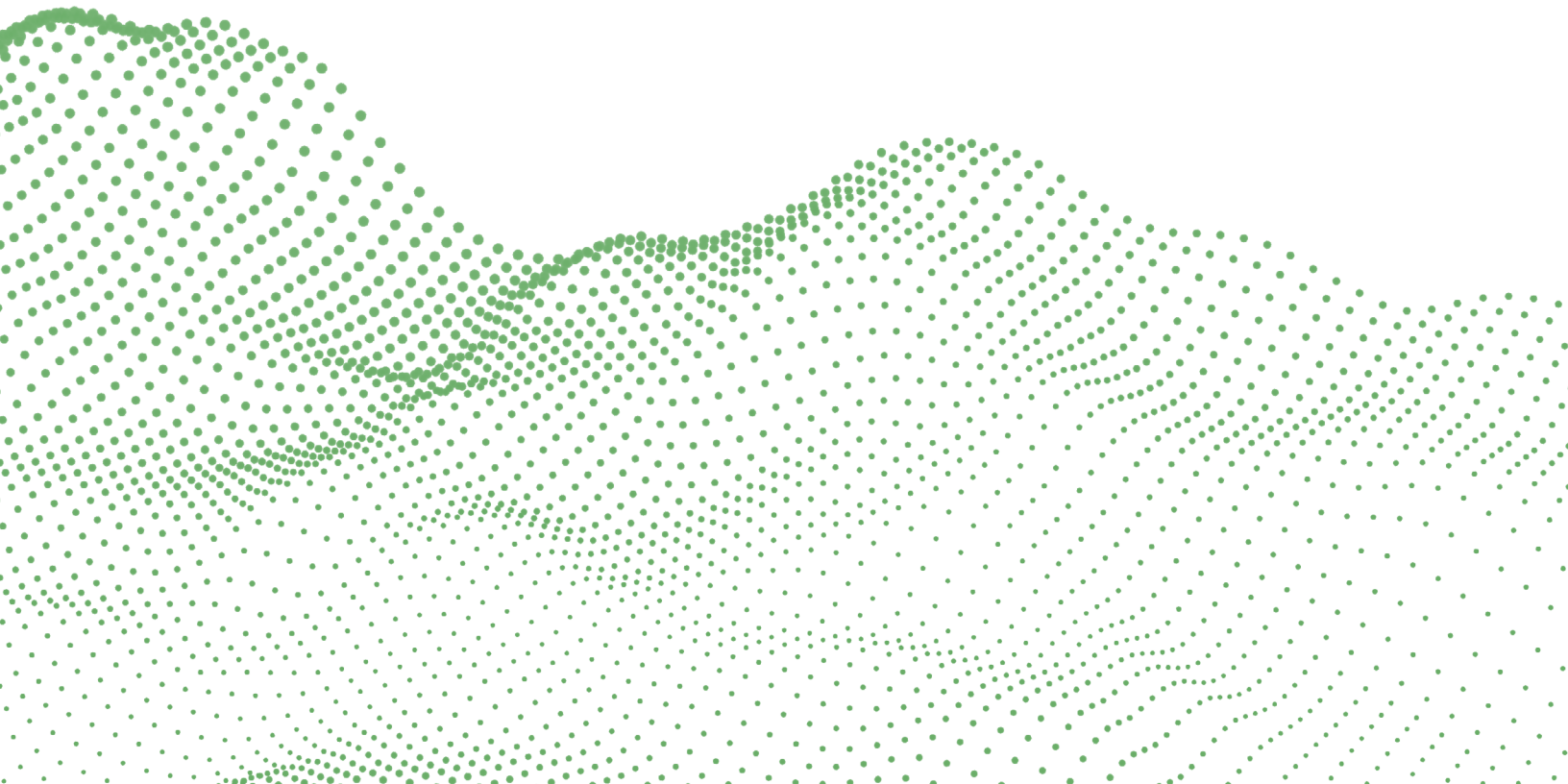
GROVE TECHNOLOGIES

Cybersecurity Maturity Model Certification

What it is and what it means for your Small to Mid-Sized business

Whitepaper

Version 1.0, January 2021



About

We work with clients big and small across a range of sectors and we utilize our resources to ensure that your problems are handled with care. We believe that analysis of your company and its systems is key in responding effectively to your systematic needs and we will work with you to fully understand your business tech needs to achieve the greatest amount of success as possible so that you can see a true value from your tech investment.

