CMMC COMPLIANCE AND MANAGED SERVICES

Any organization hoping to work within the defense contract supply chain will need to meet the standards set by the Cybersecurity Maturity Model Certification (CMMC). Managed by the Department of Defense, CMMC compliance is a tiered system of compliance measures, which are ultimately intended to evaluate the maturity of the organization's cybersecurity systems, processes, and contingencies. It was introduced in 2020, refined in late 2021 and will be fully required by 2026.

Even organizations not hoping to work with the DoD may be interested in CMMC compliance. Being CMMC compliant can benefit any business because it works to actively improve the organization's cybersecurity measures.

Red River

aws PARTNER

Contents

What is CMMC Compliance?

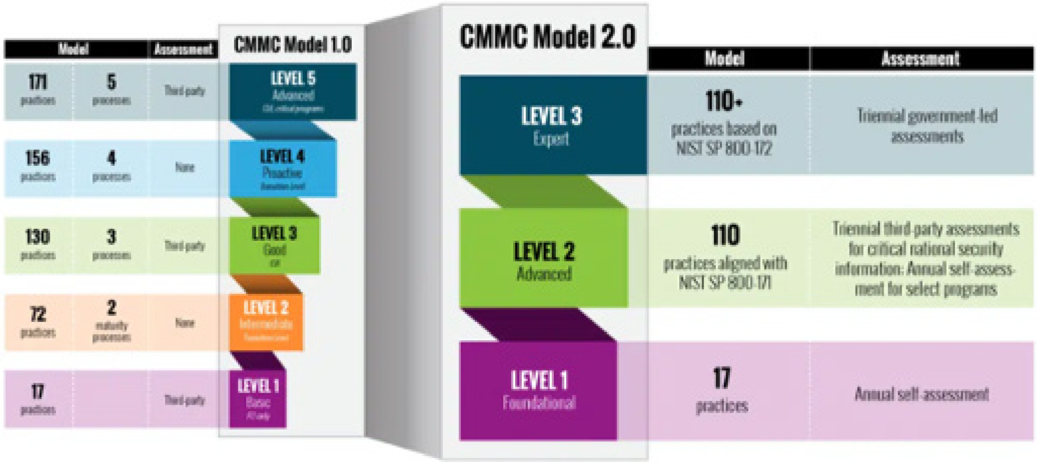
> *"CMMC stands for "Cybersecurity Maturity Model Certification" and is a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB). The CMMC framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level."*
>
> **- THE OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION & SUSTAINMENT CYBERSECURITY MATURITY MODEL CERTIFICATION**

The Cybersecurity Maturity Model Certification (CMMC) program is aligned to DoD's information security requirements for DIB partners. It is designed to enforce protection of sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program provides the Department increased assurance that contractors and subcontractors are meeting the cybersecurity requirements that apply to acquisition programs and systems that process controlled unclassified information.

Most organizations with basic security measures may be able to attain the lowest level of CMMC compliance. Achieving higher levels may take some work.

What Are the Tiers of CMMC Compliance?

CMMC 1.0 introduced five levels of security maturity. With the release of CMMC 2.0 the quantity of maturity levels was reduced from 5 to 3. The progression of the 3 levels is described in the image below.



Though CMMC compliance is designed to ensure that an organization is taking measures to protect controlled unclassified information (CUI), it's a well-rounded compliance framework built around NIST SP 800-171 and NIST SP 800-172 control sets. Through targeting the higher maturity levels in the CMMC model, an organization will be able to demonstrate their initiatives in obtaining advanced or expert levels of control and optimization than it would on its own.

What Levle of CMMC Compliance Does Your Organization Need?

The US Department of Defense is requiring that all DIB contractors to have some level of CMMC compliance. If an organization is not working with and will not handle CUI data, they can self-assess at maturity level 1. Organizations with access to CUI will need to work to meet maturity level 2 and will be required to go thru a C3PAO (Certified 3rd Party Assessment Organization) assessment. There will be occasions where a company is working with the most sensitive data and may be required to obtain a maturity level 3 assessment. This assessment must be performed by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). At this time, the DoD is still in the process of determining how organizations seeking maturity level 3 compliance will be assessed.

How Do You Get CMMC Certified?

