

Getting CMMC Ready

A Guide to Preparing for CMMC Compliance.



Table of contents

➤ PROACTIVELY MITIGATING GROWING CYBERSECURITY RISKS.....	3	➤ GET CMMC READY: SIX WAYS TO HELP PREPARE YOUR ORGANIZATION	9
➤ UNDERSTANDING CMMC	4	➤ PREPARING FOR YOUR CMMC AUDIT	15
➤ CMMC CAPABILITY DOMAINS	5	➤ SETTING ACCURATE EXPECTATIONS FOR CMMC CERTIFICATION TIMELINES	16
➤ CMMC CAPABILITY DOMAIN DESCRIPTIONS	6	➤ ENTRUST CMMC SOLUTIONS	17
➤ CMMC MATURITY LEVELS	8		



Proactively Mitigating Growing Cybersecurity Risks

Increasing cyberattacks targeting government agencies present a growing threat to national security, as well as the day-to-day functioning of government agencies and programs. To address this growing cyber risk, the U.S. Department of Defense (DoD) established the Cybersecurity Maturity Model Certification (CMMC) as a unified standard for assessing and enhancing cybersecurity posture across DoD's contracting network – the Defense Industrial Base (DIB) – which includes over 300,000 companies.

DID YOU KNOW ...

» The average cost of breaches caused by nation state attackers is **\$4.43 million.**¹

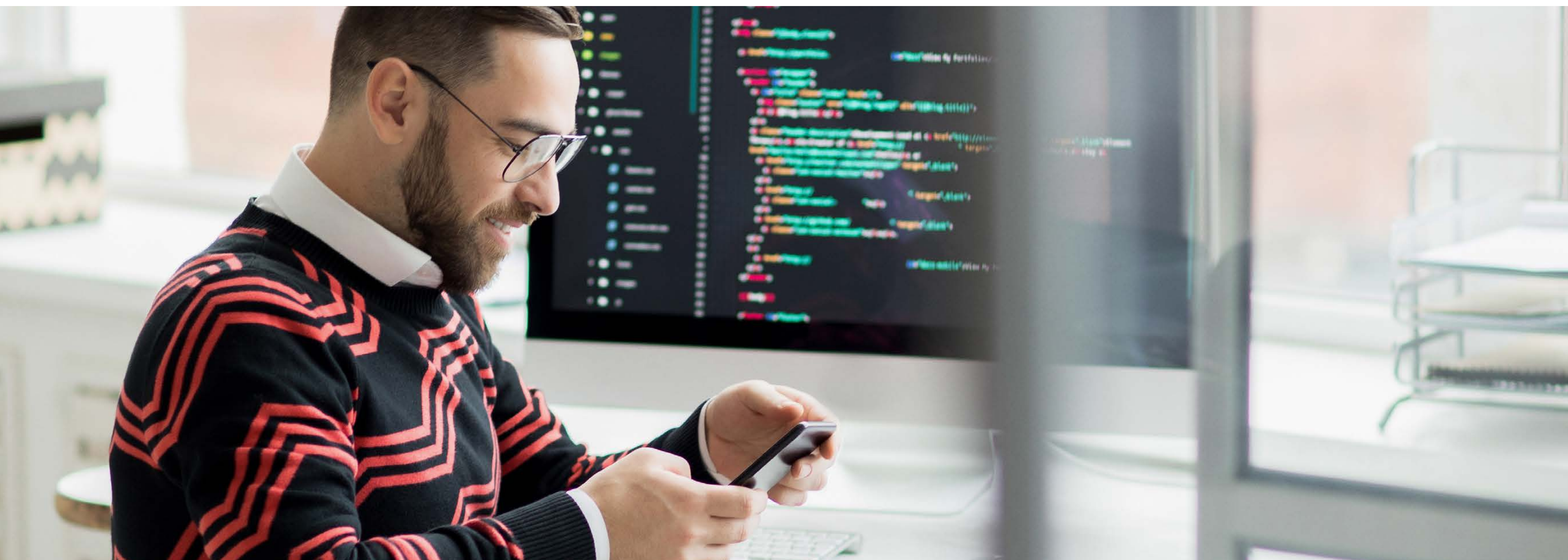
» Up to **18,000 SolarWinds** customers downloaded a compromised software update that allowed hackers to spy unnoticed on businesses and agencies for almost nine months.²

» Cyberattacks on state and local governments rose by **50%** in 2020.³

¹ IBM Cost of Data Breach Report 2020

² U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack, Reuters, Dec. 14, 2020

³ "Cyberattacks on state, local government up 50%," September 2020, GCN





Understanding CMMC

CMMC is intended to serve as a verification mechanism to ensure that DIB companies implement appropriate cybersecurity practices and processes to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their unclassified networks. The CMMC program consists of 17 capability domains, which are made up of 171 practices and processes, that fall under five different maturity levels.

