MAINSTAY TECHNOLOGIES

2026

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 several 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?

CMMC applies to all organizations within the DoD supply chain that handle **Federal Contract Information (FCI) or Controlled Unclassified Information (CUI)**, including prime contractors, subcontractors, and suppliers of all sizes. This *includes* **small and midsize businesses** that may not have previously considered themselves in scope, as CMMC requirements can now be introduced through new DoD contract clauses at any tier of the supply chain. Organizations that handle CUI are expected to meet CMMC Level 2 requirements, while organizations that handle FCI only and do not process or store CUI may meet compliance through CMMC Level 1. Because these requirements are now formally enforced through contracts, any company that touches DoD data should assume CMMC applicability unless explicitly determined otherwise.

When will this take effect?

CMMC 2.0 is already in effect and has moved from rule-making into active implementation. The Final Rule became effective on December 16, 2024, and the DoD is now executing a phased rollout. Phase 1 is underway, with CMMC requirements beginning to appear in new contracts and solicitations, including Level 1 and Level 2 requirements and associated self-assessments. In Phase 2, expected in 2026, contracts that define Level 2 will increasingly require third-party certification. Phase 3 will extend certification requirements to the renewal of existing contracts, and Phase 4 will complete full implementation, making CMMC a standard requirement across all applicable DoD contracts.

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?

As CMMC enforcement takes effect, noncompliance now carries direct and material business consequences. CMMC serves as a gate in the DoD contracting process, preventing organizations without the required certification level from bidding on or receiving new contracts, and contracting officers may add CMMC clauses at renewal that condition continued performance on certification. As a result, noncompliance can lead to disqualification from new awards, inability to bid, or contract termination. At the same time, misrepresenting an organization's cybersecurity posture creates significant legal and administrative risk. False or outdated self-assessments submitted to SPRS may trigger enforcement actions, including potential liability under the False Claims Act, as demonstrated by the March 26, 2025 Department of Justice **press release** announcing that defense contractor MORSECORP Inc. agreed to pay $4.6 million to settle allegations it violated the False Claims Act by submitting false claims tied to inaccurate cybersecurity compliance reporting on DoD contracts.

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)**.

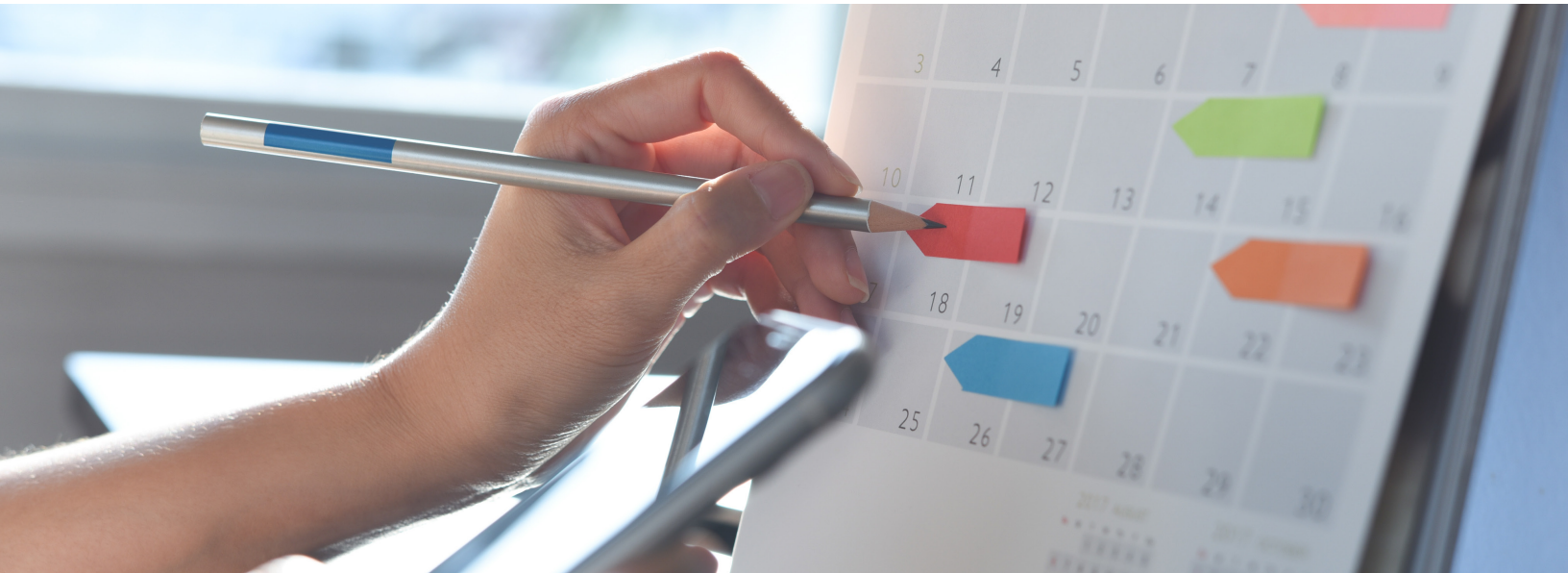
Simply put, it's challenging. Unless you already have extremely secure technology and are under other robust compliance, it's an enormous lift for the organization. Think of it as an ISO certification + upgrade to technology.

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?