We have a number of different teams within our agency that specialize in different areas of business so you can be sure that you won't receive a generic service and although we can't boast years and years of service we can ensure you that is a good thing in this industry. Our teams are up to date with the latest technologies, media trends and are keen to prove themselves in this industry and that's what you want from an technology agency, not someone who is relying on the same way of doing things that worked 10 years, 5 years or even a year ago.

Whatever the level of support you require, we are sure that we will have a package that meets your needs. All of our virtual professionals are highly experienced in the areas in which they work and have been through a thorough recruitment process to ensure they deliver to the high standard that you would want for your business.

We will work with you to fully understand your business and your technology needs and digital strategy. Using the outcomes from the Technology Analysis, we will put together a plan for the most effective technology strategy to get the best results for your business

1. What is the CMMC and how did it come about?

The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense's (DoD) latest cybersecurity program designed to ensure that cybersecurity controls and processes adequately protect Controlled Unclassified Information (CUI) that resides on Defense Industrial Base (DIB) systems and networks. The DIB consists of all suppliers of DOD related services including primes / subs / consultants that provide any type of service on a DOD related contract.

The DoD implemented requirements for safeguarding CUI information and cyber incidents through the release of Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 in October 2016. The DFARS directed DoD Contractors to self-attest that adequate security controls were implemented within contractor systems to ensure that CDI confidentiality was maintained. The security controls required to be implemented by the DFARS are defined within the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The DoD required that the entire defense industrial base submit a self-assessment in November 2020 to baseline their cybersecurity due diligence to understand what the current baseline is like across the industry.

DFARS is entirely reliant upon self-assessment by the company itself, there was never a formal attestation to ensure the necessary cybersecurity controls were in place. Upon implementation of DFARs, several notable breaches including ransomware attacks and attacks on DoD contractors have occurred which required the DOD to rethink its strategy thus the basis of CMMC came about.

The Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD (A&S)) started the process of creating the CMMC in March 2019, with the finalization of the CMMC v1.0 occurring in late 2020. Starting in 2021, the defense industrial base will be required to become CMMC certified to win DOD contracts at the required maturity level that is stipulated in that contract. The DoD is taking a phased-in approach by only requiring a small amount of DoD contracts to have CMMC requirements in 2021 with the number of contracts increasing incrementally until all new DOD contracts will have a CMMC requirement by 2025.

PITFALL #1

Unlike other types of cybersecurity compliance frameworks and standards such as NIST CSF, ISO 27001, and SOC 2 Type 1, a maturity model has some very rigorous requirements that organizations struggle to comprehend about how to meet them.

The CMMC has some unique and rigorous requirements that organizations may not have the experience or expertise in-house to properly prepare and maintain the accreditation that is required. Stating the obvious, the CMMC is only required for organizations that provide services to the DoD or they are a DoD contractor.

The CMMC is not required for organizations that support non-DOD agencies at this time. However, this might change soon given some of the high-level statements that have come out of the General Services Administration (GSA) about CMMC requirements down the road.
In a maturity model, an organization must show that cybersecurity is ingrained within its organizational culture. This needs to be reflected in both policies and procedures as well as the

implementation of solid cybersecurity practices and cyber hygiene requirements as mandated in CMMC. The CMMC is not a snapshot in time of cybersecurity practices; it is a continual improvement and evolution in the defined baseline of the organization for their cybersecurity requirements. Before a CMMC assessment, an organization needs to be sure that all of the requirements for the maturity level they're going for have been fully implemented and documented with artifacts available for a defined period.

