MAINSTAY TECHNOLOGIES

2025

Guide to CMMC Compliance for Business Leaders

Your Practical, Non-Technical Guide to Navigating CMMC Requirements

Paige Yeater
CISO / COO

Learn More!

INTRODUCTION

If you are part of the Department of Defense supply chain, you may be facing challenges related to the **Cybersecurity Maturity Model Certification (CMMC)**. These challenges are especially felt by small and mid-sized businesses who lack teams of dedicated information security professionals. How do you make sense of the complexity of CMMC? And how can you approach it with a wise, reasonable budget?

Answering those questions is the goal of this guide. We are going to assume you already know why the Department of Defense is enforcing it, and that you are aware your contracts require compliance (or will soon!).

If you're looking for a technical guide, this isn't it. This is for business leaders looking for answers to pressing CMMC business questions.

OVERVIEW

The effort to implement CMMC requires work across the entire leadership team in your organization. The overall framework requires 3 critical elements: **people**, **process**, and **technology**.

- **People** - Business leaders in operations, finance, and executive teams
- **Process** - Whoever has organizational responsibilities over finance, HR, business processes and operations
- **Technology** – Despite being only 1/3 of the overall framework, technical requirements are the vast majority of the 110 required controls of CMMC. This fact makes this the most significant investment cost-wise.

This is complex. It’s vast. And yes, it’s difficult. But it’s very doable! We have helped dozens of organizations on their way. Through CMMC, you won't just meet a compliance requirement, you'll also significantly reduce your cybersecurity risk. As a business leader you need to recognize the right destination, walk the wisest path, and know how to get started. Our goal is to equip you to do just that.

We have been helping northern New England companies prepare for CMMC for the last 6 years. Our IT and InfoSec teams have guided business leaders from "what is this thing?" all the way to achieving and maintaining long-term standards.

Through that experience, we have found a few frequently asked questions.

THE MODEL

Who does this apply to?

This applies to anyone in the DoD Supply chain that is receiving **Federal Contract Information (FCI), or Controlled Unclassified Information (CUI).** Since CMMC is based on **NIST 800-171 Rev. 2** most organizations in the DoD supply chain already have these requirements in their contract.

When will this take effect?

At the time of publishing (Jan 2025), the DoD is well into the rule making process and actively seeking approval of this rule. The rollout will be conducted in phases over the next three years.

- Phase 1, which will be rolled out through 2025, we will start to see language show up in contracts, with self-assessments being required.
- Phase 2, which will roll out in 2026, we should start to see certifications being required where Level 2 is defined in contracts.
- Phase 3, which will roll out through 2027, will start to require certifications for renewal of existing contracts.
- Phase 4, which will roll out through 2028, CMMC will be fully in effect in all contracts where applicable.

Where can I go for updates?

An excellent resource for timely and significant updates is **CMMC News** from **The Cyber AB**.

Are there penalties for non-compliance?

Yes, depending on the contract language in your current DoD contracts, there are repercussions for noncompliance. With CMMC, there will be a gate in the contracting process, which will prevent organizations who have not been certified at the appropriate level from receiving contracts. This also means that during a contract renewal process there may be a new clause added that will preclude the contract from being renewed without the appropriate certification level.

THE PROCESS

How would I get started, and how difficult is this?

An excellent way to determine where you are and what you are missing is doing a **Compliance Gap Analysis and POAM (Plan of Action and Milestones)**.

Simply put, it's challenging. Unless you already have extremely secure technology and are under other robust compliance, it's an enormous lift for the organization. Think of it as an ISO certification + upgrade to technology.

Unfortunately, there are many **myths** surrounding CMMC. People take this opportunity to leverage fear as a marketing tool. There is no "one stop shop" product or service that will "solve" this. The only way is a systematic approach to people, process, and technology.

Regardless, compliance is an inevitable reality that you'll have to contend with, given that CMMC is soon going into law (more on the timeline later).

How long does it take to achieve compliance?

Depending on where you are starting from, how quickly you can move through the process and investments needed, this process could take anywhere from 6-36 months (about 3 years). It is important to know that after meeting compliance, it is an ongoing process to maintain it. An organization should expect to spend 12 - 24 months implementing the controls to be ready for an assessment. Timing can vary based on the aggressiveness of the implementation strategy and current technical debt.

What are the benefits of taking this on?

- Excellent cybersecurity protection. The majority of this aligns with NIST cybersecurity best practices generally.
- This will allow you to continue taking on government contracts.
- Unlike many government requirements, the security posture that CMMC requires is extremely beneficial to the business. It's sort of like seatbelt or helmet requirements – it can be annoying at first, but the consequences of not having a seatbelt or helmet on are so severe that it's well worth the initial annoyance.
- The results of moving into more sophisticated IT management, security controls, and solid information security governance are dramatic increases in the operational maturity of the business while significantly mitigating costly risk. This is the best of both worlds for business leaders, and a valuable opportunity to align the entire organization.

How much should I expect this to cost?

Ballpark Costs Gap Analysis/Plan of Action and Milestones (POAM)

- $7,000-10,000 for most organizations

Ballpark Costs for Security System Plan (SSP) Development

- $7,000-10,000 for most organizations.

These two projects will get an organization to the point where they know where they currently sit in relation to being compliant, have a plan for closing the gaps, and have built a policy to define the security program. Once these costs are spent, the organization will need to implement any changes. The current regional market cost for an assessment for a small to mid-sized business is estimated at $30k – $50k.