CMMC is based largely on the NIST framework, specifically NIST 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations). In fact, all 110 requirements from NIST 800-171 are captured within Levels 1-3 of the CMMC, accounting for 85% of the Level-3 practices.

Important CMMC dates

» January 1, 2020:

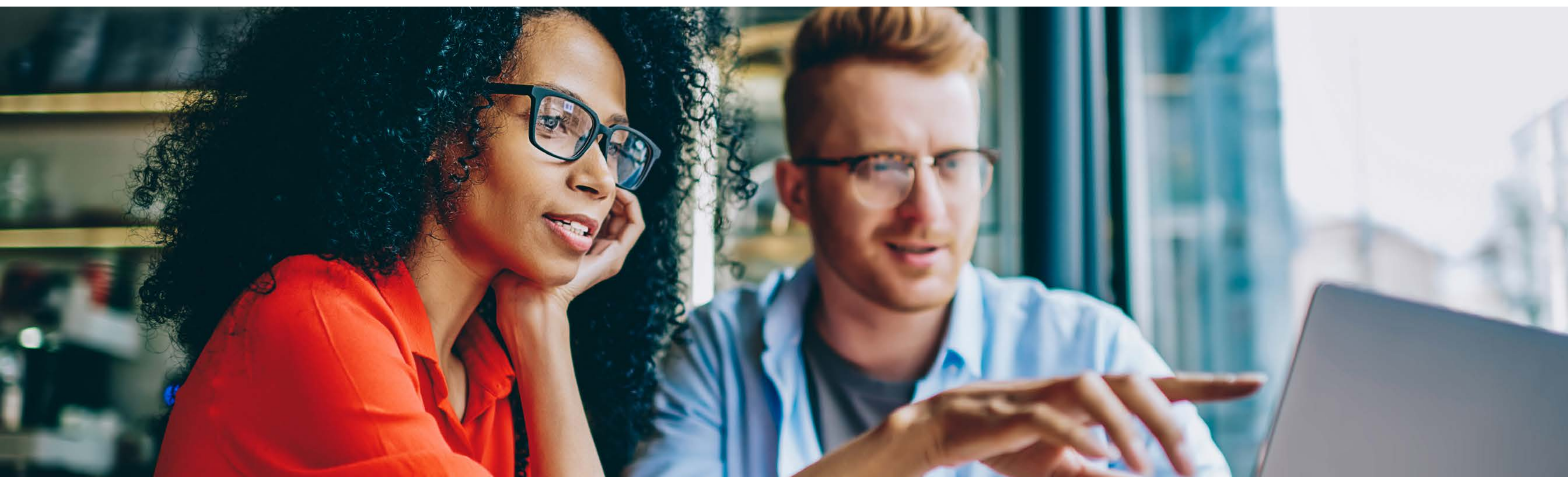
CMMC release date.

» November 30, 2020:

DoD began incorporating CMMC requirements into select RFPs, RFIs, and research contracts.

» October 1, 2025:

All DoD contract awards will require at least some level of CMMC certification. By then, nearly every vendor in the national defense supply chain will need to become CMMC certified - with many, and especially those dealing with CUI, requiring Level 3 or higher certification.

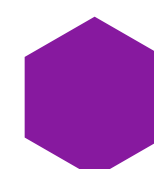


CMMC Capability Domains

There are 17 different domains in the CMMC framework. Each domain is essentially a category or grouping of security practices. Most of them have been pulled from recognized standards like the Federal Information Processing Standards (FIPS), and the National Institute of Standards and Technology (NIST).

Capability domain descriptions are on pages 6 and 7.



 = Domains in which Entrust has security solutions to help you meet CMMC certification.

 = Domains in which Entrust has technology partners with security solutions to help you meet CMMC certification.



CMMC Capability Domain Descriptions

› Access Control (AC):

Requires your organization to establish who has access to your systems and what their requirements are to operate effectively, who has remote access, who has internal system access, and the limitations of their roles in the system.

› Asset Management (AM):

Requires you to locate, identify, and log inventory of the assets to your organization.

› Audit and Accountability (AU):

Requires you have a process in place for tracking users that have access to your organization's CUI and for performing audits of those logs to ensure they are held accountable for their behavior. You will need to define the requirements of each audit, have a method to perform the audit, protect and secure the results of that audit, and manage audit logs.

› Awareness and Training (AT):

Requires that you have training programs in place for all personnel and conduct security awareness activities.

› Configuration Management (CM):

Requires that you establish configuration baselines as a measure to judge the efficiency of your systems. This is necessary to conduct audits and accurately measure the posture of your systems.

› Identification and Authentication (IA):

Ensures the proper roles within your organization have the correct level of access and can be authenticated for reporting and accountability purposes.