1. Develop an SSP (System Security Plan) and self-assess against NIST 800-171 r2 controls.
2. If you had gaps identified from your self-assessment, build a POAM (plan of action and milestones) to improve your DoD SPRS (supplier performance risk system) score. The max score you can obtain is 110.
3. Identify your scope. Is your scope the entire organization, a specific company unit, or do you have a specific enclave where your CMMC platform will operate from?
4. An optional step, but very beneficial is to get a preliminary gap assessment with an accredited C3PAO. They can help determine any remaining gaps in your preparation for CMMC compliance.
5. Address the gaps
6. Conduct your assessment with a C3PAO. You can find a C3PAO by going to the Cyber-AB Marketplace: Cyber-AB Marketplace
7. Address the gaps
8. Get certified

A CMMC certificate will be valid for three years, after which it will have to be renewed. An organization will want to conduct audits of its security to ensure that it maintains its compliance.

For organizations seeking CMMC level 3 certification, the above process is functionally identical, except the assessor is the government rather than a third party

*The organization will then have 90 days to fix any issues that the assessor has discovered.

When Will CMMC Compliance Be Required?

It's important to note that CMMC compliance is not a new initiative. CMMC 2.0 is simply a vehicle to now enforce NIST 800-171, 172 and DFARS clauses that are already in contracts today. The CMMC framework was introduced in January 2020. Organizations currently subject to DFARS, Prime contractors, the Defense Contract Management Agency (DMCA), and legal teams can ask for proof of NIST 800-171 compliance today.

How Can A Managed Services Provider Help?

Most organizations cannot dedicate a significant portion of their time to achieving greater levels of CMMC compliance. Organizations need to focus on daily tasks; they need to focus on revenue-generating activities. Achieving CMMC compliance requires a dedicated focus and many IT organizations do not have the sufficient bandwidth or skillset to take in on entirely with their staff.

(Interweave AWS and how to use it – insert info here)

Whether you are seeking CMMC compliance for your entire organization or just a portion of it, Red River can help you stand up an AWS environment that will meet the NIST controls requirements and with Red River Managed Services' CMMC Assist, can help ensure that your environment stays compliant.

Auditing the Organization's Current Compliance Levels

Before an organization can improve its CMMC compliance, it needs a thorough audit of where it currently stands. Security audits are almost always best done by a reliable, trustworthy third party. An MSP will be able to dig into the organization's current security and compliance posture.

A regular security audit is beneficial to any company. A company will receive an audit from an assessing organization that not only outlines gaps within the current system, but also its recommended remediation activities. Going thru the actions to remediate will improve your overall security stance and it can also improve the organization's efficiency and cost metrics.

