INTELLIGENT
TECHNICAL SOLUTIONS

CMMC 2.0 Compliance Made Simple: A 7-Step Guide for Executives

by Kharmela Mindanao

Table of Contents

Introduction

Are you struggling to navigate the complex requirements of the Cybersecurity Maturity Model Certification (CMMC)? Do you wonder how achieving CMMC compliance can benefit your organization beyond just meeting Department of Defense (DoD) mandates?

Achieving CMMC compliance is more than a regulatory hurdle; it's a strategic asset that can elevate your organization's financial stability and operational efficiency. We learned this in our years of business providing compliance services.

In this eBook, we promise to guide you through the intricacies of the CMMC framework, showcasing how adherence to its stringent cybersecurity standards not only protects sensitive federal information but also fortifies your national security contributions.

We'll explain:

- The essential steps for achieving compliance,
- The benefits of certification beyond the baseline requirements, and
- How this commitment to cybersecurity can unlock new opportunities.

Discover how to leverage CMMC for a competitive edge in securing DoD contracts and affirm your organization's dedication to cybersecurity excellence with this eBook.

Step 1: Understand your CMMC requirements

The first step towards CMMC 2.0 compliance is identifying the right CMMC level for your business and its corresponding requirements.

The latest CMMC guidelines outline three levels of cybersecurity practices and processes: Foundational, Advanced, and Expert. Most contractors will likely land at the Advanced level. Determining the right level for you depends on the type of information your business handles, the risk it poses to the DoD, and your ability to meet the requirements of each level.

The financial and operational implications of each level vary; higher levels require more sophisticated cybersecurity measures, implying increased upfront and ongoing investments.

However, achieving a higher CMMC level can enhance your competitive edge, potentially leading to more lucrative contracts and improved operational resilience against cyber threats.

The levels are:

Level 1 (Foundational)
This level follows the most basic cybersecurity practices based on the 17 controls found in FAR 52.204-21 or the Basic Safeguarding of Covered Contractor Information. These controls protect covered contractor information systems and limit access to authorized users.

Level 2 (Advanced)
Compliance with Level 2 applies to companies working with CUI (Controlled Unclassified Information) and mirrors the NIST SP 800-171 guidelines.

It aligns with the 14 levels and 110 security controls developed by the National Institute of Technology and Standards (NIST) to protect CUI.

Level 3 (Expert)
The highest level of the CMMC 2.0 model focuses on reducing the risk from Advanced Persistent Threats (APTs). It is designed for companies working with CUI on DoD's highest priority programs. The model is also based on NIST SP 800-171's 110 controls and a subset of NIST SP 800-172 controls.

Once you've identified the right CMMC level, you're ready to go to step two.

Step 2: Conduct asset identification and management

Identifying critical assets and data involves understanding what information and systems are essential to your operations and the DoD contracts you serve.

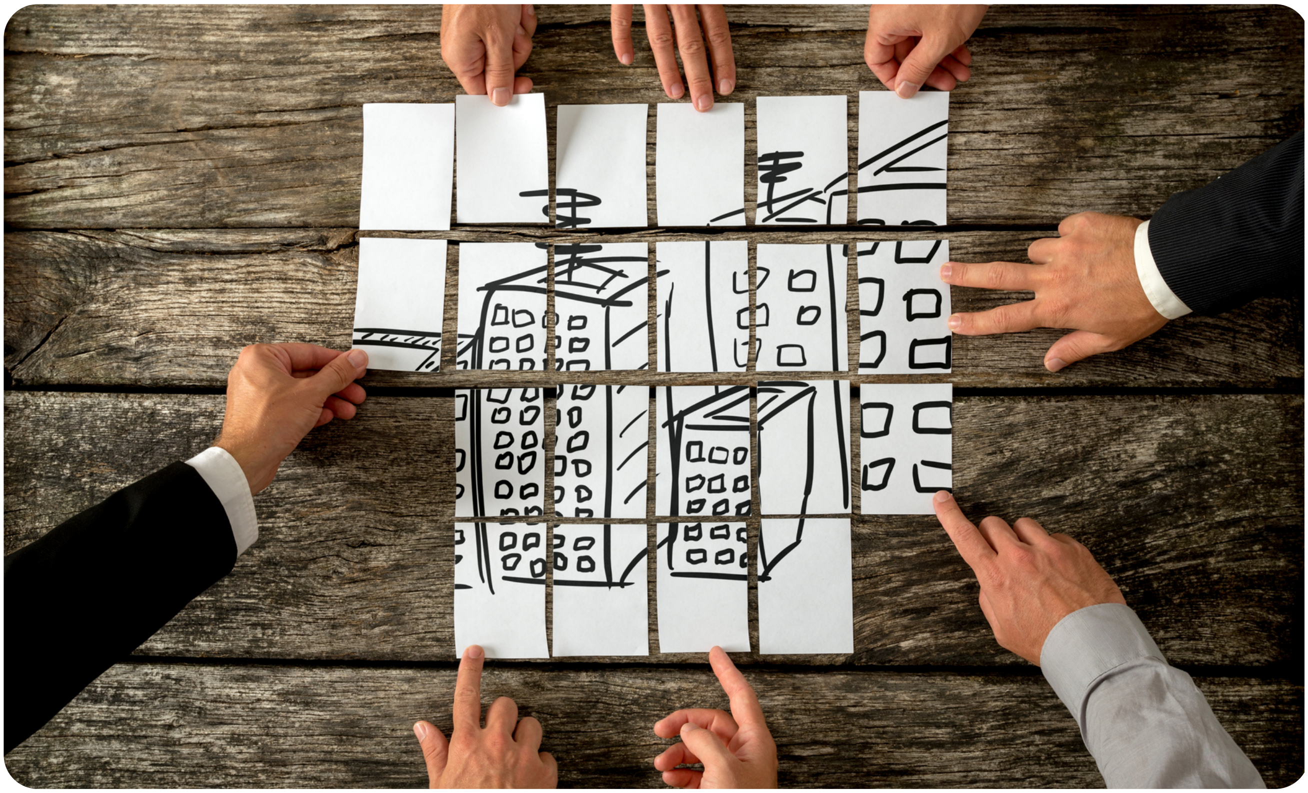
This step is a must for CMMC compliance, as it determines the scope of cybersecurity measures you need. To minimize compliance costs, organizations should adopt strategies for efficient asset management.

