybersecurity practices, and not maintaining continuous monitoring of security controls. Effective process management is pivotal in CMMC compliance. It's not enough to merely document policies and procedures; they must be actively and consistently implemented in day-to-day operations. This means ensuring that all team members are trained, aware of, and following these guidelines, as well as regularly reviewing and updating processes to reflect any changes in the compliance landscape or organizational structure.

It's critical that your company prioritize CMMC readiness and know the actions that need to be undertaken from an organizational perspective to meet the various control requirements.

Organizational issues

Some organizational issues that arise could be not understanding which CMMC level applies to your organization, failing to allocate sufficient resources for compliance, and not involving leadership in compliance efforts. Critically important to understand, CMMC compliance is not solely an IT issue. The individuals who engage with Controlled Unclassified Information (CUI), including program staff, engineers, other functions like HR, Facilities, Business Development, and Contracts departments, are all involved in the process. If IT is expected to bear the responsibility, it is crucial that there is executive involvement to drive cross-functional support. Without this holistic approach, the efforts to achieve the necessary cybersecurity standards may be fragmented and ineffective.

Making sure your organization is in alignment at the start of the CMMC compliance process is important, otherwise efforts to achieve the necessary cybersecurity stature could be haphazard and compromised.

How to Prepare for a CMMC 2.0 Assessment

CMMC readiness checklist

CMMC Level 2 is required for handling CUI.

Identify which CMMC level (1, 2, or 3) applies to your organization based on the type of information you handle. Review your DOD contracts to understand specific requirements.

Conduct an assessment and enter the result into the Supplier Performance Risk System (SPRS).

Perform a comprehensive assessment to see where you are in terms of compliance with the 110 required controls of CMMC 2.0. This aligns with Step 1 on the AIM process outlined above. After you have completed your assessment, you need to score it and then log that information with the DOD via SPRS.

The SPRS scoring system ranges from a positive 110, if you're fully compliant, to negative 203, if your organization has done nothing in terms of cybersecurity controls implementation. Contracting Officers access SPRS and verify that each contractor has an assessment on record. If you are a prime contractor, you should consider implementing Supply Chain Risk Management processes to verify that your subs have done their SPRS submission.

SPRS scores determine contractor eligibility.

SPRS is a government website–and entering your score is rather like submitting your taxes. As part of your submittal you attest to the date that you have completed your assessment, as well as your score.

An important thing to keep in mind is that by entering your score, your company is committing to a path toward full compliance. In fact, there's a field for your plan of action completion date. Perhaps your score is negative 125, which is not uncommon. The government wants to know and wants you to attest to a date when your plan of action and milestones is going to be complete.

Make sure all the controls are implemented and documentation is in place.

Verify with confidence, rigor, evidence, or at least direct observations, that you are fully compliant with all 110 controls of CMMC 2.0 and that you have the required documentation in place to confirm your status.

Documentation requirements include:

- **System Security Plan (SSP)** - A comprehensive document describing the system environment, security requirements, and implementation status of all controls.
- **Policies and procedures documentation** - Written policies and detailed procedures for all required domains, including Access Control, Incident Response, Risk Assessment, and others.
- **Asset inventory** - Up-to-date, documented inventory of all hardware, software, cloud services, and data assets in scope for CMMC.
- **Access control records** - Documents showing user access privileges, role assignments, and account management processes.
- **Risk assessment reports** - Records of periodic risk assessments, findings, and risk mitigation strategies.
- **Incident Response Plan** - Formalized plan detailing how to respond to cybersecurity incidents, plus incident logs and after-action reports.
- **Security training records** - Documentation that staff have completed cybersecurity training required by CMMC.
- **Configuration management documentation** - Change management procedures, system configurations, approved baseline configurations, and patch management tracking.
- **Audit logs and monitoring records** - Saved logs and evidence of log review/monitoring activities.
- **Physical security documentation** - Evidence of facility access controls and monitoring.
- **Continuous monitoring plan** - Maintenance logs, vulnerability scan results, and mitigation evidence.
- **POA&M** - Active tracker for deficiencies with planned corrective actions and completion dates.
- **Third-party compliance management** - Documentation of third-party risk assessment and contracting controls (especially regarding data access and security expectations).

- **Data protection and media handling** - Procedures and records for handling, storing, and destroying sensitive media and data.
- **Security assessment reports** - Results of security assessments, penetration tests, or vulnerability scans.

Conduct pre-assessment preparation.

Self-assess your organization using the CMMC assessment guide and then implement any necessary controls and remediate any identified gaps. Review and finalize required documentation such as your SSP, POA&M, and Policy and Procedures. Make sure that everything is up to date, well-written, and easy for an assessor to understand.

CMMC Assessment Process

CMMC 2.0 self-assessment requirements

For CMMC Level 1 (Foundational), which focuses on protecting FCI, an annual self-assessment is required, where a company must demonstrate basic cyber hygiene practices. This process includes an organization:

- Documenting their compliance with security practices.
- Asserting compliance through an annual affirmation.
- Maintaining evidence of security control implementation.
- Reporting of self-assessment scores to the DOD.

For CMMC Levels 2 and 3, self-assessment revolves around demonstrating compliance with NIST 800-171 Rev 2 as a means of starting your process. This involves conducting a comprehensive assessment of your company's cybersecurity posture, identifying any gaps, and developing a plan to address them.

This self-assessment is initially used to determine compliance, and then a formal certification assessment is required. The results of the self-assessment are submitted to SPRS as discussed above.

