Red River

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 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.

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) is intended to describe an organization's preparedness against key security issues. A low score on the CMMC compliance model means that your organization is ill-prepared for potentially malicious actions, whereas a high score on the CMMC compliance model will mean that your organization has taken active, critical steps toward mitigating malicious actors.

Most organizations with basic security measures should be able to achieve the most basic level of CMMC compliance. But getting higher levels may take some work.

What Are the Tiers of CMMC Compliance?

There are five tiers of CMMC certification. Each higher-level tier contains the requirements of previous tiers.

1. **CMMC level 1** is the most basic level of compliance. This includes basic security practices, including having access controls, implementing identity controls and performing password protection. A level 1 organization is not likely to have a complete security strategy nor complete security practices. Rather, they will simply know the basics of security. Many organizations fall at CMMC level 1 before they start improving their security solutions.

2. **CMMC level 2** is a reasonably advanced level of security compliance. Organizations hoping to work with Controlled Unclassified Information (CUI) will need this level of compliance. There are many additional requirements for Level 2, but most notable is the need for documented policies and procedures.

3. **CMMC level 3** requires that organizations be able to log, monitor and report incidents, as well as respond to them quickly. Organizations will need to be able to back up and restore their data through tested, comprehensive backup solutions, and should be using measures to protect themselves from malicious traffic. CMMC level 3 is the most basic level of compliance that can be considered good cyber hygiene; an organization at CMMC level 3 will be adequately prepared to protect against security threats.

4. **CMMC level 4** describes a more proactive organization. At CMMC level 4, organizations must not just be prepared to react to security threats, but actively protect against them occurring. This includes whitelisting processes, using a SIEM or similar technology and establishing and maintaining a security center with a 24/7 response capability. While most organizations cannot maintain this type of response internally, they can hire an MSP that will.

5. **CMMC level 5** is the highest level of certification and what most organizations should ultimately aspire to. Organizations should be practicing advanced and progressive cyber hygiene, continually optimize their security processes, and analyze their network traffic. Organizations will need a sophisticated understanding of auditing, accountability, access control, and incident response.

Though CMMC compliance is designed to ensure that an organization can be trusted with unclassified and classified information, it's a well-rounded compliance measure. Through targeting CMMC certification, an organization will be able to achieve far better levels of control and optimization than it would on its own.

What Level of CMMC Compliance Does Your Organization Need?

Any organization working with the DoD in any capacity will at minimum need CMMC compliance level 1. CMMC level 1 is not a difficult certificate to get. Most organizations who have invested in their security in any capacity should meet this standard. An organization that does not meet CMMC level 1 must improve its security.

Depending on the contract, a different CMMC level may be noted. An organization that's interested in dealing with controlled information will want to get a Level 3 certificate at minimum. While Level 2 certificates do exist, they are largely intended to be transitive; they denote that the company is working from Level 1 to Level 3.

Before applying for CMMC certification, an organization may want to investigate the contracts that they are interested in working on. Each contract will deal with different levels of information and consequently different certification requirements.

How Do You Get CMMC Certified?

Before an organization gets CMMC certified, the organization itself must decide what level of certification it is working toward. This may require an informal audit of the organization, such as an audit by a third party such as a knowledgeable managed services provider. The organization will then request an assessment from an individual third-party assessment organization.

The third-party assessment organization will send an assessor to dig into the organization's qualifications. The assessor will evaluate the organization to determine whether it meets the requirements for the level of certification that it is requesting. It is possible that the assessor will find issues and gaps at this time.

The organization will then have 90 days to fix any issues that the assessor has discovered. An MSP will again be able to help the organization respond to the audit and ensure that the organization meets the required standards. If the organization meets its sought-out compliance, the certificate will be rendered. If the organization meets a lower level of compliance, it will get a lower-level certificate. An organization can request a different certification process once it has fixed its issues.

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.

