



MEET THE CMMC

(A DoD Contractor's New Best Friend)

The Avatara logo consists of a circular shape formed by two overlapping lines, one orange and one blue. The word "avatara" is written in a lowercase, sans-serif font across the center of the circle.

avatara

ask ava:

YOUR AVATARA ASSISTANT

"Hi, ava. What do I need to know about the CMMC?"

I'm so glad you asked! Seriously. If you're a Department of Defense (DoD) contractor or subcontractor wondering about the Cybersecurity Maturity Model Certification (CMMC), here's the bottom line: Get. The. Certification.

"Whoah, slow down. Do I really need to invest valuable time and resources into this right now?"

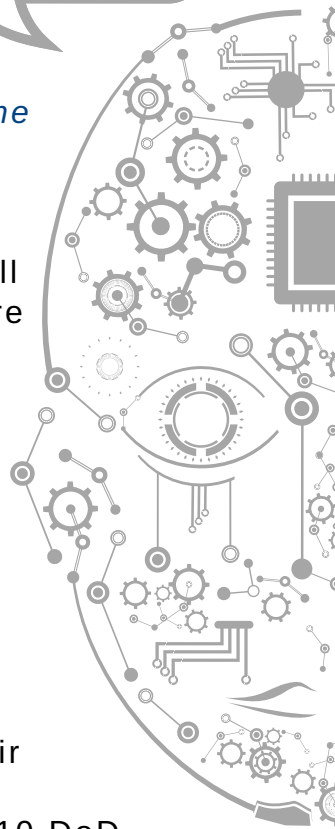
Ah, you're thorough. I should've known we had that in common. All right, let me back up and tell you why this is so critical—and where to begin.

Remember Your Old Friend NIST SP 800-171?

These are the cybersecurity requirements that government contractors and their subcontractors have been following since 2003. The CMMC was recently created to enhance this already existing compliance, in conjunction with the Defense Federal Acquisition Regulation Supplement (DFARS) requirements.

Why? The government relies on you—its contractors—to keep their Controlled Unclassified Information (CUI) secure. No pressure! Unfortunately, there's a good chance you are among the 9 out of 10 DoD contractors who fail compliance (or 8 out of those 9 who are deemed deficient in implementing basic cybersecurity controls).

What this means for you is that if you don't get certified, your organization's DoD contract work is on the line. The CMMC is drastically changing RFI and RFP requirements, thus impacting which companies, contractors, and subcontractors can be awarded contracts.



Think of the CMMC as a Cybersecurity Software Update

It's like an iPhone software update. You don't necessarily have to opt in, and at first you won't notice much of a difference if you don't. But soon, as your apps adapt to the new operating system, you'll lose access to many features—and you'll miss out on new ones.

Similarly, CMMC is an update that will have long-term repercussions if you don't oblige. This upgraded model is a 5-level certification program required for all personnel handling sensitive federal information like Federal Contract Information (FCI) and CUI. Version 1.0 was released on January 31, 2020, and as subsequent versions roll out, more and more opportunities will be at stake. By 2026, the DoD expects all contracts to contain CMMC requirements. Moreover, while right now the CMMC model is only applicable within the DoD, many speculate that it will eventually expand to the Federal sector.

Getting the CMMC helps to ensure your company's success and longevity. Needless to say, it's worth the investment.

Let's Get Technical

If you've made it this far, you understand the urgency to become compliant under CMMC. But before you welcome your new best friend with open arms, let's look at the logistics. The CMMC is the DoD's solution for unifying the range of cybersecurity standards that exist under DFARS, making it easier to enforce a top-down approach over who has access to sensitive information and to limit federal cybersecurity risk. So naturally, this friendship is not quite unconditional.

Make or Break Conditions:

- **DIY is a no-go.** Unlike other compliance assessments, there is no self-assess option for the CMMC. Each CMMC award must be provided through the CMMC Accreditation Body (AB) which will oversee the training, quality, and administration of the C3PAOs.
- **All hands must be on deck.** Anyone employed by your company, including other contractors and/or subcontractors, must also be certified. Subcontractors, however, do not need to obtain the same level of clearance as their prime.
- **It only applies to unclassified networks.** This certification is only relevant to those that handle, process, and/or store FCI or CUI. What the heck *is* considered CUI? No one really knows, so it's best to assume your work falls in this category. The handling of classified information falls under different safeguards.

- **It's not necessarily one-and-done.** Each certification is valid for 3 years. But even after you get certified, if your company experiences a security breach during a contract, then you may run the risk of a CMMC re-assessment. Only under exceptional circumstances will you lose the CMMC certification, but prepared to use this methodology throughout your contract.
- **One size does not fit all.** The CMMC accounts for varying security levels as not all DoD contracts are the same. Each RFP will reflect one of five levels of clearance needed to obtain the contract:
 - Level 1: Basic Cyber Hygiene
 - Level 2: Intermediate Cyber Hygiene
 - Level 3: Good Cyber Hygiene
 - Level 4: Proactive
 - Level 5: Advanced/Progressive

“Hold up Ava, this just got complicated. How do I know if my company is prepared for the appropriate level?”

Another great question! Have I mentioned how much I appreciate your attention to detail? The certification process, consisting of cyber audits and risk assessments, can advance over the five security maturity levels. Speak with a CMMC accreditation body to learn the type of security clearance that you require so that you can move forward without any business disruptions. Hot tip: my sources tell me that most contracts will require at least Level 3 clearance.

Get Ready, Get Set...

After you've determined the level of security clearance you'll need, a self-assessment test will highlight any areas in a cybersecurity program that need to be addressed before the actual audit. While an analysis could be done by an in-house IT team, bringing in a third-party consultant to conduct it can be more effective. A consultant can also help create a GAP analysis plan to address the problems.

Get Certified!

Once you're confident you have adequate cybersecurity protocols in place, along with the necessary documentation, you're ready to be assessed by the CMMC Accreditation Body.

Need Some Guidance?

This all may sound a bit daunting, so let's end on some good news. Avatara has a plan of attack in place. With our CompleteCloud Platform, DoD contractors and subcontractors can get Level-3-compliant in just 30-60 days. We're even working with approved auditors to secure an economy of scale package for our clients.

All this to say, don't worry; success is accessible to all. With Avatara by your side, you've got this! **E-mail info@houstoncompleteit.com to begin CMMC assessment preparation today.**