This includes categorizing assets based on their criticality and sensitivity, implementing a centralized asset management system, and regularly reviewing and updating the asset inventory to reflect changes in the operational environment or regulatory requirements.

Efficient asset management not only aids in achieving compliance but also enhances overall operational efficiency by ensuring that cybersecurity resources are allocated effectively.

RELATED: How to Manage Your Assets (Simple Tools for Your Business)

Step 3: Design a compliant technical infrastructure



When selecting technical solutions for CMMC compliance, consider solutions directly addressing the cybersecurity practices and capabilities defined at your required CMMC level.

Prioritize solutions offering scalability, integration capabilities, and compliance reporting features.

For cost-effective infrastructure upgrades, consider phased implementations focusing on high-priority areas first, leveraging cloud services for flexibility and cost savings, and exploring open-source tools for certain cybersecurity functions.

Engaging in partnerships with vendors offering compliant-ready solutions can also reduce the overall cost and complexity of meeting CMMC requirements.

Step 4: Implement cybersecurity measures

Implementing cybersecurity practices using Microsoft Government solutions involves leveraging their comprehensive suite of tools designed for compliance and security.

Start by assessing your current cybersecurity infrastructure against CMMC requirements.

Then, utilize security and compliance centers to configure policies and protections across your digital environment. For operational benefits, you should invest in cybersecurity tools that improve efficiency through automation, enhanced data protection that builds client trust, and reduce the risk of costly breaches.

RELATED: 10 Best Cybersecurity Tips & Practices From Experts

Step 5: Partner with the right MSP or MSSP

When selecting a managed services provider (MSP) or managed security services provider (MSSP) for CMMC compliance, referenced as ESPs (External Service Providers), you should assess their cybersecurity expertise, understanding of DoD requirements, and financial alignment with your needs. Select ESPs known for their:

- CMMC readiness
- Multi-layered security services
- Cost transparency

Additionally, while no ESPs are fully CMMC Level 2 certified yet, they must actively work with a CMMC Third-Party Assessor Organization (C3PAO) to navigate their certification process. Ensure any ESP you consider is well-versed in these procedures and inquire about their specific plans for assessment and certification.

Filtering for MSPs going through the certification process mitigates the risk of non-compliance. It also leverages the MSP's expertise and potentially offers significant ROI by offsetting the need for extensive in-house cybersecurity capabilities and ensuring continuous compliance to avoid penalties or contract losses.

Step 6: Document and prepare for CMMC Assessment

For best practices in documenting cybersecurity policies and procedures, prioritize maintaining clarity, comprehensiveness, and accessibility.

Policies should clearly define roles, responsibilities, and protocols for security measures, ensuring they are easily understood by all stakeholders. Regular reviews and updates to reflect the evolving cybersecurity landscape are crucial.

Preparing your team for the CMMC assessment involves comprehensive training on a competitive edge.

Step 7: Begin the CMMC assessment process

Once ready, select a C3PAO from the official CMMC Accreditation Body website to conduct the formal assessment.

Work with the C3PAO to schedule and undergo the CMMC assessment. If the assessment is passed, the company will receive their CMMC certification, indicating their compliance level.

Once you're set and confident in your cybersecurity measures, it's time to take the final step. Head to the official CMMC Accreditation Body and pick the C3PAO that fits your company. These firms will conduct the formal assessment and have the final say in your CMMC accreditation.

Next, you'll collaborate with your chosen C3PAO to schedule your CMMC assessment. You want to ensure everything is spotless; this assessment is your moment to shine and prove that your cybersecurity goes above and beyond.

If you pass, you'll be awarded your CMMC certification, a badge of honor that shows the world—particularly the Department of Defense—that you're serious about protecting sensitive information and that you meet their stringent compliance standards.

What's next in your CMMC journey?

The road to securing your digital environment is paved with more than compliance checkboxes. It's about deeply understanding each step, from demystifying the CMMC's intricate demands to strategically managing your digital assets and enhancing your cybersecurity defenses.

Each milestone reflects your dedication to protecting not just sensitive data but also fortifying the backbone of our national security.

But why is this journey so important for your company's success?

Beyond regulatory adherence lies the opportunity to boost operations and sharpen your competitive edge. It's about crafting a cybersecurity posture that's not only strong and adaptable but also capable of outmaneuvering the most advanced threats.

This is where the power of an MSP shines. For example, here at ITS, our compliance experts can transform CMMC compliance from a daunting task into a strategic asset that elevates your operational prowess and security to new heights.

So, are you ready to take your cybersecurity to the next level?

Schedule a consultation with our compliance professionals today. Together, we'll craft a bespoke CMMC compliance strategy that doesn't just meet DoD standards but propels your organization towards achieving operational excellence and unmatched security.

Intelligent Technical Solutions
(885) 204-8823
www.itsasap.com