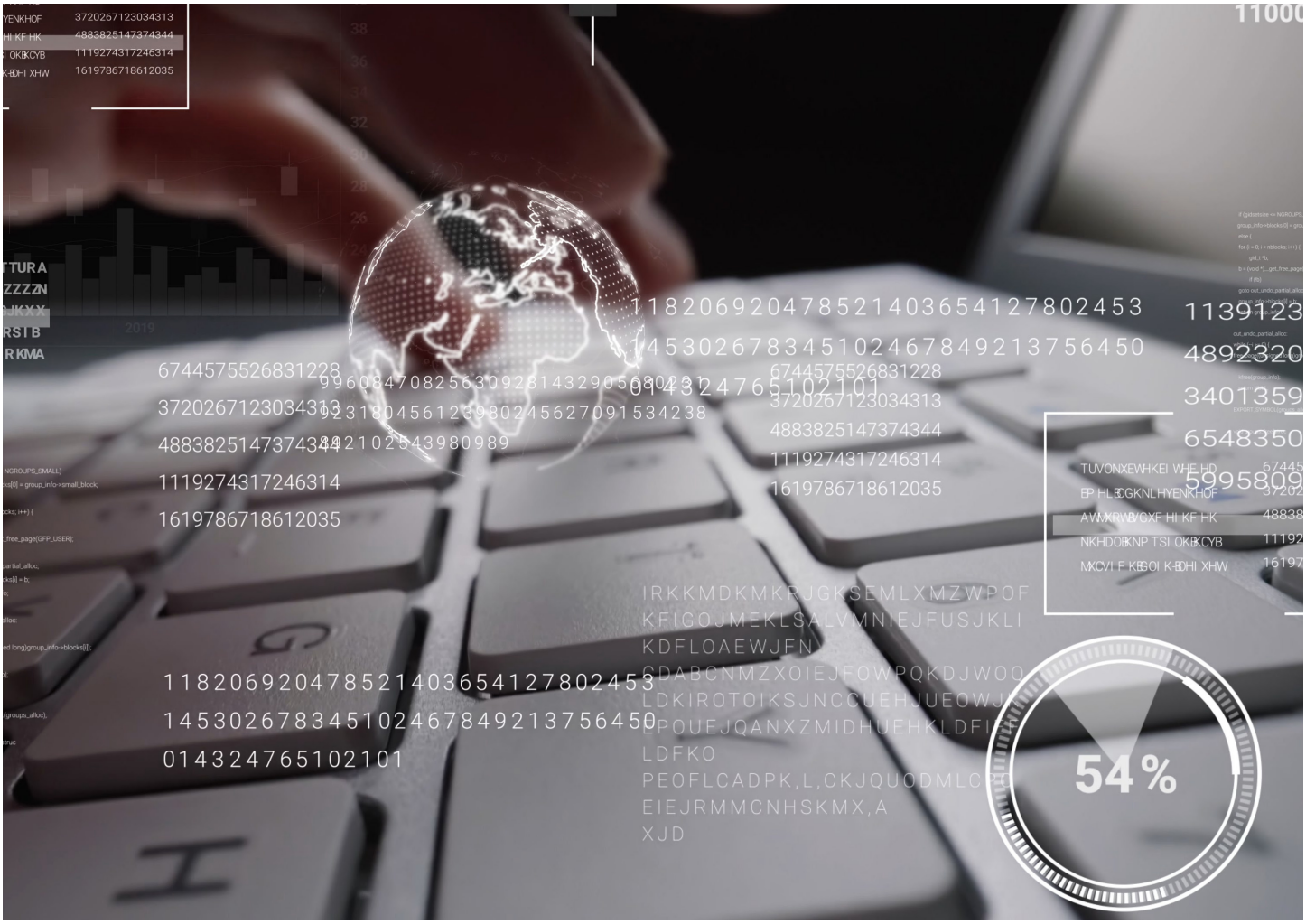
When Will CMMC Compliance Be Required?

It's important to note that CMMC compliance is a new initiative. The CMMC certificate was introduced in January 2020. CMMC certification will not be a set requirement by the DoD until 2026. Organizations have time to prepare for the certification process — but they should start now. Five years may be a significant amount of time, but it's not a long time for an organization to completely rewrite its processes and procedures, nor is it a long time to completely change an organization's infrastructure.

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. The IT departments within an organization are usually focused on putting out fires, answering help desk tickets and working towards large-scale business initiatives.

An MSP will help an organization in four stages: auditing, planning, implementing and maintaining.



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 security with fresh eyes and will have in-depth knowledge of current security standards.

A regular security audit is beneficial to any company. A company will receive an audit from an MSP that not only outlines gaps and redundancies within the current system, but also its recommended improvements. And not only does this improve the overall security of the organization, but it can also improve the organization's efficiency and cost metrics.

An MSP's goal isn't only to improve the organization's security, but to improve security in the best possible way. And that means better, more efficient processes and more cost-effective solutions.

Planning the Organization's Roadmap to Better Security Health

When does an internal IT department have the time to build a comprehensive improvement roadmap? For many organizations, security falls behind because the IT department simply doesn't have the time to devote to cybersecurity improvements. The IT department may not be able to research the newest, best-in-class security solutions, nor have time to implement them. There may always be "one more thing" they need to finish first, as well as help desk issues they need to sort out.

With an MSP, the organization can rely upon a trustworthy partner to build a full roadmap. And an MSP is experienced and knowledgeable enough that they will be able to build in fail safes and contingencies. They will be able to plan ahead to reduce (or entirely eliminate) disruption for the organization.

Implementing the Organization's Cybersecurity Changes

From pre-training employees to supporting large infrastructure transitions, an MSP can handle all of 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. The MSP 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.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions. To learn more, visit redriver.com.