Brought to you by:

SteelCloud

CMMC

for dummies

A Wiley Brand

Understand CMMC compliance

Accelerate the CMMC compliance process

Reduce costs with automation

SteelCloud Special Edition

Jack A. Hyman

About SteelCloud

SteelCloud develops STIG, CIS, and CMMC compliance software for government customers and its contractors. Its products automate policy and security remediation by reducing the complexity, effort, and expense of meeting government security mandates. SteelCloud has delivered security policy-compliant solutions to military components worldwide, simplifying implementation and ongoing security and mission support. SteelCloud products are easy to license through its GSA Schedule 70 contract. SteelCloud can be reached at (703) 674-5500. Additional information is available at www.steelcloud.com or by email at info@steelcloud.com.

CMMC

SteelCloud Special Edition

by Jack A. Hyman

for dummies®
A Wiley Brand

CMMC For Dummies®, SteelCloud Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-81936-3 (pbk); ISBN: 978-1-119-81937-0 (ebk).

Some blank pages in the print version may not be included in the ePDF version.

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Ashley Coffey

Business Development Representative: Matt Cox

Contributors: Brian Hajost, Jamie Coffey

Acknowledgements

Special thanks to Karen Walsh for sharing her cybersecurity insights and compliance expertise.

Table of Contents

Introduction

To address the many cybersecurity challenges that face the Department of Defense (DoD) and its supply chain, the Cybersecurity Maturity Model Certification (CMMC) will be used as a single-source reference model to handle all security issues for unclassified information for nearly 300,000 DoD contractors. Currently, government contractors, with Defense Federal Acquisition Regulation (DFAR) clauses in their contracts, must meet strict compliance requirements. However, in the near future, all prime contractors and subcontractors will need to be certified to a minimum CMMC level. The DoD has made significant headway in positioning a combination of security frameworks into a unifying standard.

Based on NIST 800-171, the model focuses on more than just policy compliance. It aims to protect the government by securing the IT infrastructures operated by the contractors that comprise the Defense Industrial Base (DIB). Complying with the technical side of the CMMC requirements means hardening systems using the Security Technical Implementation Guides (STIGs) or the Center for Internet Security (CIS) Benchmarks. The IT side of the compliance process can be difficult and tedious. Why not try automation?

About This Book

Whether you're trying to understand the ABCs of CMMC, figuring out what your company needs to do to get certified as part of your DoD contractual obligation, or looking to better address compliance process automation, you've found the right book. You discover how to automate CMMC processes, to fulfill contractual requirements, speed up CMMC compliance, and reduce the costs of compliance and audits.

Understanding STIGs and how they align with CMMC's control requirements may be a bit confusing. If you're bidding on a DoD contract or intend to, this book helps you begin identifying your automation needs, addressing ways to speed up CMMC compliance, and reducing the cost of STIG automation in your quest to be ready for more DoD work.

Icons Used in This Book

Icons call attention to themes as well as highlight significant issues you may want to steer clear of on your CMMC journey. In this book, I use the following icons:


REMEMBER

Remember icons are friendly references and suggestions to emphasize content worth storing in your brain for later use.


TIP

Tip icons give you information that helps you cut cost, save time, and much more.


WARNING

Warning icons help you address mission-critical topics to avoid costly mistakes. They can also help you stay on top of those business gotchas. Pay attention to these icons so you can avoid problems down the road.


TECHNICAL STUFF

CMMC and discussing STIG/CIS compliance can get quite technical. These callouts drill down into complex ideas. If you have a technical mindset, you may enjoy this info. If you don't, skip this content. Your knowledge won't suffer.

Beyond the Book

The body of knowledge that's available on the Internet is growing when it comes to CMMC compliance, and there is only so much I can squeeze into this book. To enhance your CMMC knowledge beyond what's offered in this book, check out these additional resources:

- **cmmcab.org**: The CMMC Accreditation Body (CMMC-AB)
- **www.acq.osd.mil/cmmc/draft.html**: Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification
- **www.steelcloud.com/configos-cybersecurity**: ConfigOS Command Center
- **www.steelcloud.com/cmmc:** SteelCloud for CMMC Compliance

IN THIS CHAPTER

- Defining CMMC compliance
- Understanding how CMMC applies to you
- Figuring out your CMMC maturity level

Chapter 1
CMMC 101

Depending on your company size and the types of contracting work, the Cybersecurity Maturity Model Certification (CMMC) program can be a complex process for contractors engaging with the Department of Defense (DoD). This chapter introduces you to CMMC and what you need to get certified.

What Is CMMC?

CMMC creates a set of cybersecurity best practices that needs to be implemented into mature processes. It draws from multiple cybersecurity standards, frameworks, and references. CMMC is a collaborative effort that includes the Defense Industrial Base (DIB), DoD, and research centers. The maturity model aligns processes and practices with a set of domains and then maps those domains to five CMMC levels that include descriptions and types of information protected. Check out Table 1-1 for more info.

CMMC maturity specifications and mappings consider processes and practices that include regulatory controls, types of information (Federal Contract Information [FCI] and Controlled Unclassified Information [CUI]), sensitivity, threats (such as Advanced Persistent Threats [APTs]), costs, technical and compliance complexity, and diversity measures across the DoD community.

