3 Key Steps To Achieve CMMC Compliance

Essential steps for navigating CMMC regulations

Gus Cervantes - CEO & CISO
ITS Team

Table Of Contents

To get **CMMC 2.0 (Cybersecurity Maturity Model Certification)** certified, you need to understand the **requirements, levels, and process** involved. CMMC 2.0 is designed to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) in the Defense Industrial Base (DIB). Here's what you need to know:

Having worked for the largest U.S. defense contractors in the world, I have over 30-years' experience with compliance in the DoD space. I have a deep understanding of what it takes to get your business compliant. Reach out today for free consultation.

1. Understanding the Requirements

01

Understand The Requirements

Review the CMMC Framework:

Familiarize yourself with the CMMC model, which is structured across three levels, each with a set of practices and processes. Levels 1-3 increase in complexity and maturity, with Level 1 being the most basic, Level 2 being the most common, and Level 3 the most advanced. Note that CMMC 2.0 Levels 2 and 3 require that you meet all 110 controls of NIST SP800-171 R2.

The 3 levels of CMMC 2.0:

Level	Purpose	Focus	Basis
Level 1	Basic Cyber Hygiene	Protect FCI	17 practices from FAR 52.204-21
Level 2	Advanced	Protect CUI	110 Controls of NIST SP 800-171
Level 3	Expert	Protect CUI from APTs	NIST SP 800-171 + parts of NIST SP 800-172

Determine Required CMMC Level:

Check your DoD contract requirements or speak with your prime contractor if you're unsure. Assess which CMMC level your organization needs to achieve based on your involvement with Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Contracts and requests for proposals (RFPs) will typically specify the required level.

- **Level 1:** For contractors that only handle FCI.
- **Level 2**: For contractors handling CUI (most common for subcontractors).
- **Level 3**: For highly sensitive DoD programs (Tier 1 contractors).

- **Gap Analysis:**

Conduct a gap analysis to compare your current cybersecurity practices against the CMMC requirements for your target level. This helps identify areas that need improvement.

Completing a thorough and accurate gap analysis is the next critical step after completing an assessment scope of your CUI boundaries in your organization. Too broad a scope can potentially waste tens of thousands of dollars. We have the expertise and experience to help you scope your CMMC boundaries, so you are not wasting precious time and financial resources.

2. Develop and Implement a Plan

Develop and Implement a Plan

• Scope your CUI boundary:

Define the boundaries of your organization that touch FCI and CUI. This will help in defining what part of your organization will be under audit for CMMC 2.0 L2 or greater certification.

Create a System Security Plan (SSP):

Document your current security practices and how they meet (or don't meet) the CMMC requirements. An SSP is a critical component of your compliance efforts.

• Remediation Plan:

Develop a plan to address gaps identified in your gap analysis. This plan should include specific actions, timelines, and responsible parties for implementing necessary controls.

• Policy and Procedure Development:

Establish and document policies and procedures that align with the CMMC practices. Ensure that these are communicated and enforced within your organization.

• Evidence and Artifacts:

Collect evidence and artifacts you will need to demonstrate you have implemented the required controls under audit of a C3PAO.

DoD Supplier Performance Risk System (SPRS):

Create a DoD SPRS account and report your progress frequently

Remediation Plan:

Develop a plan to address gaps identified in your gap analysis. This plan should include specific actions, timelines, and responsible parties for implementing necessary controls.

• Policy and Procedure Development:

Establish and document policies and procedures that align with the CMMC practices. Ensure that these are communicated and enforced within your organization.

• Evidence and Artifacts:

Collect evidence and artifacts you will need to demonstrate you have implemented the required controls under audit of a C3PAO.

DoD Supplier Performance Risk System (SPRS):

Create a DoD SPRS account and report your progress frequently

• Engage a C3PAO:

Engage a Certified Third-Party Assessment Organization (C3PAO) to conduct a formal assessment of your compliance. This step is crucial for achieving certification and demonstrating your compliance to the Department of Defense (DoD).

Our software solution and expertise help automate the complex creation of the required SSP. Our software also centralizes where we keep your required compliance evidence and artifacts. With our subject matter experts and our software, we get you CMMC compliant efficiently. Our software makes short work of the required POAM for your remediation plan.