The recommended defined time period is at least 90 days before going to an assessment, but this might have to increase based on the maturity level and or complexity of the gap that has been remediated before the assessment.

PITFALL #2

CMMC is 100% pass/fail assessment. Unlike other cybersecurity maturity certifications where you can have findings or failures yet still passed your assessment, the CMMC requires that all of the control requirements for that maturity level be satisfied.

At maturity level 3, 130 required practices must be implemented by the organizations seeking certification. if 127 are compliant and three have findings with those findings being considered failures by the C3PAO, then the organization would not be certified at maturity Level 3 instead of being certified at material level 2.

It is this level of complexity and attention to detail that requires an organization seeking certification to have the proper knowledge of compliance requirements as well as the specialty in implementing CMMC specific security engineering and architecture controls to satisfy these requirements.

The Cybersecurity Maturity Model Certification Path at Grove Technologies

At Grove Technologies we take cybersecurity very seriously and we work hard to ensure that you are put on the right path from day one. Trust our team of advisors to get you over the CMMC finish line.

Step 1

Understand the CMMC Requirements set forth by the CMMC-AB.

Step 2

Identify your scope. Find out what is FCI, CUI in your organization from your PRIME.

Step 3

Identify the Maturity Model that you need to be in compliance with. CMMC Level 1, 2, 3, 4 or 5.

Step 5

Preassessment with a registerd practitioner organization like Grove Technologies

Step 6

GAP Analysis of your organizaion. Start to identify problems, and assess overall risk.

Step 7

Document a Procedure, Policy and a Plan for each control family for your desired CMMC Level.

Step 8

Set a budget for each of the control families to show budgetary and overall cybersecurity maturity.

Step 9

Gather artifacts and ensure that you can provide documentation to an assessor proving your maturity posture.

Step 10

System Hardening of all of your SaaS based tools in conjunction with your practices, policies and plans.

Step 11

Proactive monitoring to ensure overall health of your systems while following the practices, policies and plans.

Step 12

Assessment Preperation. Run a post assesment with a registered practiioner organization like Grove Technologies

Assessment

Conduct an assessment with a C3PAO listed on the CMMC-AB Marketplace portal

Details of the CMMC Framework & What Level Am I Required to be Certified at?

Level 1 – Basic Cyber Hygiene: Includes basic cybersecurity appropriate for small companies utilizing a subset of universally accepted common practices. The processes at this level would include some performed practices, at least in an ad hoc manner. This level has 35 security controls that must be successfully implemented.

Level 2 – Intermediate Cyber Hygiene: Includes universally accepted cybersecurity best practices. Practices at this level would be documented, and access to CUI data will require multi-factor authentication. This level includes an additional 115 security controls beyond that of Level 1.

Level 3 – Good Cyber Hygiene: Includes coverage of all NIST SP 800-171 Rev. 1 controls and additional practices beyond the scope of current CUI protection. Processes at this level are maintained and followed, and there is a comprehensive knowledge of cyber assets. This level requires an additional 91 security controls beyond those covered in Levels 1 and 2.

Level 4 – Proactive: Includes advanced and sophisticated cybersecurity practices. The processes at this level are periodically reviewed, properly resourced, and are improved regularly across the enterprise. Besides, the defensive responses operate at machine speed and there is a comprehensive knowledge of all cyber assets. This level has an additional 95 controls beyond the first three Levels.

Level 5 – Advanced / Progressive: Includes highly advanced cybersecurity practices. The processes involved at this level include continuous improvement across the enterprise and defensive responses performed at machine speed. This level requires an additional 34 control.

Each maturity level builds upon the previous maturity levels as they increase. So, for example, if an organization seeking certification wants to go for a maturity level 3 they must implement all of the CMMC requirements for levels one and two. Determining what maturity level your organization needs to receive can be a difficult question without proper guidance.