TABLE 1-1 The CMMC Levels

Level	Processes	Practices	Types of Info to Protect
Level 1	Performed	Basic cyber hygiene	Protects FCI data
Level 2	Documented	Intermediate cyber hygiene	Protects some CUI data
Level 3	Managed	Good cyber hygiene	Protects CUI data
Level 4	Reviewed	Proactive	CUI data (also reduces the risk of APTs)
Level 5	Optimizing	Advanced/ Progressive	CUI data (also reduces the risk of APTs)

REMEMBER

The difference between FCI data and CUI data boils down to how the DoD classifies information. FCI data is a broad category of information not intended for public release. It's provided by, or generated for, the government as part of a contract for products or services. However, information the government provides to the public, such as public websites or payment processing activity, isn't FCI data. FCI data follows the minimum-security requirements outlined in the basic safeguarding clause 48 CFR 52.204-21. Virtually every DoD contract includes FCI data.

CUI data, on the other hand, is created or owned by the government. Also, other laws, regulations, or agency policies may already require companies to protect the information. CUI data excludes classified and sensitive information. To comply, follow the guiding principles outlined in the National Institute of Standards and Technology (NIST) SP 800-171 (see the next section for more on NIST SP 800-171).

TIP

Companies handling FCI data must meet CMMC Level 1 certification. Level 2 is a transition that starts putting protections in place required for CUI data. To handle CUI data, companies must meet CMMC Level 3 requirements for computer systems that store, process, or transmit CUI data.

How Does CMMC Apply to Me?

If you want to do business with the DoD or one of its prime contractors, you need to be CMMC certified at the appropriate

level required by your contract or prime contractor. If you plan to conduct business with the DoD, the Defense Federal Acquisition Regulation Supplement (DFARS) Clause 242.204.7012 states that if you're handling CUI data, you need to meet all 110 security controls listed in NIST 800-171. Both CMMC and the DFARS Interim Rule (see Chapter 3 for more) use NIST SP 800-171 as their foundations, which makes 800-171 the de facto basis for all cybersecurity best practices across the DIB.

Identifying Your Level

To identify your CMMC level, start with your contract because it *should* define the type of data you handle, but you still need to make sure that the contract is correct. The CMMC level requirement may also be set by the prime contractor.

To get certified, you need to know or document the processes and practices you have in place. Larger organizations often have many controls in place, but smaller contractors with less mature programs often haven't written down what they do. CMMC guides your organization to establish policies and procedures that create a series of achievable benchmarks that makes your cybersecurity programs effective. The good news is that you can start with the controls you have in place and add more controls and documentation. For instance, to meet Level 1 Basic Cyber Hygiene requirements, you need to perform practices, but to move to Level 3, you need to document everything you do. To go past Level 3, you have to enhance practices, take corrective actions, and proactively implement practices that protect CUI data from APTs.


REMEMBER

Reaching Level 5 isn't easy because you need to standardize and optimize your processes. Most importantly, your practices must be consistent across all systems that store, process, and transmit CUI data to protect information from APTs.

Are you Level 3 or above?


REMEMBER

If you have DFARS clause 252.204-7012 in your contract, you must meet the Level 3 minimum requirement because you're handling CUI data, as referenced in NIST SP 800-171. Some questions that can help you determine your level include the following:

- How does your organization store, process, and/or transmit the CUI data and encompass all its security requirements specified in NIST SP 800-171?
- Does your organization consider the 20 additional practices under CMMC to mitigate threats?
- Does your organization have an established plan to demonstrate basic management processes that support activities and practices for cyber hygiene? Does the plan integrate missions, goals, project plans, budgeted resources, required training, and stakeholder mapping?

If you've considered this list, you have a good start toward meeting Level 3 requirements.

Prime versus subcontractor

The DFARS Interim Rule (flip to Chapter 3 for more info) starts moving primes and subcontractors toward CMMC compliance. CMMC Level 3 includes all NIST 800-171 practices *and* 13 additional practices. Also, both CMMC and the Interim Rule include a "flow down," which means everyone is responsible for understanding the cybersecurity maturity of the companies they contract. As part of the DFARS Interim Rule guidelines transition, Plans of Action and Milestones (POAMs) are no longer supported; all 110 800-171 controls need to be implemented and documented.

REMEMBER

The DoD prime contractor is held fully accountable for knowing that their subcontracts are certified to the appropriate CMMC level based on the data the subcontractor handles. For example, a subcontractor may only need to handle FCI data. That subcontractor only needs Level 1 certification. If the sub will handle CUI data, the prime must make sure the sub is CMMC Level 3 certified. Primes normally need to be at least CMMC Level 3 certified but often may be Level 4 or 5.

Organizations must meet all the requirements specific to the CMMC level defined in their contracts with either the DoD or the prime contractors. An organization that needs Level 3 certification that meets Level 3 practice implementation but only Level 2 process implementation won't be certified to Level 3, only to the lower CMMC Level 2. So, prepare well in advance if the mandate from the agency is for the higher-level certification.