› Incident Response (IR):

Requires an Incident Response Plan with the ability to detect and report events, develop and implement responses to declared incidents, perform post-incident reviews, and test your response in an effort to measure your entity's preparedness in the event of a cyberattack.

› Maintenance (MA):

Requires you have a maintenance system in place to maintain and effectively operate your systems.

› Media Protection (MP):

Requires you to have your media identified and appropriately marked for ease of access. You must also provide evidence of a media protection protocol, sanitation protocol, and transportation protection in place.

› Physical Protection (PE):

Requires evidence of the physical security surrounding your assets and proof the assets are protected.





CMMC Capability Domain Descriptions (continued)

› Personnel Security (PS):

Requires that your personnel have been properly screened with background checks. You must provide evidence that your CUI is protected during personnel activity such as employee turnover or transfer.

› Recovery (RE):

Requires that you keep and log backups of media necessary to your organization. These need to be logged for continuity among backups and to mitigate lost data.

› Risk Management (RM):

This is the process of identifying and evaluating the risk that affects your company using periodic risk assessments and vulnerability scanning. Includes your organization's risk as well as that of your vendors.

› Security Assessment (CA):

Requires that a system security plan be in place. You will also need to define and manage controls and perform code reviews for your organization.

› Situational Awareness (SA):

Requires evidence of a threat monitoring system. This helps supplement other domains and keeps your organization secure in the event of a cyber incident.

› Systems and Communications Protection (SC):

Requires you to define the security requirements of each system and communication channel your organization uses to provide evidence your organization has control of communications at system boundaries.

› System and Information Integrity (SI):

Requires you to identify and manage flaws within your system, identify hazardous and malicious content in-system, implement email protections, and monitor your network and system.