If your organization only handles FCI information, then you should only seek a maturity level 1 certification. If your organization handles, stores, and transmits CUI information then you should seek a maturity level 3 certification. Maturity level 2 is considered a step level between one and three but should not be attempted to obtain certification at that level. Maturity levels four and five are for organizations that are required by the DOD contract or have a contractor relationship potentially with a prime that might stipulate that.

The organization might want to go for a level four or five if they feel that they are ready with a solid and mature cybersecurity program or for the sake of winning advanced DOD contracts. At this time, we generally do not recommend organizations seek certifications at level four or five due to the unnecessary and unclear pathway that might be required for current DOD contracts unless it is expressly required. The majority of DOD contractors will only be required to have maturity level 1 if they handle FCI information only. However, many DOD contractors handle CUI information which would then raise the level to maturity Level 3 as our base-level recommendation. If an organization is not completely sure about what maturity level is

required, it is best to seek guidance from their government contracting officer if they have an existing contract with the DOD or visit the official CMMC website.

CMMC – In Practical Terms

Let us put the CMMC in practical terms. Let's say an organization is seeking certification at maturity level 3 because they handle CUI information and they want to bid on new DOD contracts that require that maturity level. So, for ML3, they will need to have a Policy, Procedure and Plan for each of the 17 following control families.

- Access Control
- Asset Management
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Security
- Recovery
- Risk Management
- Security Assessment
- Situational Awareness
- Systems and Communications Protection
- System and Information Integrity

Can your CMMC Team do this?

Not only is our team of CMMC experts CMMC-AB certified and approved, we are comprised of CISSP professionals and systems engineers to help ensure that your policies are written correctly and your systems are hardened proficiently all by the same dedicated staff.

51

DOCUMENTS

That means they will have a total of 51 (17 * 3 = 51) documents to address CMMC Maturity Level 3

130

PRACTICES

To make things more concrete, there are 130 unique "practices" for ML3 across those 17 control families

A policy and procedure for each control family should address the applicable practices respective to that family. Practice AC.2.016, "control the flow of CUI per approved authorizations" should have both a policy and procedure portion written for it as part of the overall Access Control Policy/Procedure required.

Not also will an organization be required to have a policy, plan, and a procedure for each control family at maturity level 3 they will need to ensure that all of the required controls are properly implemented and configured to properly address those requirements.

This is where the security engineering side of the CMMC kicks into overdrive.

A shortlist of technical requirements for a maturity level 3 might include:

- Enabling MFA
- Using a SIEM tool
- Using Fedramp Cloud Services
- Vulnerability Management Program
- Secure SDLC procedures (if applicable)
- Incident Response/Contingency Plans
- Data Storage and Retention Requirements
- FIPS 140-2 Encryption Requirements

Just to name a few.

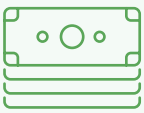
This shortlist of requirements is only the tip of the iceberg for security engineering areas of importance for maturity level 3 that must be addressed and implemented by the organization seeking certification. If the organization is not adequately prepared or does not understand the subtle nuances and compliance requirements of CMMC they might inadvertently implement a misconfigured control which might lead to a finding or a costly oversight that would have to be corrected. This is where Grove can help organizations drive home CMMC implementations and get prepared for their assessment at the desired maturity level.

How Grove can help!

No matter your organizational cybersecurity baseline, Grove can help you achieve your desired CMMC maturity level.

Our Process

One of the first things we like to do is to perform a gap analysis on your company's existing policies and procedures against the desired CMMC maturity level your organization is seeking to determine what level of compliance and maturity you're currently at. We will go through all of your policies and procedures to determine whether you're compliant, not compliant, or have gaps as aligned to the CMMC model and prepare a remediation plan with recommended steps for implementing the required gaps as necessary. If your organization has never had a gap analysis performed it is recommended to have this done to have another pair of eyes to look inside at what your organization currently does to determine the cybersecurity baseline for which you must achieve.