The overall cost for some organizations will be well over $100k. For others, it may be less, but it is helpful to know that an organization will likely be unable to reach compliance for less than $50k.

From the 3 critical elements (people, process, and technology) of the CMMC framework, the technology aspect will be most costly.

People and process requires devoting some internal leadership team time and working with an experienced professional in CMMC. This either means hiring (very costly) or working with a firm like Mainstay who can carry responsibilities at a lower cost (typically $1,500-$3,000 per month depending on your company's size).

On the technology side, additional layers and technology requirements MUST be implemented and maintained. Some of these will be one-time project costs and others will be ongoing costs. Upon achievement of compliance, you'll have a secure network infrastructure, compliant cloud infrastructure, up-to-date and encrypted workstations, multi-factor-authentication on all logins, and ongoing security monitoring solutions. There is indeed no "end" to this process, however; you get to compliance, and then you work to maintain it.

Total cost will vary depending on how you answer the following questions:

- Is all IT infrastructure up to date, with supported operating systems, business-class network infrastructure, and reliable equipment?
- Are advanced security layers already in place, to protect against cybersecurity risk?
- Are there full cybersecurity layers with ongoing security monitoring and testing (training in house/outsourced or a combination of both)?

We work with our clients across all aspects of cost to attempt to be as wise as possible. Some of these investments are just good business sense anyway, that help technology to be stable and secure. Some of them are expensive and simply to meet compliance.

This must be weighed against the alternate cost of lost contracts.

How do the Assessments work?

There are different assessment processes associated with CMMC. It is expected as CMMC is rolled out that contracts will call out whether a self-assessment is required or a certification performed by a C3PAO. The Self-Assessment process is for any organization that holds Federal Contract Information (FCI) or needs to align with Level 1 of the CMMC Framework and in some cases Level 2. The C3PAO Assessment Process is for those organizations that hold Controlled Unclassified Information (CUI) and therefore must adhere to Level 2 of the CMMC framework at a minimum and are likely seeking certification. There is also a Level 3 assessment within the framework performed by the Department of Defense. For this guide, we are focusing on CMMC Levels 1 and 2.

The Self-Assessment Process

To get started, you will access the Assessment Guide for the CMMC Level you are looking to achieve from the defense.gov website, **CMMC Resources & Documents**, which will walk you through the requirements for meeting each level's expectations. From there, you will need to complete a Self-Assessment form, noting where you are in alignment and where you are not. As part of this form, you will have to calculate a score associated with your compliance. Each requirement has a numerical value, and once you have completed the self-assessment, you can calculate your score. In addition, you will need to create a Plan of Action and Milestones (POAM) which is a list of items that you are working to implement with a corresponding timeline.

Once you have completed the questionnaire, calculated your score, and built out a POAM with dates, you will enter the information into the **SPRS database**.

The C3PAO Assessment Process

The Assessors will first do a pre-assessment evaluation to confirm your organization's assessment feasibility determination. The Level 2 process requires an assessment from a third-party assessor, called a C3PAO (Certified Third-Party Assessing Organization). This process flows differently from the Self-Assessment process, takes longer and is more costly. The Assessment process can be found **here**.

There are a few initial steps you must complete to begin this project. First, you must identify and engage with a Third-Party Assessor Organization (C3PAO) that is authorized by the DoD; the CMMC assessment itself will be conducted by them. Then, to prepare for future certification, be sure to consult with an officially designated Registered Practitioner (RP) Organization, like Mainstay Technologies. These organizations are specially trained to help guide and partner with companies working toward CMMC.

The Assessors will work with your organization to gather evidence of alignment with each of the 110 requirements within the **NIST 800-171 Rev. 2** Special Publication. These are broken down into three categories:

- Interview – Discussions with individuals to assess full implementation, staffing and training
- Examination – Review, inspection, observation, studying or analyzing assessment objects (documents, mechanisms, activities)
- Testing – Demonstrations of certain practices being carried out

At least two pieces of evidence will be required per Practice, and 2 of the 3 evidentiary categories above must be represented. This process is likely to take several months to complete, on top of any pre-assessment preparation time needed.

Once the assessment work is finalized the C3PAO will make a recommendation to the CMMC-AB. The CMMC-AB will review the work and award a certification if they agree with the C3PAO's assessment.

Why Partner with Mainstay for CMMC Services?

A Mainstay Client Story: Tech Resources, Inc.

Tech Resources, Inc. is an 80-person company in Milford, NH specializing in sophisticated electronic test equipment and technical logistic services.

This case study from NH Manufacturing Extension Partnership (NH MEP) tells the story of how Tech Resources partnered with Mainstay's security team to achieve CMMC and NIST 800-171 compliance, resulting in incredible retained sales revenue and increased investments.

Ultimately, CMMC will tangibly benefit your business, saving you loads of time and money.

What can I outsource, and what is the value of working with Mainstay?

While the answer to this will be highly specific to each organization, it's valuable to understand that outsourcing gives you access to a broader range of skill sets, but this can be addressed either by hiring or by outsourcing.

Mainstay Technologies is a CMMC-AB Registered Provider Organization™, authorized by The Cyber AB (Formerly CMMC Accreditation Body). As seasoned experts, we're positioned to help you prepare. We help business leaders like you to understand their current situation, the compliance requirements, and the path that helps them to be successful and makes sense for their unique business, tailored to each client.

Contact us to discuss services and solutions that not only check the box for compliance but also give real cybersecurity and business value to your entire organization.

Scan, or visit:
www.mstech.com/contact/

MAINSTAY TECHNOLOGIES