IN THIS CHAPTER

- Understanding key regulatory terminology
- Discovering how lower-level controls support CMMC
- Discussing the role of STIG and CMMC controls

Chapter 2
Understanding DIB Compliance Alphabet Soup

Federal regulations are notorious for their use of abbreviations, acronyms, and a whole lot of numbers. Almost every federal agency seems to have its own special language with dictionaries to help guide employees, contractors, and citizens. This chapter unravels much of the confusion around Defense Industrial Base (DIB) compliance lingo.

Learning Your Regulatory ABCs

Cybersecurity Maturity Model Certification (CMMC) compliance requires a crash course in key regulations. If you're a contractor, you need to know Federal Acquisition Regulation (FAR) terms and conditions. Organizations that plan on having Department of Defense (DoD) data on their systems need to learn about the Defense Federal Acquisition Regulation Supplement (DFARS). The basis of CMMC is the use of NIST SP 800-171 and SPS 172.

FAR

FAR guides government procurement in the United States and is codified in Chapter 1 of Title 48 within the Code of Federal Regulations, 48 CFR. Contracts with the DoD, NASA, and even top-level civilian agencies have at least one clause referencing FAR.

Where does cybersecurity fit? For every issued contract, contracting officers must insert a clause about handling information that resides on your IT systems. FAR § 52.204-21, nicknamed "The Basic Rule," defines the rules for protecting an inflow or outflow of data in an IT system. The rule creates the most basic United States government system security rules and best practices for all contractor systems that process, store, or transmit Federal Contract Information (FCI) data.

DFARS

All DoD contractors that process, store, or transmit Controlled Unclassified Information (CUI) data must meet DFARS minimum security standards to keep their contracts. DFAR 252.204-7012 provides a set of adequate security controls to safeguard information systems where contractor data resides and references NIST SP 800-171 (see the next section).

NIST 800-171 & NIST 800-172

The National Institute of Standards and Technology (NIST) builds many technical frameworks, one of which is a cybersecurity framework born under special publication (SP) 800. When it comes to CMMC, pay attention to two:

- **NIST SP 800-171:** With NIST SP 800-171, the focus is on protecting CUI that resides on nonfederal systems.
- **NIST SP 800-172:** NIST SP 800-172 takes security up just a notch. It tackles the confidentiality, integrity, and availability of CUI by evaluating highly sensitive programs, high-value assets, and advanced persistent threats (APTs). NIST SP 800-172's enhanced security requirements are the guiding principles for CMMC Level 4 and 5. Check out Chapter 1 for more on different levels.

Addressing Lower-Level System Controls: The Superglue of CMMC

The DoD uses CMMC to implement a tiered approach to auditing contractor cybersecurity. There are five different maturity levels (see more in Chapter 1). Although contractors have had to comply with NIST 800-171 since 2018, the DIB still suffers from cybersecurity incidents, which is why the DoD had to take a firm stance against prime contractors and subcontractors.

CMMC's laddered approach reduces the chance for a single point of failure in CMMC. Starting in 2021, contractors must be certified to a CMMC level. The more sensitive data you handle, the more cybersecurity expectations increase. In other words, as you handle more sensitive information, you need to put more practices into place. You can't jump from basic to advanced without a few pit stops along the way.

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S) has made it clear that security is foundational for all DoD acquisition. Security shouldn't be compromised for the purpose of cost, schedule, and performance.

To capitalize on existing resources and save contractors time, OUSD A&S built the CMMC framework around NIST SP 800-171. Both are built on three core tenants:

- **Adequate security:** All organizations must follow NIST 800-171's 110 security controls.
- **Contractual flow down:** Prime contractors and their subcontractors must meet DFARS and CMMC requirements. However, subcontractors won't necessarily be held to as strict of a requirement as prime contractors. At minimum, you must meet Level 1 baselines before moving onto the next ladder rung.
- **Incident response:** For CMMC Level 2 and up, you must follow a formal cyber incident reporting process. The audits assess your ability to prepare, detect, analyze, contain, and recover from an incident.

REMEMBER

Ultimately, CMMC is a big jigsaw puzzle that addresses regulations (DFAR 252.204-7012) along with a host of cybersecurity standards and best practices to create a single roadmap. Organizations can map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. The organization must fulfill each maturity level, in order, to reduce risk against cyber threats.

Getting from 800-171 to 800-53 to 800-128

CMMC starts with NIST SP 800-171, which covers all matters related to protecting CUI in nonfederal systems and organizations. NIST SP 800-171 references NIST SP 800 53 a lot — 102 references to be exact. NIST 800-53 sets out specific security and privacy controls for systems and organizations.

As if that didn't complicate things enough, NIST SP 800-128 presents a guide for security-focused configuration management of information systems. This publication crisscrosses with 76 derived references from NIST 800-53 and 7 derived references from NIST 800-171. In other words, all these different suggested best practices link back and forth to one another, which makes it hard to locate the required security technical controls.

Figure 2-1 shows how all these publications are connected and how they all lead back to NIST 800-128.

Like a treasure hunt, if you look hard enough, you can find the controls. In this case, NIST 800-128 is the technical control treasure you need. NIST 800-128 talks about the National Checklist Program (NCP), which is the technical security treasure at the end of your treasure hunt because now you can find the specific technical controls that get your company secure and compliant.