Cost Effective Solutions

OUr innovatave approach to CMMC saves you money by targeting the systems you need to harden on day one. Our risk assessment will give you the tools you need at a fraction of the cost of the other guys.

If your organization does not have any cybersecurity baseline or very little in the way of documentation, Grove can help your organization document the needed policies and procedures for CMMC against the 17 control families at the various maturity levels for each practice. This might include areas such as access control, identity access management, systems, and network communication, incident response, configuration management, and personnel security to name a few areas. Your policies and procedures must reflect the best practices and recommendation in which are vCISOs can address. Our vCISOs have significant experience with CMMC, NIST 800-53, NIST 800-171, and NIST CSF controls that apply to the maturity model your organization is seeking.

Grove can also assist your organization in implementing security engineering in various cyber-

security architecture requirements as mandated from gap analysis findings or best practices required for the maturity level you are seeking. Our Grove vCISOs can work with your infrastructure providers or can utilize our services as a managed service provider to implement and harden the needed control requirements for the maturity level required. Our common security engineering services include vulnerability management such as patching, cloud service provider administration and hardening based on what services your organization uses, or identity access management including access control requirements for various on-premises and cloud-based services.

Grove can also provide long term or as needed continuous monitoring for security engineering and compliance requirements for your organization. CMMC requires that the organization maintain their compliance perform continuous monitoring and continual improvements on their cybersecurity baseline as needed. Continuous monitoring activities include things such as audit logging and monitoring, vulnerability management and remediation, significant updates to policies and procedure, and how it affects your cybersecurity baseline to name a few key areas. Grove can help your organization realize these significant changes and maintain these activities as needed as a turnkey, on-demand solution.

What makes Grove stand out from the competition? Simple, our level of expertise and dedication to our clients. Grove is a registered practitioner organization (RPO) with the CNMC Authorizing Board (CMMB-AB) which means we are certified to provide CMMC level support to organizations seeking certification. Grove also employs several registered practitioners who have been trained and are updated on the latest CMMC requirements and understand the subtle nuances of NIST controls and security engineering implementation guidelines.

Our employees are also certified in a wide variety of other cybersecurity disciplines including pentesting, cloud security, cloud architecture with several of our employees having a CISSP.

Finally, Grove is dedicated to helping organizations get certified so they can support the essential mission and business functions as mandated and required by the DoD to ensure our strategic national defense. At the end of the day what is most important is to ensure that we can preserve and strengthen our national defense resources through a rigorous cybersecurity program to prevent bad actors and foreign threats from compromising our essential systems. This is something we here at Grove feel very strongly about.

Still, have additional questions about the CMMC? Schedule an appointment with us today! Our Grove consultants can help you determine where your CMMC baseline is and make the best recommendations that are both impactful as well as cost-efficient.

Client Testimonial

"Their responsiveness is second to none and they clearly take pride in the service that they provide.

I can recommend this business with full confidence and look forward to continuing our partnership."