A 15-minute phone call with us can help give you clarity on this subject and save you hours of frustration and wasted resources. Reach out today.

3. Conduct Regular Training and Assessments

Conduct Regular Training and Assessments

- **Employee Training:**

Train your employees on the new policies, procedures, and security practices. Regular training ensures that everyone understands their role in maintaining compliance and security.

- **Internal Audits and Assessments:**

Perform regular internal audits to verify compliance with CMMC requirements. Use these audits to continuously improve your cybersecurity posture.

Beyond The Three Critical Steps

In the defense industrial base, compliance is not a one-and-done event; it's an ongoing process that demands constant vigilance. Beyond the foundational steps, ensuring that your operations remain compliant with CMMC 2.0 is critical to maintaining national security standards and protecting valuable contracts.

The landscape of defense contracting is highly dynamic, and non-compliance can lead to delays, penalties, or the loss of critical government contracts. Continuous monitoring and proactive risk management are essential for safeguarding long-term operational success.

Remember that recertification is mandated every three years. Staying compliant over time is key to reducing the risk of disruptions and ensuring smooth, uninterrupted operations. As the military adage goes, "It’s easier to keep the mission in motion than to scramble when systems fail." The same holds true for compliance — staying ahead is not just more efficient, it's more cost-effective.

Ongoing Compliance

Ongoing Compliance

- **Remediation Plan:**

· Annual affirmations (for Levels 1 and 2 where allowed).

· Reassessments every **3 years.**

· Maintain documentation, conduct internal audits, stay updated with changes to NIST standards.

Useful Resources

NIST SP 800-171

- NIST SP 800-172
- **CMMC Program Site (DoD)**
- **Cyber AB**


The Risk of Waiting

The Risk Of Waiting

• Starting November 10, 2025, FAR 48 kicks in and CMMC requirements will start appearing on federal contracts. Not meeting the requirements could cost you the opportunity to bid on and win DoD contracts.

• Prime contractors' CMMC certification requirements flow down to their subcontractors. Soon primes will be demanding their subs meet the certification requirements or they may look to other suppliers who have met the requirements.

• Finally, there are many more organizations that need to get CMMC Certification then there are Third-Party Assessment Organizations (C3PAO)'s, so waiting to start preparing for certification, could put you behind many others and may take several years before they can complete your assessment.

At this point there is no time to waste. You need to ACT NOW if you wish to continue working with the Federal Government. We have the experience and expertise to get you CMMC compliant quickly and efficiently.
Contact us TODAY! We offer a free no obligation consultation.

How We Can Help

How We Can Help

We can remove the stress and complexity of getting you CMMC compliant!

• We can complete the entire project with our team of experts, or we can work with your existing IT personnel to get this effort completed.

• We have the experience, expertise, and software to help you get CMMC compliant.

• We have helped companies with as few as 11 employees and others with more than 1,200 employees prepare for CMMC certification.

• We have best in class solutions with regards to software, hardware, and network architecture so you don't lose time trying to figure this out.

Break Radio Silence...

We understand that time is of the essence. So please reach out to us for a **free no obligation 15 -minute phone call** to see how we may be able to help. Call our office at (858) 538-4729 or reach out to me personally, Gus Cervantes, on my cell phone at (858) 449-2078

As the founder of ITS Team, I have worked in and around the DoD my entire carrier. I have worked for Huges Aircraft, Scientific Atlanta, General Dynamics, Raytheon, & Lockheed Missiles & Space Company before starting ITS Team.

Grounded in years of experience across Compliance and Cybersecurity, I approach this work with unwavering commitment and a mission-first mindset. For me, this field isn't just a profession—it's a calling.

Gus Cervantes - President & CISO
Office (858) 538-4729
Cell (858) 449-2078
Gus@itsteam.com

Three Critical Steps for CMMC Compliance

Achieving Cybersecurity Maturity Model Certification (CMMC) compliance can be straightforward with the right guidance. This book outlines three critical steps: understanding CMMC requirements, developing and implementing a compliance plan, and conducting regular training and assessments. With expert insights and practical strategies, you'll be equipped to navigate the complexities of CMMC and secure your organization's future in government contracting.

Gus Cervantes - President & CISO
(858) 538-4729
Gus@itsteam.com
www.itsteam.com