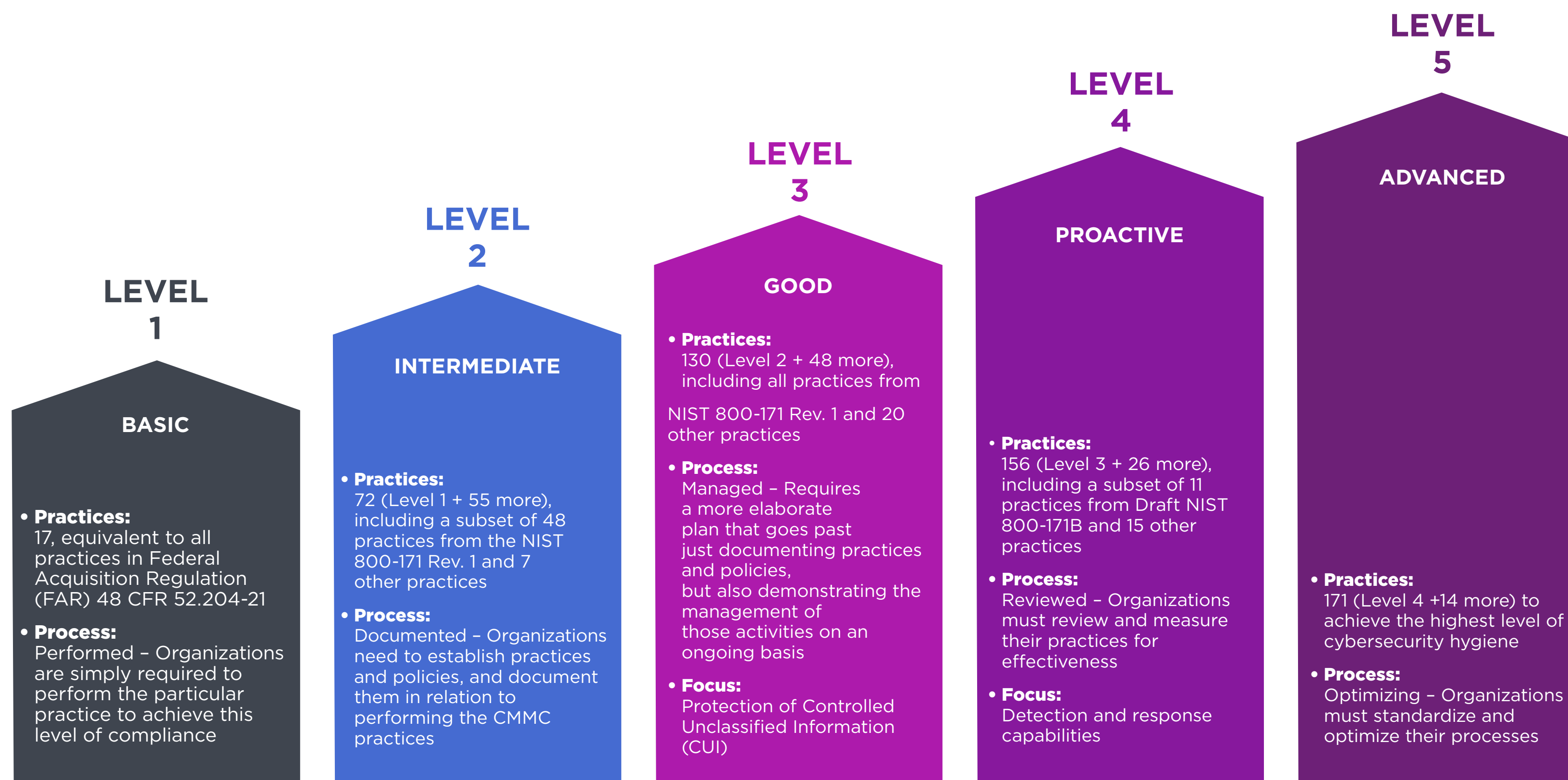




CMMC Maturity Levels

There are five maturity levels in the CMMC model, ranging from 1 (basic cyber hygiene) to 5 (advanced cyber sophistication). To get certified in a particular CMMC level, you need to demonstrate both practices and processes.

Here's a quick overview of the practices and processes associated with each level:





Get CMMC Ready: Six ways to help prepare your organization



1. Determine the correct level of CMMC maturity for your organization

The DoD divided CMMC into five levels to ensure right-sized cybersecurity requirements for contractors of all sizes, types, and levels of engagement. Since CMMC is largely focused on protecting the U.S. defense supply chain, one of the most basic ways to think about the levels is to connect them to the supply chain.

Level 1 is intended for contractors at the lowest levels of the supply chain (a subcontractor that supplies a single type of wheel lug nut, for example.) Moving up the supply chain, any organization that touches controlled unclassified information (CUI) will need obtain at least a Level 3 certification, and those organizations that deal with highly sensitive information would need Level 4 or 5 certification.

The starting point for determining which CMMC maturity level your organization requires is to do a thorough inventory of your systems and networks to identify where and how you use or touch FCI (Federal Contract Information) and CUI.

CUI Inventory Quick Guide

Here's a brief overview to help identify what to look for as you inventory networks and systems to assess your engagement with CUI:

What are you looking for?

- DoD contract documents
- Project plans (schematics, blueprints, CAD files, etc.)
- Financial information (tax info, accounting, etc.)
- Communications (emails, texts, chats, etc. containing CUI)

Where does it go?

- How did the CUI come into your organization?
- Where is this information stored (digitally and/or physically)?
- Who accesses this information regularly?
- Does this information get sent/ passed along to another party?