-- Eleven Peppers Studios

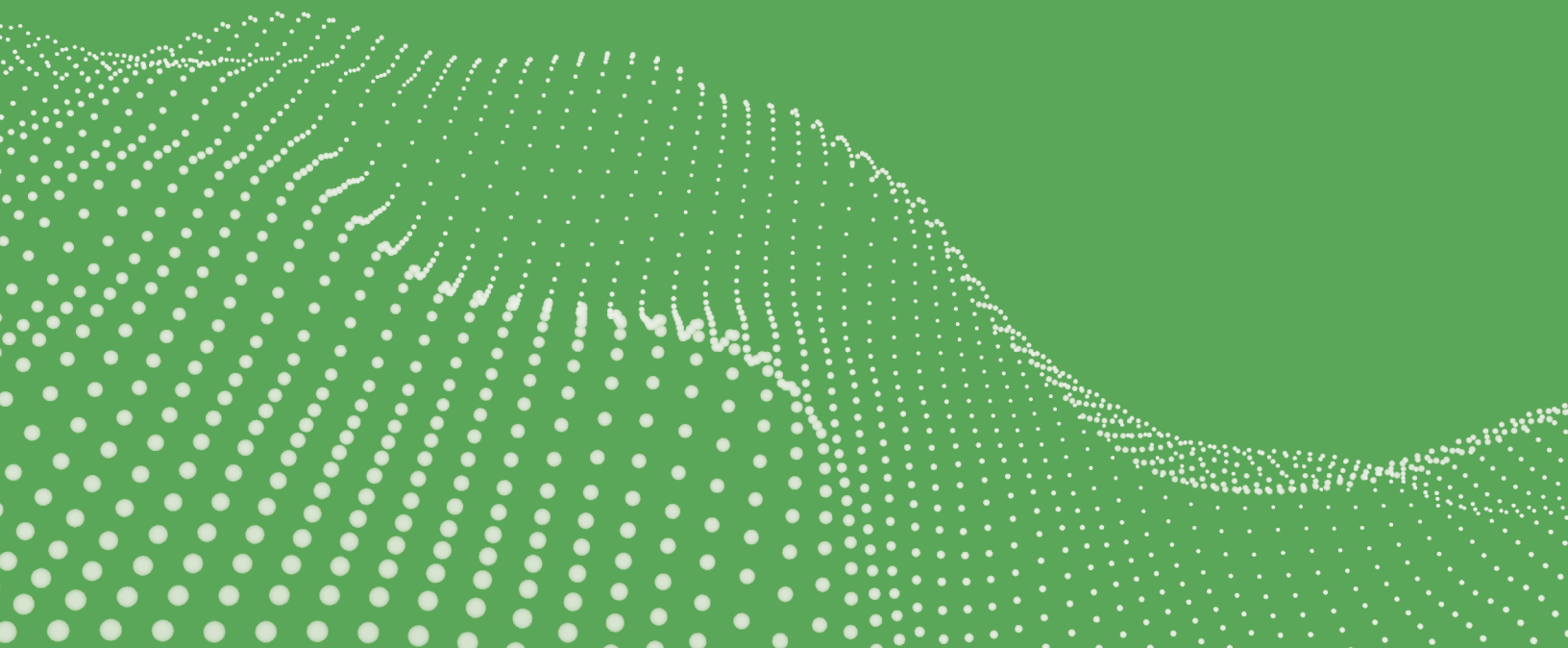
GROVE TECHNOLOGIES

CMMC Consulting done right.

We take the fear out of preparing for a CMMC assessment. We provide, fair, honest and reliable CMMC guidance provided by CMMC Registered Practitioners.

Contact us today and see how we can help you!

(888) 253-9103



Team

Jon Brown

CEO & CMMC RP

jon@grovetech.co

Jon is a charismatic leader, entrepreneur, teacher & mentor who helps businesses take their Mac, Cybersecurity & Networks to the next level.

Scott Campbell

CISO, CCSP, CMMC RP

scott@grovetech.co

20 years of experience in providing executive consulting for cybersecurity and IT clients needs in a vCISO role for compliance, CMMC and more.

Michael Tedesco

CISO, CISSP

michael@grovetech.co

With a background in the US Coast Guard, Michael helps the needs of our

CISSP® Certified Information Systems Security Professional

CCSP® Certified Cloud Security Professional

CSSLP® Certified Secure Software Lifecycle Professional

EC-Council E|HA Ethical Hacking Associate

Contacts Us

Adress
1030 15th St NW Suite 1050w, Washington, DC 20005

Phone
(888) 253-9103
(240) 451-8688

Email
support@grovetech.co

Consultants Network