Implementing the Organization’s Cybersecurity Changes

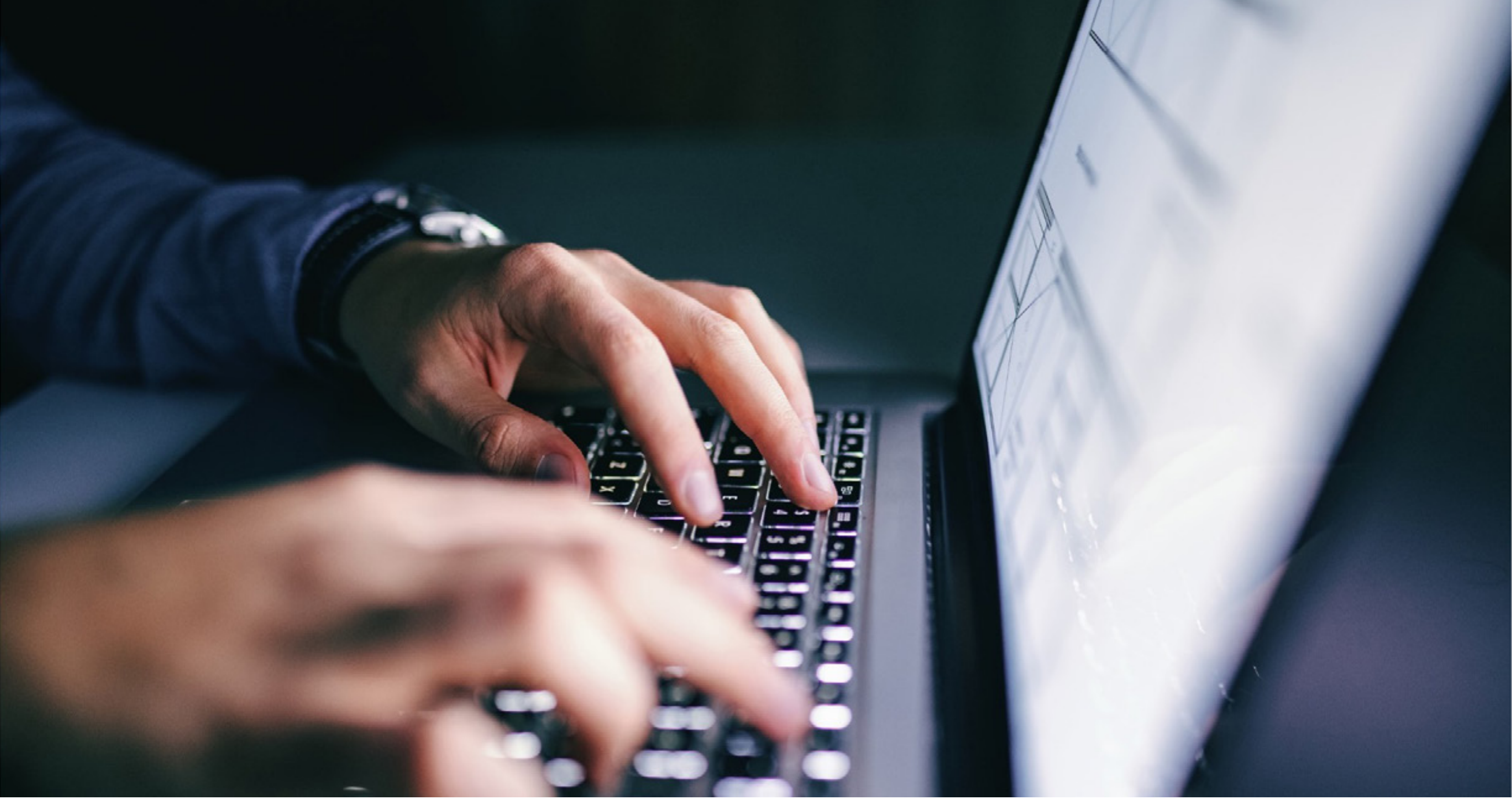
From pre-training employees to supporting large infrastructure transitions, an MSP can handle all the organization’s security compliance needs. An MSP will have the time, energy and support staff to manage the organization’s key cybersecurity changes on its own — so the organization’s own IT team doesn’t have to be pulled off their current initiatives.

An MSP will plan ahead to ensure that these cybersecurity changes aren’t disruptive — and will continue to support employees as the transition occurs. MSPs will be able to provide help desk support and continual training, so the organization is able to safely move to new processes and new systems.

Maintaining Cybersecurity Processes and Proactively Improving

Once the organization has achieved its new cybersecurity ecosystem, it’s not done. An MSP will continue to maintain cybersecurity processes, identify potential issues and scan for malicious actions. Red River will also be continually looking into areas of improvement for the organization — something that internal IT departments usually don’t have the time to do. An MSP will “future proof” the organization by investing in technology that the organization can rely upon for some time and will find better systems to improve the organization’s performance and revenue.

Ultimately, the MSP will provide a guided and active effort throughout the entire process of improving the organization’s security. Whether an organization already has a grand vision for its security solutions or does not know how to get started, the MSP can help. And because the MSP will bring many of these security processes and solutions to the organization out-of-the-box, it will be critical in achieving fast, streamlined CMMC compliance.



CMMC Compliance and Managed Services

A business can think of CMMC compliance as a measure of their general cybersecurity health. While CMMC has been designed specifically for DoD contracts, most of the requirements of CMMC apply to any organization dealing with critical, personally identifiable or protected   information.

To tackle most DoD contracts, organizations will need basic CMMC compliance. But that doesn't mean that achieving better compliance shouldn't be the ultimate goal of an organization and its IT team.

By working with a managed services provider, a business can ensure that they are moving toward better cybersecurity — including CMMC compliance requirements. An organization won't need to devote significant amounts of internal time toward compliance and will be able to achieve better compliance faster.