- Strengthens cybersecurity by **aligning** the organization with proven NIST-based best practices
- Preserves **eligibility** for new DoD solicitations issued after December 2024
- Reduces the **risk** of disqualification, non-award, or contract disruption under updated DFARS and CMMC clauses
- Improves protection of CUI and **enhances** supply-chain risk management amid an evolving cyber threat landscape
- Increases overall **operational maturity** through more disciplined IT management, security controls, and governance
- Helps **future-proof** the organization against evolving requirements, including updated NIST standards and expanded compliance mandates
- Positions the business to meet rising **security** expectations from non-DoD federal agencies and commercial customers
- Delivers long-term risk reduction and **business resilience** that extend well beyond compliance requirements

How much should I expect this to cost?

CMMC compliance costs vary significantly based on organization size, current security maturity, and the CMMC level required by contract. For many small to mid-sized organizations, early-stage planning costs typically include:

- **Gap analysis and POA&M development**: $7,000–$10,000
- **Security System Plan (SSP) development**: $7,000–$10,000

These efforts establish current compliance posture, document required controls, and define a remediation roadmap. Beyond planning, organizations must budget for remediation, tooling, and ongoing program maintenance. For contracts requiring Level 2 certification:

- **Third-party (C3PAO) assessment costs**: commonly $30,000–$50,000.
- **Total compliance investment**: may exceed $100,000 for some organizations, depending on required remediation and infrastructure changes.

While some organizations may spend less, achieving and sustaining compliance for under $50,000 is increasingly unlikely under the CMMC 2.0 Final Rule.

From a cost perspective, the three pillars (**People, Process, and Technology**) of CMMC impact budgets differently:

- **People and Process**: internal leadership time plus support from experienced CMMC professionals, either through hiring or ongoing advisory partnerships with organizations like Mainstay Technologies.
- **Technology**: typically the largest expense, including secure network and cloud infrastructure, endpoint protection, encryption, multi-factor authentication, logging, and continuous monitoring

Because CMMC 2.0 is now formalized and Phase 1 enforcement is underway, actual costs may vary and may increase as certification requirements, remediation expectations, and security baselines evolve.

Organizations should plan for additional overhead, particularly where future contracts require enhanced controls or alignment with updated NIST standards, and consider building a 6–18 month compliance buffer to account for assessment timelines, remediation work, and increased demand across the defense industrial base.

How do the Assessments work?

Under CMMC 2.0, assessment requirements are formally defined by the Final Rule and are driven by the CMMC level specified in contract language. Level 1 requires a **self-assessment**, while Level 2 may require either a self-assessment or a third-party certification performed by a DoD-authorized C3PAO, depending on the contract and the sensitivity of the information involved. For this guide, the focus is on CMMC Levels 1 and 2. Regardless of assessment type, organizations are required to submit assessment results and scores to the Supplier Performance Risk System (SPRS), a requirement that is already being enforced under Phase 1.

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 the 320 objective across 110 controls 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.

Case Study: Supporting Pendar Technologies Through a Successful CMMC Assessment

The Challenge

As a subcontractor to the U.S. Department of Defense, Pendar Technologies undertook a CMMC assessment that required sustained coordination and focus across the organization throughout 2025. To support this effort, Pendar partnered with **Mainstay Technologies** for guidance and execution throughout the process.

As Pendar's leadership described it, the effort involved "**substantial documentation work alongside many fast-paced technical control projects**," a reality that shaped both the pace and complexity of the engagement.

The Mainstay Approach

Mainstay partnered closely with Pendar throughout the engagement, providing structured guidance, hands-on documentation support, and technical leadership to help navigate the CMMC landscape.

Ajdin Hasanefendic-Carroll, IT Manager at Pendar, highlighted the importance of leadership and clarity during the process, noting that Mainstay's guidance "***made a complex and unfamiliar landscape not only manageable, but constructive and growth oriented***".

Mainstay's team worked collaboratively with Pendar to ensure every requirement was addressed with rigor and precision. As Ajdin shared, "***The professionalism, integrity, and dedication each of you demonstrated reflects the highest standards I have come to expect in mission-critical work***".

Execution and Collaboration

Throughout the engagement, Mainstay emphasized partnership and accountability. Pendar's leadership consistently pointed to the value of this approach during the most demanding phases of the assessment.

Romain Blanchard, Chief Operating Officer at Pendar Technologies, shared that Mainstay's "***consistency, responsiveness, and depth of expertise were critical in helping us navigate the process successfully***" and that "***we landed exactly where we needed to, and we are very satisfied with the outcome***".

The engagement was characterized by close coordination, trusted communication, and sustained effort on both sides. As Ajdin noted, Mainstay's support created "***a collaborative environment rooted in trust and mutual respect, which made even the most demanding moments feel aligned and achievable***".

Results & Looking Ahead

Pendar successfully completed its CMMC assessment, meeting its compliance objectives and strengthening its security posture in support of Department of Defense requirements. Reflecting on the outcome, Romain stated, "***We greatly value this partnership and appreciate the level of care and commitment you brought to this effort***".

Ajdin echoed that sentiment, adding, "***Thank you all for your partnership, your support, and the impact you have made. It has been a privilege to work alongside you, and I look forward to what the future brings***".

With a successful assessment complete, Pendar and Mainstay are positioned to build on this foundation over the coming years. As the organization continues to evolve its security and compliance posture, the relationship established during this engagement sets the stage for continued collaboration and long-term success.

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