So You Need to Comply with NIST 800-171 & CMMC

A GUIDE FOR CHOOSING THE MOST APPROPRIATE ROUTE FOR YOUR ORGANIZATION'S JOURNEY

EDUCATIONAL ARTICLE

VESTIGE
Digital Investigations

So You Need to Comply with **NIST 800-171 & CMMC**

While some would argue that an organization's compliance with DoD Cybersecurity regulations NIST SP 800-171 and the newly minted Cybersecurity Maturity Model Certification (CMMC) are arduous requirements, the truth is that's an inaccurate perspective.

For cybersecurity practitioners, we tend to feel these frameworks are the bare essentials – representing Best Practices that all organizations should be following to protect their own sensitive information – let alone Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Regardless, you've rightfully come to the conclusion that you need to comply (forced or unforced) and as such are now looking to determine how to get there.

Our Adversaries Want Our Information!

It is no secret that our adversaries are always interested in gaining any upper-hand that they can. If that means stealing intellectual property, or gaining access to sensitive defense information – even if it means breaking into our computer systems – so be it. If all of our Nation's sensitive information were stored in one central system and we put all of our Nation's resources into securing that information, we might be in a better place than we are. The fact of the matter is that's not how it works. Intellectual property and our sensitive information is more often found in the hands of Primes and Subcontractors strewn around a delicate balance of computer systems – most of which are not adequately secured for the organizations' own sensitive information, let along the information entrusted to it by the government.

> *The theft of intellectual property and sensitive information undermines our nation's defense posture and economy. Global costs last year are estimated at $600 billion, with an average cost per American of $4,000. It is time for action.*
>
> ***-CMMC ACCREDITATION BODY***

The DoD's initial attempt at bringing this under control, NIST 800-171, has awkwardly been met with resistance or downright lack of awareness that organizations need to follow it. And while there are penalties for non-compliance, they are back-end loaded – with the damage having already been done by the time it is determined that an adversary has gained access and exfiltrated sensitive information.

Enter CMMC

CMMC takes things in a different direction. Gone are the days of simply self-assessing your compliance with NIST 800-171 – for many companies certification now requires an outside assessor (CMMC Third Party Assessing Organization, C3PAO for short) to agree that you have the appropriate controls in place. And even if you are one of the companies that can self-attest – recognize the stakes have been raised by requiring attestation by a Company Officer. Gone are the days of back-end loading the requirements – as a CMMC-designated contract requires, for the most part, entities working on the contract to be certified at or above the maturity level required by the contract prior to being awarded the contract. So, we're righting the equation and putting the horse back in front of the cart! There are a number of other nuances that need to be taken into consideration, including understanding the difference between Federal Contract Information (FCI) and Controlled Unclassified Information (CUI); what the various Maturity Levels mean; and the addition of Processes into the mix – including much more poignant policies, procedures, plans, etc.

Suffice it to say, the bar has been raised. And while this is a good thing overall for the security of our Nation's sensitive information – many, many organizations are woefully unprepared for this change. What's worse is there's a lot of misunderstanding about what it takes to become compliant. Misunderstanding about the timing, the requirements, and most notably how to actually implement the practices and processes in such a way as to pass the assessment and obtain your certification.

Like most things in life that are perceived to be "hard", everyone is looking for the silver bullet...the magic solution that can be implemented with minimal effort. Unfortunately, there is no easy button on this one. Sure, there are all kinds of solution providers that can make it easier, but there will be no simple wave of the magic wand and you're now compliant.

EVALUATING YOUR OPTIONS

Which leaves us to understanding what your options are and what makes most sense for your organization. First, understand that only about 50% of the requirements of CMMC are true "technology" requirements. Roughly 25% of the requirements are "administrative" (think policies) and another 25% are "operational". When you understand that, you can start to understand why no silver bullet can address it all.

So, what to do? In short, here are your most viable options:

- Do-It-Yourself
- Work with an outside IT company
- Hire a Cybersecurity company to assist
- Engage a Registered Provider Organization (RPO - part of the CMMC ecosystem)
- Bring in a Certified Third Party Accrediting Organization (C3PAO - also part of the CMMC ecosystem) in a consultative approach
- Engage with a CMMC Expert Solution Provider that specializes in Cybersecurity, Compliance and the CMMC (RPO or C3PAO)

DIY: Do-It-Yourself

The good news about the CMMC is that there is absolutely no requirement that you use professionals to prepare your organization for the certification. Many organizations will, in fact, choose this route. The advantages of course are that cash outlay for outside services is minimized if not eliminated altogether. If you are considering going it alone and using internal IT staff, internal compliance individuals or others to prepare for compliance, you'll want to ensure that you set yourself up for the best success. Compliance, in general, is a tricky thing – as you need to make sure in reviewing the framework's control objectives that you thoroughly understand what those requirements really mean. Far too often, I have seen organizations "believe" they know what the requirement is, proceed to implement their perceived solution, only to find out that they had woefully misunderstood the requirement. I've actually seen this go both ways – believing that what they're putting in-place is enough to comply with the requirement and putting in-place things that far exceed the requirement.

Even more important, however, is ensuring that those that are involved have had experience with an evidence-based assessment. The job of an outside assessor, such as the C3PAO, is to evaluate your organization in enough detail to form an opinion on whether you have the required controls in-place and working as designed. This can be a tall order, considering that the C3PAO needs to collect enough evidence to put into their workpapers when they turn the assessment results over to the CMMC Accreditation Body (CMMC-AB). From there the Quality Assurance assessors of the CMMC-AB review the C3PAO's workpapers (including evidence) to come to the same conclusion as the C3PAO as to whether your organization has achieved the requirements. And what is that evidence?