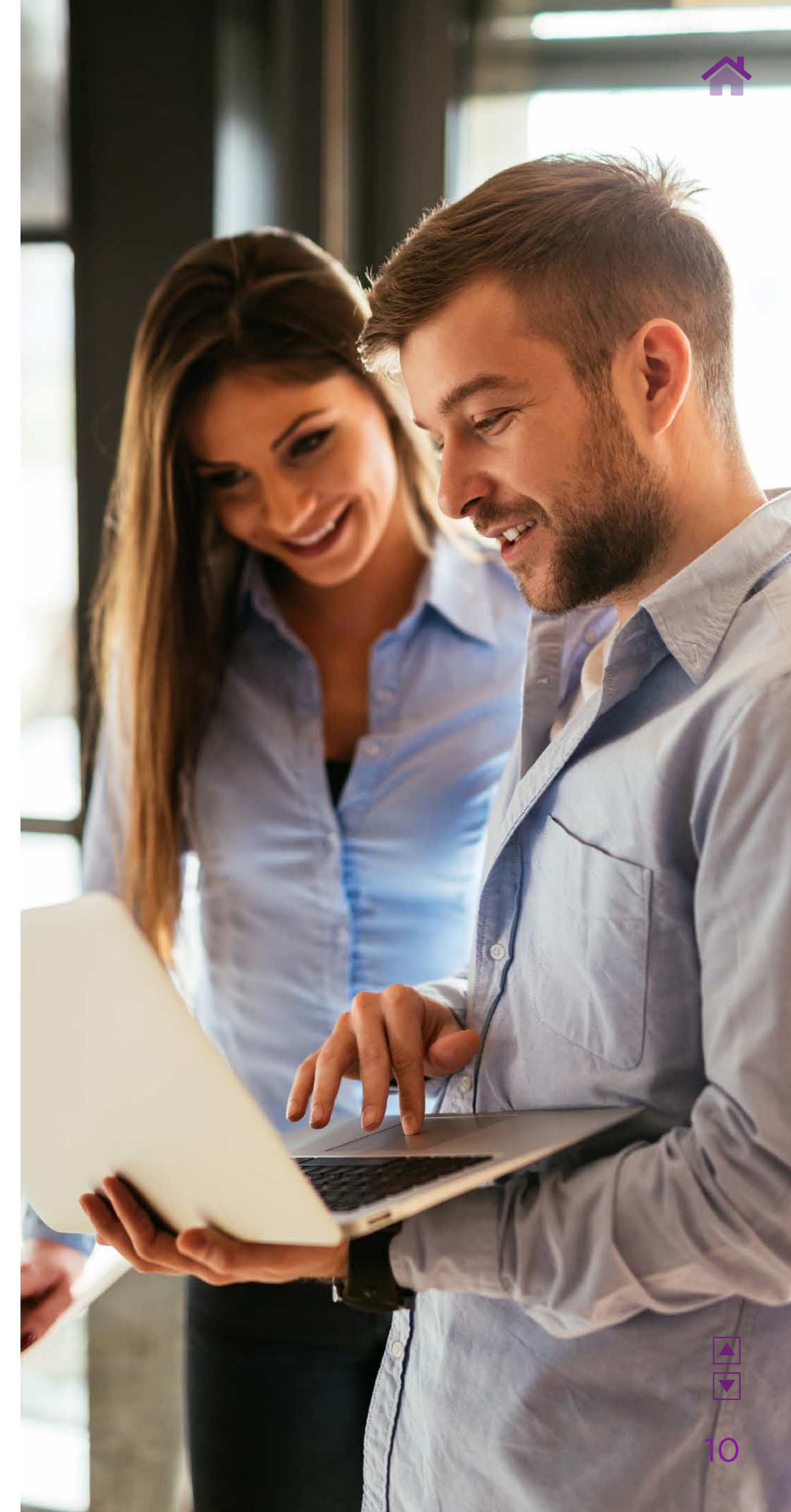


2. Identify the scope of your CMMC compliance initiative

The next step in building a CMMC compliance strategy is to understand exactly how CMMC requirements apply to your business. This will determine the scope of your CMMC compliance program – or, put another way, which practices and processes within your business fall under CMMC requirements.

In some businesses, DoD contract work falls within a relatively siloed portion of overall operations, while in others, the DoD work touches nearly every aspect of the organization. As you strive to streamline the scope of CMMC compliance, it's imperative to ensure all relevant practices and processes are covered.

One strategy is to take a hybrid approach of certifying your entire organization to Level 1 and obtaining a higher level (at least a Level 3) for those sections, departments, or specific practices and processes that execute DoD contracts and handle CUI.





3. Do the NIST self-assessment to identify gaps

Although CMMC differs from NIST (see sidebar), there is definitely some overlap and shared objectives as it relates to enhancing cybersecurity and protecting CUI and FCI.

All Level 3-5 applicants are required to complete and submit the [NIST 800-171 DoD Assessment Methodology](#). And even those organizations seeking only Levels 1 or 2 certification can use the NIST self-assessment as an excellent starting point.

The self-assessment will help you evaluate where you stand today on meeting the relevant CMMC requirements within your defined CMMC scope and identify gaps that will require corrective actions to achieve the desired CMMC certification.

You can also engage a third-party assessor to do a Boundary Determination and Gap Analysis for you.

The difference between CMMC and NIST

CMMC was created, in part, because following only NIST SP800-171, and without independent certification, was insufficient at protecting CUI and FCI in the DoD supply chain. CMMC has more rigorous standards.

- CMMC is based on maturity models with different levels of compliance, meaning the more secure your practices are, the higher level of certification you achieve. With NIST, you are either compliant or not, which means organizations can do as little as possible to “check the box” to meet compliance.
- With CMMC, a plan of actions and milestones (POA&M) is not sufficient for compliance.
- Cybersecurity maturity is based on more than compliance. It’s based on more than just having a security program; it’s also based on how you’ve implemented it, how you’re using/following it, and how it’s working.
- CMMC maturity must be certified by a third-party auditor, whereas compliance with NIST SP800-171 is self-reported.



4. Build your system security plan

One of the most critical pieces of information required for CMMC certification at any level is the System Security Plan (SSP) as required under NIST 800-171.

The SSP is essentially a map of your security landscape and control capabilities as they exist today. It helps identify:

- The distinct system environments and the boundaries of those environments.
- How systems and networks connect or otherwise interact.
- How relevant security requirements are executed across these environments.

In developing an SSP, contractors should take care to ensure the plan accurately reflects how systems and security controls operate in practice, as the theoretical or ideal control environment does not always play out in the real world.