Third-party assessment process

Following the initial self-assessment and score entered into SPRS, higher levels (Level 2 and 3) require third-party or government-led assessments rather than self-assessments to verify compliance. CMMC ultimately sees contracts involving CUI requiring a CMMC Level 2 third-party certification.

- **Engage a Certified Third-Party Assessment Organization (C3PAO).** Coordinate with third parties and service providers and communicate that you are ready for an assessment. Then select a C3PAO from the list of authorized organizations on the

Cyber-AB Marketplace and contact the chosen C3PAO to discuss your organization's specific needs and schedule an assessment. You can schedule a scoping call with them to ask questions about the process as relates to your assessment. Review your documentation and your processes to see if you're ready to schedule that assessment.

- **Get a formal assessment.** The C3PAO then performs an on-site or remote assessment. Assessors will review your cybersecurity practices, processes, and documentation—and they're going to look to you to demonstrate your processes and compliance. The assessment will verify compliance with the required CMMC level.
- **Achieve certification.** The C3PAO submits the assessment report to the DOD. If satisfactory, you will be granted a CMMC Certification.

CMMC certification lasts three years.
Once you successfully go through your assessment and receive your CMMC Level 2 certificate, that means that you will be good for three years. In the in-between years you will have to conduct your self-assessment in accordance with NIST 800-171 control 3.12.1. This is where the annual affirmation requirement comes into play where a senior company official will go into SPRS and make an annual affirmation to the government that your company is maintaining compliance throughout that three-year lifecycle.

CMMC FAQs

1. **What is CMMC 2.0?**
   CMMC stands for Cybersecurity Maturity Model Certification. It is a unified standard for implementing cybersecurity across the DIB, intended to protect CUI.

2. **Who needs to be CMMC certified?**
   Any organization that does business with the U.S. DOD and handles CUI must obtain a CMMC certification at the required level for their contracts.

3. **How many levels does CMMC 2.0 have?**
   CMMC 2.0 has three levels, ranging from basic cyber hygiene to advanced/progressive practices. Each level requires organizations to meet progressively more rigorous security requirements.

4. **What is CUI?**
   CUI stands for Controlled Unclassified Information. It refers to sensitive information that the U.S. government creates or possesses, or that an entity receives or develops for or on behalf of the government, that requires safeguarding or

dissemination controls according to laws, regulations, or government-wide policies.

CUI is not classified at the level of "confidential," "secret," or "top secret," but it is still considered sensitive and must be protected appropriately—especially in contexts like defense contracts, where mishandling CUI can pose security risks and jeopardize compliance with the CMMC framework.

Examples of CUI can include:

- Technical drawings or specifications
- Export-controlled data
- Financial data involving government contracts

The proper handling, marking, and protection of CUI is a core requirement in U.S. federal contracts, particularly for organizations supporting the DOD and other federal agencies.

5. How do I determine which CMMC level my organization needs?

The required level is specified in DOD contracts and depends on the sensitivity of the information you might access or process. Most organizations will fall into Level 1 (Foundational) or Level 2 (Advanced).

6. How do organizations get certified?

Certification is obtained through an independent third-party assessment by a certified C3PAO.

7. How long is CMMC certification valid?

Certification is generally valid for three years, after which a reassessment is required to maintain compliance.

8. What are some key requirements for CMMC Level 2 (Advanced)?

Level 2 includes the implementation of NIST SP 800-171 controls, covering areas such as access control, incident response, risk management, and system maintenance.

9. What is the timeline for CMMC requirements in contracts?

The CMMC 2.0 rule is currently under review by the Office of Information and Regulatory Affairs (OIRA), with publication of the final 48 CFR rule expected by October 2025. At that point, CMMC language will begin appearing in new DOD contracts. Contractors will be required to attest to full compliance with CMMC Level 2 in the Supplier Performance Risk System (SPRS) to meet contract award requirements. Based on the DOD's published phased rollout, certification by a C3PAO is expected to become mandatory by October 2026.

10. What are C3PAOs?

Certified third-party assessment organizations or C3PAOs are authorized to certify an organization for compliance with CMMC. They perform pass/fail assessment only and focus on certification quality.

11. What happens if my organization fails a CMMC assessment?

If your organization does not meet the required CMMC level during an assessment, you will receive a report outlining the deficiencies. You'll need to address these gaps and undergo a reassessment before you can bid on or participate in contracts that require CMMC certification. It's important to proactively remediate issues to avoid delays in contract eligibility.

12. How do I get started?

The first steps include understanding CMMC requirements and assessing your company's current cybersecurity practices against them. If you need assistance, give us a call, we are the CMMC experts and we are here to help.

Resources

These resources offer official templates, assessment tools, and actionable documents that you can use as part of your journey to CMMC certification.

- NIST SP 800-171A Rev. 3 (https://csrc.nist.gov/pubs/sp/800/171/a/r3/final) – Includes link to PDF with full document.
- Office of the DOD CIO – CMMC (https://dodcio.defense.gov/CMMC/) – Official CMMC documentation, process guides, Level 1 self-assessment templates, assessment guides, and scoping guidance directly from the Department of Defense.
- Cyber AB, CMMC Accreditation Body (https://cyberab.org/Resources/Downloads) – Consolidated links to the final CMMC rule, assessment process, and more.
- National Archives CUI Toolkit (https://www.archives.gov/cui/training.html) – Training modules, marking guides, and checklists for CUI, a critical focus area within CMMC.