The CMMC-AB has provided guidance to the C3PAOs that for each and every control objective, the C3PAO needs to collect and document a minimum of two pieces of corroborating evidence – with no more than one piece of evidence coming from each of: interviewing subject-matter experts, direct observation of a practice/process being carried out, or testing.

The Outside IT Company

Choosing to work with your outside IT company can have a lot of benefits as well. After all, they know your environment. They're probably extremely knowledgeable about the practices and processes in-place and in fact are likely part of the process. If you subscribe to a Managed Service Provider's (MSP) service, it is quite likely that they have put into place a lot of the best practices that are encapsulated in the CMMC framework. This can save time and effort, which translates into less cost. The big consideration here is ensuring that they understand the cybersecurity requirements, interpret the framework's control objectives correctly and understand the nuances of the CMMC framework. There's also the subtle, but pesky little issue of whether there's a perceived conflict of interest – after all, if you expect them to have already put the best practices in-place, will their assessment accurately reflect the true status of your environment if their own performance would be called into question?

The Cybersecurity Route

So you've properly recognized that CMMC is about information security and cybersecurity is a type of information security – so what about hiring a Cybersecurity Professional? Bravo. This can be an excellent choice. But just like any profession (think medical, legal or even the broader stroke of IT), specialization is key. There are many facets to cybersecurity – implementation of software or hardware solutions, monitoring, architecting a secure system and even compliance. Your first task in evaluating a Cybersecurity Professional is ensuring that they focus on compliance – after all, CMMC is all about complying with the framework. Additionally, you need to ensure that they are familiar with the nuances of the CMMC framework. While the CMMC framework is "non-prescriptive" (meaning it tells you WHAT you need to do; but doesn't tell you HOW to do it), there is vast room for interpretation…at least until it comes time for the C3PAO to evaluate the environment. Ensure that any Cybersecurity Professional that you evaluate has intimate knowledge of the framework. Familiarity with FAR and DFARS rules will help ensure that they understand the seriousness and sensitivity of the requirements.

Registered Provider Organization

The CMMC ecosystem includes a number of roles and entity-types that may prove to be very useful in your CMMC journey. Registered Provider Organizations or RPOs are required to employ or align with Registered Practitioners who have undergone specific training around the CMMC framework and have had to pass a competency test. This helps ensure that they have the baseline knowledge to appropriately advise Organizations Seeking Certification (you!) on what the control objectives of the framework mean, how the certification process works and shows a level of commitment to the CMMC process that other previously mentioned options don't address. Finally, RPOs are bound to a code of conduct consistent with the CMMC Accreditation Body's viewpoint. There's a lot of positives in choosing this route. One thing to watch for – what experience do they have on the remediation side? There are a lot of entities that can do a great job assessing an organization and telling you whether you are in-or-out of compliance (the "what"), but don't know how to get you over the finish line.

C3PAO as a Consultant

Another excellent choice is hiring a C3PAO in a consultative role. While ethics and requirements of the CMMC prohibit a C3PAO from being both a consultant and the certifying assessor for the same entity, there are no restrictions on a C3PAO assisting non-conflicting clients with their CMMC preparedness. As part of the CMMC ecosystem and the ones responsible for making a determination of an organization's fitness in achieving CMMC, C3PAOs, like RPOs, can be a great choice. They absolutely understand the nuances of the framework which can be a huge help in getting your organization ready. Like the RPO, make sure they have deep experience with the remediation and being able to answer the "how".

CMMC Experts: Cybersecurity + Compliance + RPO/C3PAO

Lastly, you could engage with a Professional Solution Provider that offers the best of all worlds – Cybersecurity + Compliance + CMMC Expertise. There are Cybersecurity Professionals that specifically focus on compliance – that understand the intricacies of compliance frameworks like CMMC. They've conducted hundreds of engagements assessing, advising and preparing their clients to meet compliance with a variety of frameworks. This gives them a perspective on what works in a wide range of organizations and the specific situations that an organization finds itself. In essence, they understand the "how". Couple this with being an RPO or C3PAO and you've found yourself a rare solution. This kind of organization has demonstrated its commitment to the CMMC ecosystem, will understand the nuances of the requirements (the "what") and has the requisite experience, know-how and expertise to implement (the "how"). The downfall? Perceived cost. These organizations aren't cheap. However, when put into context, "if you think hiring an Expert is expensive... wait until you've hired an amateur!" Or, as the old adage goes..."you get what you pay for".

If you think hiring an Expert is expensive...wait until you're hired an amateur!

The Wrap Up

Achieving CMMC is likely a big deal for your organization – otherwise, why take on the effort to do so? With that much at stake, it behooves organizations to carefully plan their CMMC journey.

What you don't want to do is engage the C3PAO for your certification assessment only to find that you are not adequately prepared. Otherwise, you're relegated to having to repeat the process over – a costly mistake. And for those organizations that can self-attest, you don't want to be in a situation where a Company Officer is attesting to having the controls in place, only to learn too late that the controls are not in-place, as there are financial, civil and even possibly criminal penalties.

Keep in mind, preparing for CMMC in-house can easily take 12 to 18 months. With an expert, that can be pared down. Choosing the right path forward as you start can have a profound impact on the success of your journey.

Damon Hacker, MBA, CISA CSXF, CMMC-RP, is a principal and Expert at Vestige Digital Investigations, the leading compliance-driven Cybersecurity and Digital Forensics solution provider. Vestige is an RPO with RPs on staff, has deep experience with NIST 800-171 and CMMC and works with domestic and international clients on their cybersecurity compliance. Damon is an often sought-after speaker on CMMC/NIST 800-171 compliance, cybersecurity, incident response and digital forensics.

VESTIGE
Digital Investigations

For more information Contact us today
800.314.4357 or info@vestigeltd.com