CYBERSHEATH

CMMC Level 1 Guide

Learn about the requirements that protect Federal Contract Information (FCI), as well as the self-assessment process, best practices, and more.

CMMC Level 1 Explained

If your company touches Federal Contract Information (FCI) under a DOD contract, CMMC Level 1 applies to you.

Level 1 is the entry point into the Cybersecurity Maturity Model Certification framework, and it covers every organization in the defense industrial base (DIB) that handles FCI. It is a standalone requirement with its own compliance obligations, its own self-assessment process, and its own consequences if ignored.

CMMC Level 1 is already in effect. The 48 CFR DFARS CMMC Final Rule took effect November 10, 2025. If your contract includes FCI, your compliance requirement isn't coming—it's here.

What Is Federal Contract Information (FCI)?

FCI is information not intended for public release that is provided by or generated for the government under a contract. It is different from Controlled Unclassified Information (CUI), which triggers the more demanding CMMC Level 2 requirements.

If you are doing work under a DOD contract and producing things the general public isn't supposed to see, you're probably handling FCI. Common examples include:

- Contract deliverables and work products created for a DOD program
- Internal project communications, reports, or data generated in performance of a DOD contract
- Technical documentation produced under contract that has not been cleared for public release

Understanding what FCI you handle, and where it lives in your systems, is the starting point for Level 1 compliance. You cannot protect what you have not identified.

The 17 Foundational Practices

CMMC Level 1 is built on 17 cybersecurity practices drawn from FAR 52.204-21 and NIST SP 800-171, organized across six control families. They cover the basics: who gets into your systems, how you verify who they are, what happens to old media, how your physical space is controlled, how your network is protected, and how you keep malware out.

These are required controls, and during a self-assessment you will need to demonstrate that each one is implemented and operating as intended.

Access Control (AC)

Access control is about making sure only the right people can get into your systems, and that once they're in, they can only do what they're supposed to do. This means maintaining an active list of authorized users, removing access when people leave or change roles, and making sure your public-facing systems don't expose FCI.

Practice ID	Requirement
AC.L1-3.1.1	Limit system access to authorized users only.
AC.L1-3.1.2	Limit system access to the types of transactions/functions authorized users are permitted to execute.
AC.L1-3.1.20	Verify and control connections to external systems.
AC.L1-3.1.224	Control information posted or processed on publicly accessible information systems.

Identification & Authentication (IA)

Every user, device, or process accessing a system that stores or processes FCI must have a unique identity. Shared accounts with a single login used by multiple people, or devices or process accounts that are not easily identifiable, create accountability gaps that are difficult to defend during an assessment and genuinely problematic if a security incident occurs. If your team is sharing logins, you will need to address that.

Practice ID	Requirement
IA.L1-3.5.1	Identify system users, processes acting on behalf of users, or devices.
IA.L1-3.5.2	Authenticate (verify) the identities of users, processes, and devices, as a prerequisite to allowing access to organizational systems.

Media Protection (MP)

When a hard drive, USB drive, laptop, or other media that has held FCI is being retired, repurposed, or disposed of, that media must be sanitized or destroyed. Handing an old laptop to an employee without wiping it, or dropping a hard drive in a recycling bin, does not meet this requirement.

Practice ID	Requirement
MP.L1-3.8.3	Sanitize or destroy system media containing FCI before disposal or reuse.

Physical Protection (PE)

Physical security is part of cybersecurity. Server rooms, workstations, and areas where FCI is accessed or processed need to be physically controlled. This does not require a sophisticated access control system. What matters is that access is limited to authorized individuals and that you can demonstrate that in your documentation.

Practice ID	Requirement
PE.L1-3.10.1	Limit physical access to systems, equipment, and operating environments to authorized individuals.
PE.L1-3.10.3	Escort visitors and monitor visitor activity.
PE.L1-3.10.4	Maintain audit logs of physical access.
PE.L1-3.10.5	Control and manage physical access devices.

System & Communications Protection (SC)

Your network needs a defined, defensible perimeter. Traffic entering and leaving your network, particularly where it connects to the internet, should be monitored and controlled. This typically means a firewall at your network boundary, with rules that have been reviewed and are being actively managed. Implementing subnetworks for publicly accessible components, like guest WiFi, is also important to ensure FCI is only accessible by authorized personnel and devices.

Practice ID	Requirement
SC.L1-3.13.1	Monitor, control, and protect organizational communications at external boundaries and key internal boundaries.
SC.L1-3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

System & Information Integrity (SI)

These four practices cover the basics of keeping your systems clean and current. You need anti-malware software running on your systems and updated when new definitions are available. You also require a process for identifying known vulnerabilities and applying fixes in a timely manner.

Practice ID	Requirement
SI.L1-3.14.1	Identify, report, and correct information system flaws.
SI.L1-3.14.2	Provide protection from malicious code.