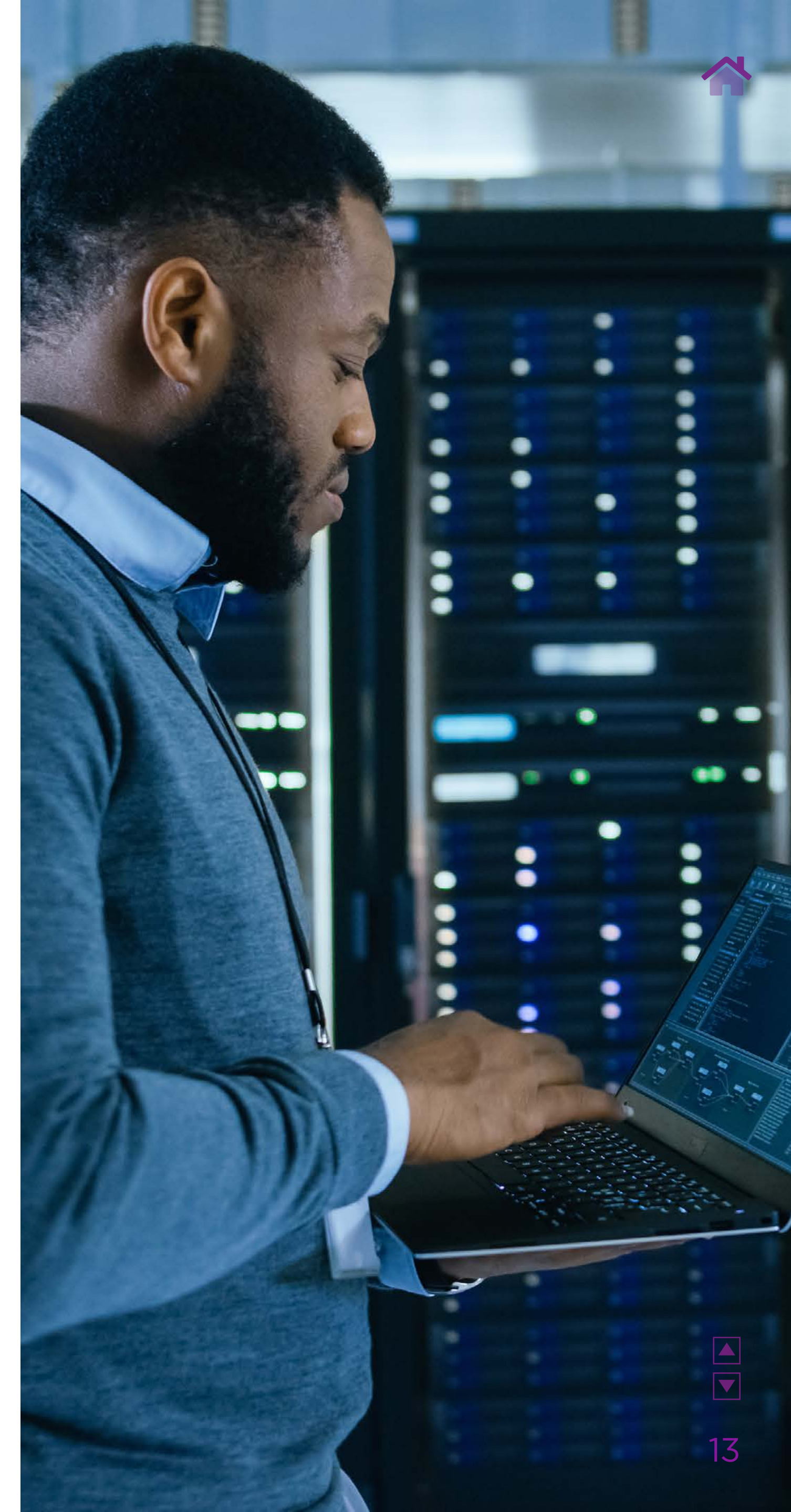
5. Make necessary investments to execute your plan

It's likely that your plan will go beyond merely restructuring or revising practices and processes – it may require the deployment of additional security technologies and solutions to bring practices and processes into CMMC compliance.

Just as with any major strategic initiative, you should be prepared to make an investment in building a future-ready security environment – and anticipate the return on these investments across a range of value, which may include:

- Winning future DoD and government contracts.
- Mitigating the internal costs and damage of future cyberattacks.
- Securing more streamlined and efficient ways of working for the business.

Because of the complexity of the CMMC levels, domains, and requirements, there is no one-size-fits-all technology solution – no single product that enables plug-and-play CMMC compliance. Rather, organizations must put together the right toolkit of security solutions to achieve the right CMMC maturity level, manage their specific CUI and FCI workflows, and address their unique security gaps.





6. Engage a third-party auditor to certify CMMC compliance

Once a CMMC compliance program has been fully implemented, you'll need to bring in a Registered Practitioner (RP), Registered Provider Organization (RPO), or a CMMC Third-Party Assessor Organization (C3PAO) to assess and validate your CMMC compliance and maturity. To minimize the likelihood of snags or other problems in the validation process, it's important to ensure that you're aligned with your assessor on the following:

- **Maturity Level:** The assessor should be looking at the correct set of requirements for the relevant CMMC maturity level.
- **Scope:** The assessor should understand the boundaries for the CMMC assessment – whether it's a whole-organization assessment, a siloed assessment, or a hybrid approach as discussed previously.