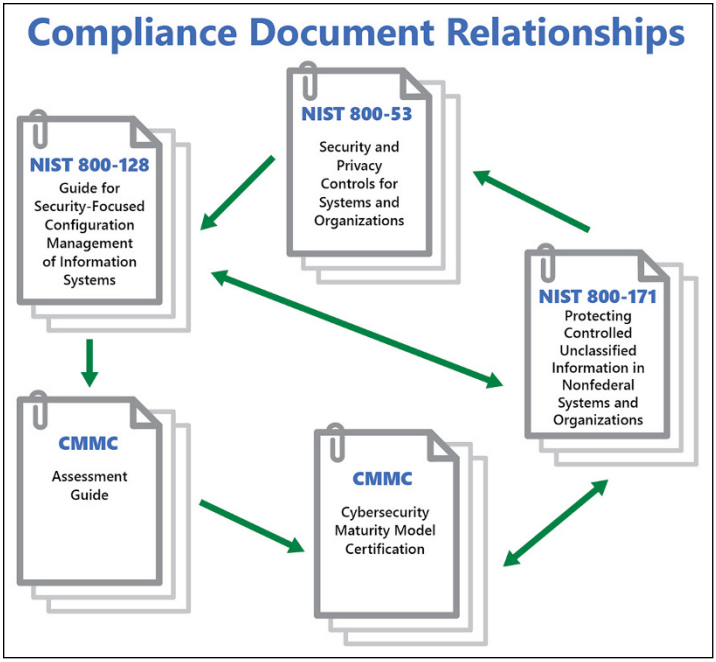

FIGURE 2-1: The relationship among the regulatory documents of CMMC.

Addressing CMMC Cyber Hygiene Standards with STIG & CIS Benchmarks

After you've found the treasure chest of NIST 800-128 (check out the preceding section), you need to figure out how to use it. The NCP is a United States government repository of publicly available security checklists, also called *benchmarks*, that detail how you can securely configure operating systems and applications. The list of approved authorities includes Defense Information Systems Agency (DISA) STIGs and CIS Benchmarks. They tell you how to configure your operating systems and applications to prevent security incidents.

WARNING

Whatever you do, don't implement STIGs or CIS Benchmarks manually. Errors are high, and the tedious work is expensive, so Automate, Automate, Automate. To achieve CMMC compliance, standardize your configuration process by using industry best practices and solutions.

Reduce IT vulnerability

NIST 800-128 explains that using well-written, standardized configurations can help you protect your data. Because NIST approves the STIG and CIS Benchmarks, it's much easier to use them as the recipe for compliance instead of making up your own configurations, documenting them, and then trying to defend them during your CMMC audit.

Set best practices

Set best practices and configurations for all your devices and software. System administrators can use STIG and CIS Benchmarks to prevent security incidents. These system-level configuration benchmarks exist for everything from operating systems to email clients to routers to printers. By using these benchmarks, you're already getting your environment more secure and knowing that you're working within DoD approved guidelines.

Standardize for consistency

CMMC maturity is all about standardizing your security practices and processes. Using standard configuration controls, like the STIG and CIS Benchmarks, is the fastest way to standardize your configurations and keep them up to date as the STIG and CIS policies are periodically updated to address emerging cyber threats. In other words, you don't need to start from scratch, and you can simplify ongoing cyber hygiene by implementing the latest STIG and CIS Benchmarks as they're published.

IN THIS CHAPTER

- Learning who you are
- Figuring out your needs
- Getting certified

Chapter 3
Mastering the Certification Process

You've decided to take the plunge and start preparing for your Cybersecurity Maturity Model Certification (CMMC) certification. Now what? Where do you even start? Getting your organization CMMC certified isn't a sprint around a racetrack; it's journey to get to the destination. If you've searched the Internet, you've probably found a lot of checklists, recommendations, and guidance on the process and may be wondering how to make heads or tails of it all. This chapter gives you the key points on how to get through the certification process like a pro. Come back to this chapter often and use it as a reference in your CMMC journey.

Answering Who You Are

CMMC isn't just filled with a lot of alphabet soup and acronyms (flip back to Chapter 2 for more info), but you also have a bunch of "dinner guests" at your table. Make sure that the right people are added to your guest list as you work your way through the certification process.

Here is your list of attendees:

- **Organizations Seeking Certification (OSC):** That could be you or one of your sub-contracting partners.
- **Registered Practitioners (RP) or Registered Provider Organizations (RPO):** Think of these folks as the implementation wizards, giving you advice, consultation, and recommendation guidance. These people don't audit or certify; they just implement.
- **Certified CMMC Assessor (CCA) or Certified CMMC Professional (CMMC):** This credentialed individual is authorized to deliver assessments, training, and consulting as part of a CMMC Third-Party Assessor Organization (C3PAO).
- **CMMC Third-Party Assessor Organization (C3PAO)**: This authorized party manages the assessment process for an OSC.

After you have an idea of who's who, you need to find out what everyone needs to actually do.

Determining Your Needs

People involved in the CMMC process need to follow a lot of rules. It doesn't matter if you're the biggest systems integrator or a small business wanting to engage with the Department of Defense (DoD). Rules aren't meant to be broken when it comes to the government, especially defense and cybersecurity rules. But, of course, there are exceptions.

DFAR Interim Rule

First, if you're handling Controlled Unclassified Information (CUI) data, you're probably scrambling to get compliant with the Defense Acquisition Regulations Systems (DFAR) and Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041).

The DoD's Interim Rule shouts from the rooftops why the DIB supply chain needs to standardize cybersecurity practices. Of

course, like every good government novella, the rule is loaded with jargon, twists, and turns. Instead of making you read unnecessary documentation, here's a snapshot:

- The Interim Rule makes contractors implement cybersecurity requirements and enhance the protection for CUI data.
- The Interim Rule's "Background" section tells you a little secret — you're actually implementing the NIST SP 800-171 (check out Chapter 2 for more info) assessment and framework to assess contractor cybersecurity implementation.

The bottom line? If you've already been using NIST SP 800-171, the Interim Rule states that you're a few steps ahead in the game and can use the work you do here toward CMMC compliance. Keep in mind, that while NIST 800-171 allowed for A Plan of Action and Milestones (POAM), CMMC does not.


TIP

Complying with the Interim Rule gets you started on your CMMC journey. Even if it doesn't give you everything you need, here's what it does help with:

- Use your Scoring Methodology self-assessment as part of your CMMC Level 3+ certification process.
- Get prime contractors used to the information flow down across their multi-tier supply chain. This means, if you bring on a sub, their issues become yours.
- Prepare to answer audit-like questions because your contracting officer will verify everything by querying the Supplier Risk Performance System (SPRS).

NIST 800-171 scoring methodology

The scoring methodology that the DoD intends to use is like baking a cake. NIST is basically taking the teacher approach of "you're starting with an A but can lose points along the way." Every company starts with a score of 110 and then the Scoring Methodology deducts points for missing controls. The more critical the control, the more points deducted if it's not there.

The DoD establishes that the scoring methodology is used for prime contractors and subcontractors at three assessment. Table 3-1 provides you the recipe.

TABLE 3-1 NIST 800-171 Scoring Methodology

Methodology	Description
Basic (contractor self-assessment)	Engage in one or more self-assessments by documenting the current implementation. The summary level score is documented and uploaded to the DoD system. The DoD considers these scores as low confidence because you've done your own work. Who isn't going to grade themselves with passing marks?
Medium	Crafted by DoD personnel, scores are generated by someone in Program Management or a cybersecurity expert with knowledge of policies and procedures. The DoD personnel review the system security plan requirement. While they don't include documents, the DoD conducts the review results at a medium confidence level.
High (onsite or virtual)	DoD-trained experts conduct high assessments. Contractors must provide evidence of their system security plans and implementations. The type of documents ranges from recent audits to system specifications. It runs the gambit.

Timing Your Certification

If you think that you can get CMMC certified in a few days like an industry technical certification, think again. You'll need to crawl, walk, and run to get to the finish line. And then prepare to keep it up, continuously.

Yes, all contractors working with the DoD need to comply with CMMC. While only a few contractors need to be certified by the second half of 2021, getting prepared isn't going to be easy. This maturity model is an uber replacement for other standards from NIST SP 800-171, 48 CFR 52.204-21, DFARS clause 252.204-7012, and a whole host of others. The DoD has upped the ante on security and reporting standards. So be prepared for a long journey.

REMEMBER

The rollout looks like this:

- Starting in Spring 2021, the staggered rollout requiring CMMC in RFIs and RFPs begins.
- Although the compliance of all contractors isn't planned until 2026, your specific contracts requirements and/or the priorities of your prime contractors should define your schedule.

» Once in place at the end of 2021, self-reporting is only for a few companies and only under the Interim Rule Scoring Methodology. For everything else, you must have a C3PAO do an audit and give you the green light.

Stepping through the Certification Process

You're probably scratching your head, wondering where to begin. There's not one formula to get you to the finish line ASAP.

CMMC breaks out practices into 17 groups, which they call domains. Within each domain, there are 43 distinct capabilities. This is why you want to know your level because most organizations don't need to prove all 43 capabilities. The higher your maturity level, the more you need to prove. And yes, you need a C3PAO to get that CMMC stamp of approval.

TIP

To review the current state of CMMC, the domains, and capabilities mapping, go to `www.acq.osd.mil/cmmc`.

Knowing your level

If all you handle is FCI data, you just need to be performing Basic Cyber Hygiene or CMMC Level 1. In short, you don't have a lot to document. When assessors arrive at your door, you can mostly show them what you're doing. Of course, you may have some things written down. If you're using Security Technical Implementation Guidelines (STIGs) or CIS Benchmarks to harden your system, you've probably got something written down. But, at this point, it's not necessary.

If you need to be Level 2 or above, you've got a lot of paperwork ahead of you. You need policies for every practice across all the domains. You need to prove that you're following all your own rules. If you're automating STIGs and CIS Benchmarks as part of your system hardening, then you're already a step ahead of the game for meeting additional documentation requirements.

Comparing current controls with scoring methodology

To achieve Level 2 and above, you're going to sweat a little bit to make everything work. The most important controls are Basic Security Requirements for NIST SP 800-171. These are the same as the minimum requirements listed in the Federal Information Processing Standards (FIPS) 200 and are considered the high-level fundamental security requirements for handling all federal information.

Derived Security Requirements supplement basic requirements. Those requirements are listed in NIST 800-53. These requirements touch on information security, privacy, and the so-called functions and mechanisms of information security. These controls support the efficacy of basic security.

The scoring system may sound easy at first. Basic security requirements are assigned five points. Derived security requirements are generally given one point. There are 23 basic security requirements and 56 derived security requirements. Some derived security requirements earn five points, and seven basic requirements earn three points. Have I confused you yet? Most organizations are in the same boat as you are right now.

NIST feels some basic controls have more significance or weight than others. Similarly, derived security requirements are elevated because of their ability to detect and prevent cybercriminal activity. Basically, take a look at what you have, compare it to what the NIST Scoring Methodology says you need to have, and start putting in place controls you don't have.

TIP

To see a complete breakdown of the scoring methodology against the domains, check out `www.acq.osd.mil/dpap/pdi/cyber`.

Incorporating missing controls

Most likely, you're going to be missing some required controls, and that's okay. NIST accommodates this by recognizing that a first implementation may have issues or a few exceptions. Sometimes things don't work the way you expect. If you have a plan and timeline for fixing the issue as soon as reasonably possible, you can probably mark the control as implemented. But you

need to follow through on your commitment prior to your official assessment. Anything else that's missing? You'll need to get the control up and running to get to the magic 110 number.

With CMMC, however, you not only have to implement everything, but also you must have it completed long enough to show maturity.

WARNING

From time to time, problems may creep up that stop you from implementing a security solution completely. NIST calls these *enduring expectations.* For example, you may have specialized manufacturing equipment that doesn't fall into traditional software or hardware categories. NIST assumes that this is a one-off special for your organization. As long as you describe why you can't implement a control and document all activities that reduce risk, you should be okay.

Comparing current state to CMMC level

Mapping your organization's current maturity to CMMC levels may cause everyone to shed a few tears at first, but it shouldn't. You aren't alone in the game of confusion. Here is how you know where you are:

- **Level 1**: This level is relatively easy with only 17 practices. Perform the Basic Cybersecurity Hygiene practices, and you're good to go. If you've been handling FCI data for a while, you're probably already doing these things. Now you just need the C3PAO to review everything and sign off on it.
- **Level 2:** With Level 2, you need to add 55 more practices and prepare yourself to become one of the world's most prolific writers. Document your cyber hygiene across every aspect of your business to gain the credential. However, you're still only allowed to handle FCI data.
- **Level 3:** You won't be alone if you opt for Level 3. If you had to follow SP 800-171 Rev 1 in the past because you handle CUI data, you need to be at least here. This is where it starts to get even trickier. You need to get to 130 documented practices. And yes, that's more than just the NIST 800-171. It may cost you a little bit now, but the returns are far greater and shouldn't deter you.

- **Levels 4 and 5:** If your organization touches sensitive data, be prepared to spend a bit more time proving that you can mitigate advanced persistent threats. You'll need to show the tactics, techniques, and procedures in writing and possibly in action through testing scenarios.

Finding a CMMC-AB approved assessor

Only a CMMC Accreditation Body (CMMC-AB) certifies pre-assessment consultants and the C3PAOs that actually conduct CMMC assessments, submits findings, and makes certification recommendations to the CMMC-AB. No matter what level you are, you need the right CMMC level certification. Even at Level 1, you must comply and go through a rigorous assessment.


TIP

This is another place where STIGs and CIS Benchmarks can help you. C3PAOs know that NIST approves those benchmarks for securely configuring your hardware and software. If you're automating these and can prove you're performing best configuration practices, your certification will be a lot easier.

To find a qualified assessor, visit `cmmcab.org/marketplace`.

IN THIS CHAPTER

- Addressing the business challenges with attaining CMMC
- Leveraging lower level controls for CMMC compliance

Chapter 4
Challenges and Opportunities in Achieving CMMC

Cybersecurity is difficult. If it were as easy as drag-and-drop with a mouse, the industry wouldn't need to implement such rigorous processes. Navigating the Cybersecurity Maturity Model Certification (CMMC) labyrinth causes all contractors a little bit of anxiety. However, all you need is a little help, planning, sweat equity, and automation.

Dealing with Business Challenges

Mentioning the words *compliance* and *audit* can make people walk away from you at a dinner party. Unfortunately, this is one expensive business challenge you can't walk away from. The right help from the right people and technology can make the CMMC process a lot less painful.

Stop 1: Get assistance

It's easy to spot Federal Contract Information (FCI) data from Controlled Unclassified Information (CUI) data. FCI data is the broadest information classification. In fact, any contract in the DoD supply chain is going to have, you guessed it, FCI data. Even if you're only a Level 1, you still need help gathering documentation.

CUI data requires a bit more detective work. Professional talent can help you when classifying CUI data isn't cut and dry. The contract should tell you if you're handling CUI data, and a lot of times the DoD will mark the data for you. To be on the safe side, though, you want an experienced professional who can double check things.


TECHNICAL STUFF

CUI data is an umbrella term for CUI, Controlled Defense Information (CDI), and Controlled Technical Information (CTI). These are specific markings that government agencies place on unclassified content to ensure contractors and employees adhere to security controls within and outside government information systems.

Stop 2: Level 3+

This is going to come with a lot of costs. You may need to hire a Registered Professional (RP) to help you get your security plan in place. You're also going to need to write up a lot of policies. Assign people in your company to be responsible for different parts of the compliance process.

Hiring consultants is an obvious cost. But you also need to think about how much time employees would spend getting educated on the intricacies of the CMMC process instead of doing their regular jobs. Another cost consideration is around automating things like security configurations. The more you can automate, the less time your employees spend on things unrelated to their jobs.

Stop 3: Scoping out the environment

Documenting the CUI data environment with dataflows and logical network diagrams should come well before you ever get to scoping. CUI data can be in a lot of different places so you need to start by identifying the right assets. You may need to re-architect your environment so that all CUI data is on one sub-network or cloud environment. Your goal is simple: compacting the amount

of infrastructure that needs to be brought into compliance — thus, reducing scope and cutting costs.

REMEMBER

To meet regulations, check out the following considerations under four different categories:

- **Covered:** If your organization has a United States federal contract or is a supplier to a federal contract, you likely have CUI.
- **Consolidated:** When the CUI is spread across systems, it becomes cumbersome to control. Consolidating your CUI data into a single network makes CMMC compliance easier and cheaper.
- **Controlled:** Controlling data includes monitoring, auditing, and protecting it. You can't just test a physical location, network authentication, or infrastructure alone. Make sure that you control the whole, which is more than the sum of its parts.
- **Composed:** Maturing IT means following a lot of best practices, not just the ones around CUI. You need to think about whether you run backups regularly, apply patch updates regularly, and put things like antivirus software on devices.

If you can confidently say you do all these things, you've met the basic cyber hygiene test.

Stop 4: Pulling together the documentation

Preparing audit documentation is the number one area that organizations get caught up in. The net for documenting processes is so wide that it's hard to rein it in. With CMMC, you need to make sure that you document all your practices. This includes policy, process and procedure documents, training materials, plans and planning documents, and system-level, network, and data flow integrations. That's a mouthful of words that mean a mountain of documents. Using software to automate CMMC compliance processes can reduce the amount of documentation that has to be manually produced.

Stakeholders often miss something; it's inevitable because there are so many places to find "stuff" that may be important. This increases audit costs as you go on a goose chase looking for those rogue artifacts. Sometimes, auditors ask questions you need to find the answers to. You shouldn't have to pay for lost employee productivity and the auditor to sit around billing for those added hours. Prepare your documentation early!


WARNING

Knowing what is and isn't CUI data shouldn't be confusing, but surprisingly, it can be difficult to learn. If the document type isn't on the CUI data registry list, the content isn't CUI data — period. To access that CUI data registry, go to `www.archives.gov/cui/registry/category-list`.

Stop 5: Monitoring subcontractor compliance

The DoD counts on its prime contractors to follow CMMC requirements and ensure that all subcontractors are properly certified, at the right level, to meet contractual obligations. Here's the rub: If you don't follow the rules, you can't be a part of the DoD supply chain. And let's be honest, no one wants to lose money, especially not their largest, best-paying contract.

Larger prime contractors have already begun asking their subcontractors about CMMC maturity and requesting their subcontractors start the certification process now. When the time comes, you're only as valuable as your credentials. No CMMC, no work.


REMEMBER

Also, if you sub-contract work, make sure all your subcontractors get compliant. The flow-down means you're responsible for your subcontractors just like your upstream contractors are responsible for you.

Using Lower-Level Controls for CMMC Compliance

With CMMC, there's a prescription that can help your organization get compliant faster. Security Technical Implementation Guides (STIGs) and CIS Benchmarks explicitly tell you how to securely configure operating systems and applications. You don't have to figure these out yourself, so that saves you time and money.

Meeting CMMC requirements

Now, you must show that your systems talk the talk. Most likely, you're trying to harden your systems to protect yourself. The problem isn't always getting secure. More often, it's staying secure. Setting configurations isn't a once-and-done process.

TIP

Investing in systems and procuring products that can help you implement and monitor security controls can help your organization do more than just meet compliance requirements. You allow systems to communicate with one another for efficient business processes. Automation that helps you secure these system controls reduces cybersecurity risk and saves money.

Automating system control implementations

Machines are fantastic at doing certain tasks. One example where machines are excellent candidates for human replacement is handling STIG and CIS Benchmark management. STIGs and CIS Benchmarks are great for building and supporting resiliency. They tell you exactly what you need to do to configure operating systems and applications. Implementing these government-approved controls is the only practical way to prove compliance to the higher-level CMMC control.

Organizations should look to automation for ingestion, creation, and deployment process for STIG and CIS policies. Automating security configuration controls lets your people do the things that only people can do — develop policies, processes, and documentation. They should be adding value to your business; that's why you hired them. Automating your security configurations reduces the time and staffing resources necessary to get secure — and get CMMC compliant.

Implementing self-healing and self-correcting systems

Medicine heals wounds. Say you're a midsized contractor who doesn't want to automate their STIG/CIS Benchmark process. You try to fix every security configuration as it's released. Ouch, that's a lot of work. Guess what? Now a new round of security configurations is released, and you have to start all over.

While updating configurations, you find conflicts that lead to system downtime. Now your employees can't do their jobs. On top of all this, you're not even sure which configuration broke everything.

Now that you know two configurations don't play nicely together, you need to document why you're not implementing the secure configuration. And when the auditor shows up? You have to find where you wrote all this down.

Implementing automation to self-heal and self-correct your security configuration conflicts enables you get secure, stay secure, and document your security. With the right automation, you should be able to scan your systems, locate configurations that need to be updated, run the updates, and document.

IN THIS CHAPTER

- Reducing cost and effort
- Eliminating heavy documentation
- Centralizing compliance management
- Automating STIGS for CMMC

Chapter 5
Seven Reasons to Leverage Automation to Tackle CMMC Compliance

Automation makes sense. In this chapter, you discover seven reasons to leverage automation to tackle Cybersecurity Maturity Model Certification (CMMC) system control compliance. In working with customers, SteelCloud recommends targeting the following key attributes:

- **Reduce the skills gap within your organization.** Finding top security talent is tough. When you want to start from scratch and implement a Level 3+ program, getting talent is costly. Automating Security Technical Implementation Guides (STIGs)/CIS Benchmarks reduces talent acquisition costs, increases the return on your CMMC investment, and allows you to use the people you probably already have.
- **Reduce the cost and effort to comply with CMMC mandates.** Automating security configurations using NIST-approved

checklists reduces CMMC compliance costs. Instead of taking the time to figure out the right security configurations on your own, you can automate setting and updating them. With fewer staff and less time spent on compliance, you can decrease both your upfront and ongoing costs.

- **Implement a compliant infrastructure.** The hardest part of compliance isn't getting compliant; it's *staying* compliant. And it doesn't happen overnight. Sure, you can self-assess and make an attestation, but there's still a question of credibility. Automating security configuration control setting and updating gets you compliant and keeps you compliant.
- **Provide for continual compliance assurance.** Getting through a successful CMMC assessment means that you have to have a concrete written plan and budget for staying compliant. Like clockwork, you can expect new security configurations every 90 days. That means you need to keep updating your configurations and document that you're updating regularly. Automating your STIGs or CIS Benchmarks lets you regularly remediate your environment against drift and document that you're doing everything CMMC requires.
- **Simplify the ingestion of new control policy updates.** When employees manually handle processes, two things happen. First, the maturity of the security posture isn't going to improve at scale. Second, employees' productivity decreases as they focus on redundant manual tasks instead of important responsibilities. Using technology to simplify the ingestion of new control policy data accelerates organizational and security maturity and maximizes productivity.
- **Standardize processes for consistency.** People make errors and are unpredictable in the delivery of work; systems aren't. Security configuration automation removes those two burdens so that you can create consistent, standardized processes. Automated scanning, remediation, and documentation of security configurations creates a repeatable process that reduces human error risk.
- **Centralize ongoing compliance management.** Managing a security program in silos leads to unnecessary business challenges, including wasteful spending, increased data breach risks, and audit findings. Centralizing operations makes it easier to support your security and compliance posture because it gives you full visibility with continuous assurances for ongoing compliance management.

CMMC certification, here we come!

Automate compliance with SteelCloud.

DoD contractors now need third-party CMMC certification to ensure their practices meet government requirements for handling confidential information. But do you know how easy those requirements can be to meet through automation? *CMMC For Dummies* not only demystifies the process of meeting the DoD's standards of "good cyber hygiene," but also it can relieve 90% of the effort it takes to harden computer infrastructure necessary to be compliant. Better yet, when it comes time to secure your systems, we'll be there to help. Access the same solution the DoD already uses to harden their systems and satisfy your CMMC compliance requirements!

Get the thumbs up on CMMC.
Share *CMMC For Dummies* today.

www.steelcloud.com/CMMCfordummies

SteelCloud

Get Compliant. Stay Compliant.

Get compliant. Stay compliant

Complying with the Cybersecurity Maturity Model Certification (CMMC) mandate is a business imperative for Defense Industrial Base (DIB) contractors. In this book, you learn about what CMMC is, how the certification process goes, and how you can achieve continuous and consistent compliance, while saving time and effort by automating compliance for lower-level system controls. *CMMC For Dummies*, SteelCloud Special Edition, is a valuable resource for both cyber experts and those new to the field.

Inside...

- Fit STIG/CIS Benchmarks into compliance
- Automate system control implementations
- Accelerate cyber hygiene compliance
- Implement self-healing systems
- Simplify compliance; save time and money

SteelCloud

Jack A. Hyman, PhD, is a systems integration, security, and cloud expert. As the CEO of HyerTek Inc, he actively speaks and consults, working with global organizations. Jack serves on the faculty at universities across the U.S. He's an accomplished author, writing on e-learning, cloud computing, and security.

ISBN: 978-1-119-81936-3
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.