SI.L1-3.14.4	Update malicious code protection mechanisms when new releases are available.
SI.L1-3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Other Foundational Practices

In addition to the practices stated above, you are required to:

- Establish basic cybersecurity policies covering system use and protection.
- Document user access authorization procedures.
- Maintain an inventory of systems handling FCI.
- Ensure basic security awareness for employees.
- Maintain evidence (screenshots, configs, policies) for assessment.

The Self-Assessment Process

Unlike CMMC Level 2, CMMC Level 1 does not require a third-party assessment by a Certified Third-Party Assessment Organization (C3PAO). Instead, Level 1 mandates an annual self-assessment, which is conducted by your own organization, plus an annual affirmation by a senior company official submitted to the DOD's Supplier Performance Risk System (SPRS).

A self-assessment requires you to evaluate your compliance against all 17 practices and the assessment objectives that support them, produce a score, submit that score to SPRS, and have a senior official attest to its accuracy. The self-assessment is an act of commitment, not a checkbox.

Step 1: Conduct the Assessment

Evaluate your organization's implementation of each of the 17 practices. For each practice, determine whether it is fully implemented, partially implemented, or not implemented by validating whether the assessment objectives listed in the Self-Assessment Guide are implemented or met. Collect evidence for each practice, including screenshots, configuration exports, policy documents, access lists, and maintenance logs. You will need this evidence to support your score and to demonstrate compliance if your assessment is ever reviewed.

Step 2: Calculate Your Score

CMMC Level 1 is scored on a simple pass/fail basis against the 17 practices. Each practice is either met or not met. For a control to be considered met, all individual assessment objectives need to be implemented. If one or more assessment objective is not met, the entire control is considered to be not met.

Step 3: Submit to SPRS

Log in to SPRS (https://www.sprs.csd.disa.mil/) and enter your assessment score. Your submission includes the date of assessment and your score.

Step 4: Annual Affirmation

Each year, a senior official at your company must affirm in SPRS that your organization continues to meet Level 1 requirements following the annual self-assessment. This affirmation is a legal statement. It is the mechanism by which the DOD holds organizations accountable for their self-reported compliance status.

Important: Level 1 certification lasts one year. Both the annual self-assessment and annual affirmation are required to remain in compliance. Missing either one creates a gap in your compliance record that contracting officers can see.

Level 1 Best Practices

Know what FCI you have and where it lives.
Before you can protect FCI, you need to know what you have. Identify the contracts that generate FCI, the systems that store or process it, and the people who access it. This can be a simple, accurate inventory of systems and in-scope users.

Documentation is required, and it can be simple.
A self-assessment that shows full implementation but has no supporting documentation is not a defensible assessment. You need written policies, access lists, configuration records, and evidence that your controls are operating. A one-page policy is better than no policy. A screenshot showing antivirus is installed and updated is better than a verbal assurance. Keep it simple, accurate, and organized.

Eliminate shared accounts before your assessment.
Shared user accounts with one login used by multiple people are among the most common negative findings in Level 1 assessments. They create accountability gaps, complicate incident response, and directly contradict the identification and authentication requirements. Every individual who accesses a system handling FCI needs their own unique account. This is non-negotiable under CMMC.

Treat patching as an ongoing operation.
One of the most preventable compliance gaps is unpatched software. SI.L1-3.14.1 requires identifying and correcting system flaws in a timely manner. In practice, this means a regular patching cadence. Define a schedule, document it, and follow it.

Make sure your antivirus is deployed everywhere and automatically updated.
Anti-malware must be deployed on all systems in scope and kept current. A partial deployment does not satisfy SI.L1-3.14.2 and SI.L1-3.14.4. Review your deployment, confirm automatic updates are enabled, and document the configuration.

Honestly conduct a self-assessment.

The annual self-assessment is a legal attestation. Score your organization accurately. False statements to the government carry serious consequences.

Common Level 1 Compliance Mistakes

Assuming Level 1 is easy because the list is short.
Seventeen practices sounds manageable. But fully implementing all practices and their assessment objectives, with documented policies, accurate configurations, maintained records, and an honest assessment takes effort. Organizations that underestimate Level 1 tend to discover the gaps during their assessment rather than before it. Start early.

Failing to scope correctly.
Not every system in your organization is in scope for Level 1, only those that store, process, or transmit FCI. But organizations routinely either over-scope (creating unnecessary compliance burden) or under-scope (leaving systems that actually handle FCI outside the boundary). Getting the boundary right is the first step in the assessment process.

Treating the self-assessment as a formality.
The annual self-assessment and affirmation carry legal weight. Treat the affirmation with the same seriousness you would treat any other legal certification.

Not involving leadership.
CMMC compliance is not just an IT issue, your whole organization should be involved. The senior official who makes the annual affirmation needs to understand what they are affirming.