Because of the complexity and variability in assessing different organizations, you should take time to evaluate potential assessors to find one that you trust to understand the aim and scope of your CMMC compliance initiative. While validation from an RP, RPO, or C3PAO will likely not be a large line item within the context of your overall CMMC compliance program, it's still important to consider that low-priced assessors may not deliver high-value outcomes.

Entrust is not a CMMC-registered provider organization (RPO), but our deep experience in the security world enables us to help contractors evaluate and select a high-quality assessor.

CMMC Auditor Glossary of Terms*

Registered Practitioner (RP):

Professionals who provide consultative services that include non-certified CMMC advice. RPs are not permitted to participate on certified assessment teams.

Registered Provider Organization (RPO):

An organization authorized to represent itself as familiar with the basic constructs of the CMMC standard to deliver non-certified CMMC consulting services. Their CMMC-AB logo signifies that they have agreed to the CMMC-AB Code of Professional Conduct.

Certified 3rd Party Assessment

Organization (C3PAO): An entity that is certified to be contracted to an organization seeking certification (OSC) to provide consultative advice or certified assessments.

* Source: CMMC Accreditation Body





Preparing for your CMMC Audit

The bulk of the work for contractors happens before the CMMC third-party audit. These tasks include determining the correct maturity level, evaluating existing gaps and building a compliance plan, and procuring and deploying security solutions to close those gaps. But there are two key things your organization can do to prepare for the CMMC audit:

- 1. Allocate Sufficient Internal Resources:** The CMMC assessment is not an at-a-distance process; assessors will need to engage with your staff to access relevant information. Identifying staff that will serve as those key contacts is something that can be done ahead of time. These key contacts can also determine what the assessors will likely request as “adequate evidence” – and begin collecting that necessary documentation or evidence.
- 2. Testing the Control Requirements:** Since the CMMC requirements are plainly stated, you can conduct your own internal testing or assessments ahead of your third-party CMMC audit. This can help catch and correct any remaining gaps before they cause any issues with the final certification process.

Setting accurate expectations for CMMC compliance timelines

The most common frustrations around CMMC compliance revolve around timelines. The amount of time it takes to get certified depends, of course, on:

- Your current state of maturity.
- The maturity level you need to achieve.
- The complexity of your environment.

But it never seems to fail that many contractors, confident in their current security controls, have incorrectly planned on being able to obtain the relevant maturity-level certification in a matter of a month or two – and have been frustrated to miss potential contracts when the certification process dragged on longer than expected.

Moreover, underestimating the timeline is connected to another common pitfall: failing to dedicate sufficient internal resources, both in terms of staff time and budget for procuring security solutions. Attempting to take shortcuts to CMMC compliance will likely lead to a significantly protracted timeline, as issues in the initial CMMC audit lead to additional time and cost for further remediation and a second (or third) attempt at certification.

You should expect to dedicate roughly six months to the CMMC compliance process. And confidently committing staff and budgetary resources to the project can pay significant dividends in terms of both the timeline and the ultimate value of the high-security outcome.





Entrust CMMC solutions

For over 25 years, Entrust has worked with governments across the globe to provide best-in-class cybersecurity solutions that support security best practices. We are acknowledged as a leader in digital credentials for the U.S. federal market, issuing civilian agency credentials and data protection solutions that help secure the data, encryption keys, and secrets of many U.S. agencies.

With the CMMC program, our broad portfolio of digital and physical security solutions – including Identity, PKI, and HSMs – can help the 300,000+ DoD contractors address and achieve compliance in 11 (shown below) of the 17 domains. It’s no wonder why the world’s most trusted organizations trust us.



CMMC DOMAIN	CAPABILITIES	ENTRUST SOLUTIONS
Access Control (AC)	<ul style="list-style-type: none"> • Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes 	<ul style="list-style-type: none"> • Entrust Identity as a Service • Entrust Identity Enterprise • Entrust PKI • Entrust Digital Certificates • Entrust nShield® HSMs • Entrust DataControl • Entrust CloudControl
Asset Management (AM)	<ul style="list-style-type: none"> • Identify and document assets • Manage asset inventory 	<ul style="list-style-type: none"> • Entrust Certificate Hub • Entrust nShield® HSMs • Entrust CloudControl
Audit & Accountability (AU)	<ul style="list-style-type: none"> • Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs 	<ul style="list-style-type: none"> • Entrust Identity as a Service • Entrust Identity Enterprise • Entrust PKI • Entrust nShield® HSMs • Entrust CloudControl • Entrust DataControl