Confusing Level 1 readiness with Level 2 readiness.
Organizations that know they handle CUI (and therefore have Level 2 obligations) sometimes deprioritize Level 1 compliance in favor of working on the more demanding Level 2 controls. Level 1 compliance is required today, independently of Level 2 status. Do not let the bigger goal delay the immediate obligation.

How Level 1 Relates to Level 2

CMMC Level 1 and Level 2 are distinct requirements, not a sequential checklist. Level 1 applies to FCI. Level 2 applies to CUI. Many DIB contractors handle both, which means they have obligations at both levels, and must meet the requirements of each independently.

	CMMC Level 1	**CMMC Level 2**
Applies to	Organizations handling FCI	Organizations handling CUI
Controls	17 practices from FAR 52.204-21	110 controls from NIST SP 800-171
Assessment type	Annual self-assessment	Third-party assessment by C3PAO
Assessment frequency	Annual	Every 3 years

SPRS submission	Required	Required
Annual affirmation	Required	Required
Documentation required	Yes (policies, evidence, access records, etc.)	Yes (SSP, POAM, policies, evidence)

If your contracts include CUI, the path to Level 2 starts with a solid Level 1 foundation. The access control, identification and authentication, and system integrity practices in Level 1 are a subset of what Level 2 requires. Getting them right at Level 1 builds the discipline and documentation habits that Level 2 demands.

Frequently Asked Questions

1. Does every DOD contractor need CMMC Level 1?

Level 1 applies to all DIB organizations that handle FCI. Review your contract language, specifically any FAR 52.204-21 clauses, to confirm your obligations.

2. How is Level 1 different from Level 2?

Level 1 covers 17 basic cybersecurity practices and is focused on protecting FCI. It requires an annual self-assessment. Level 2 covers all 110 NIST SP 800-171 controls, is focused on protecting CUI, and requires a third-party assessment by a C3PAO every three years. If you handle both FCI and CUI, you have obligations at both levels.

3. How long does it take to get compliant with Level 1?

For most organizations, the 17 practices are not entirely new. The work is typically in identifying and closing the gaps, building the documentation, and organizing the evidence. Organizations with reasonable IT hygiene can often achieve Level 1 compliance in a matter of weeks with focused effort. Those starting from scratch may need more time, but the controls are not technically complex.

4. What is the difference between FCI and CUI?

FCI is non-public information provided by or generated for the government under a contract not intended for public release. It is the information category that triggers Level 1 requirements. CUI is a broader category of sensitive but unclassified information, which includes technical drawings, export-controlled data, financial information related to government contracts, and more. CUI triggers Level 2 requirements. If you handle CUI, you also handle FCI, so Level 1 requirements apply as a baseline.

5. Do my subcontractors need to be Level 1 compliant?

If you flow FCI down to subcontractors through your contracts, those subcontractors have Level 1 obligations. As a prime contractor, you are responsible for implementing Supply Chain Risk Management processes to verify that your subcontractors are meeting their CMMC obligations.

6. What is SPRS and how do I submit my score?

SPRS, the Supplier Performance Risk System, is the DOD portal where contractors submit their CMMC self-assessment scores and senior official affirmations. You can access it at https://www.sprs.csd.disa.mil/.

7. If we already have Level 2 certification, do we still need to do Level 1?

Level 2 certification includes Level 1 requirements, meaning that if you have achieved Level 2, you have necessarily met the Level 1 practices. However, the annual affirmation requirement still applies. Make sure your SPRS record reflects your current certification status and that your annual affirmations are up to date.

8. How do we get started?

The first step is understanding which systems and users handle FCI and are therefore in scope. Reviewing the Scoping Guide can help organizations understand the controls, requirements, and how to scope their environment before beginning the assessment. From there, evaluate your current state against the 17 practices, identify and address gaps, and build your documentation. If you want a structured starting point, a gap assessment from an experienced compliance partner can give you a clear picture of where you stand and what you need to do next.

Resources

These resources provide guidance, templates, and assessment tools for CMMC Level 1 compliance.

- DOD CIO – CMMC (https://dodcio.defense.gov/CMMC/): Official CMMC documentation including the Level 1 Self-Assessment Guide, scoping guidance, and the latest program updates.
- FAR 52.204-21 (https://www.acquisition.gov/far/52.204-21): The Federal Acquisition Regulation clause that establishes the 17 basic safeguarding requirements for FCI (the foundation for Level 1 practices).
- SPRS (https://www.sprs.csd.disa.mil/): The Supplier Performance Risk System portal for submitting and managing your CMMC self-assessment scores and annual affirmations.
- CyberSheath CMMC 2.0 Guide (https://cybersheath.com/resources/guides/cmmc-2-0-guide/): A comprehensive overview of the full CMMC framework, levels, controls, and assessment process.