Entrust CMMC solutions

CMMC DOMAIN	CAPABILITIES	ENTRUST SOLUTIONS
Configuration Management (CM)	<ul style="list-style-type: none"> • Establish configuration baselines • Perform configuration and change management 	<ul style="list-style-type: none"> • Entrust PKI • Entrust Digital Certificates • Entrust nShield® HSMs • Entrust CloudControl
Identification & Authentication (IA)	<ul style="list-style-type: none"> • Grant access to authenticated entities 	<ul style="list-style-type: none"> • Entrust Identity as a Service • Entrust Identity Enterprise • Entrust PKI • Entrust nShield® HSMs • Entrust CloudControl • Entrust DataControl
Maintenance (MA)	<ul style="list-style-type: none"> • Manage maintenance 	<ul style="list-style-type: none"> • Entrust PKI • Entrust nShield® HSMs • Entrust CloudControl • Entrust DataControl
Media Protection (MP)	<ul style="list-style-type: none"> • Identify and mark media • Protect and control media • Sanitize media • Protect media during transport 	<ul style="list-style-type: none"> • Entrust PKI • Entrust nShield® HSMs • Entrust DataControl
Physical Protection (PE)	<ul style="list-style-type: none"> • Limit physical access 	<ul style="list-style-type: none"> • Entrust Instant ID Issuance • Entrust VMaaS • Entrust PKI • Entrust nShield® HSMs
Recovery (RE)	<ul style="list-style-type: none"> • Manage backups • Manage information security continuity 	<ul style="list-style-type: none"> • Entrust PKI • Entrust nShield® HSMs • Entrust DataControl





Entrust CMMC solutions

CMMC DOMAIN	CAPABILITIES	ENTRUST SOLUTIONS
Systems & Communications Protection (SC)	<ul style="list-style-type: none"> Define security requirements for systems and communications Control communications at system boundaries 	<ul style="list-style-type: none"> Entrust PKI Entrust Digital Certificates (S/MIME, TLS/SSL) Entrust CryptoCoE Entrust nShield® HSMs Entrust CloudControl Entrust DataControl
System & Information Integrity (SI)	<ul style="list-style-type: none"> Identify and manage information system flaws Identify malicious content Perform network and system monitoring Implement advanced email protections 	<ul style="list-style-type: none"> Entrust Digital Certificates (Code Signing, S/MIME, VMCs) Entrust Certificate Hub Entrust CloudControl Entrust DataControl

Click the image below for a more detailed chart with a breakdown of subcategories of capabilities and practices, as well as product descriptions.

How Entrust Helps Address CMMC

Access Control (AC)

Capability	Practices Addressed by Entrust	Products
C001 Establish system access requirements	AC.1.001, AC.2.005, AC.2.006	Entrust Identity as a Service Entrust Identity Enterprise Entrust PKI Entrust nShield HSMs Entrust DataControl Entrust CloudControl
C002 Control internal system access	AC.1.002, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.3.017, AC.3.018, AC.3.019, AC.3.012, AC.3.020, AC.4.023, AC.4.025	Entrust Identity as a Service Entrust Identity Enterprise Entrust PKI Digital Certificates Entrust nShield HSMs Entrust CloudControl Entrust DataControl
C003 Control remote system access	AC.2.013, AC.3.014, AC.3.021, AC.4.032	Entrust Identity as a Service Entrust Identity Enterprise Entrust PKI Digital Certificates Entrust nShield HSMs
C004 Limit data access to authorized users and processes	AC.1.003, AC.2.016, AC.3.022	Entrust Identity as a Service Entrust Identity Enterprise Entrust PKI Digital Certificates Entrust CloudControl Entrust DataControl

Entrust PKI & Digital Certificates: PKI and certificates provide the ability to restrict access to data by providing secure access credentials for authentication and data management platforms, as well as a means to sign data for integrity and encrypt data for privacy. The PKI allows users to exchange data securely and validate that signatures on data are legitimate. PKI also provides a means to distribute keys/certs used for data protection to devices and users in an automated way.

For controlling internal system access, much of the requirement relates to setting up and enforcing policy around data access. PKI and certificates provide a method to enforce the policies by providing every participant with a credential that can be used to enforce the defined access policies. Typically, the path is via a corporate directory like Active Directory (AD) - access to resources is set and group policies will push users into access groups leveraging certificates for authentication. Credentials placed on access cards, in AD, or on other user devices via MDM are governing access controls. Remote system access can be VPN, secure auth, MFA - these are all backed by crypto keys and certificates.



For more information
888.690.2424
+1 952 933 1223
info@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com    

Entrust and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.
©2021 Entrust Corporation. All rights reserved. CO22Q2-getting-cmmc-ready-eb



Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact