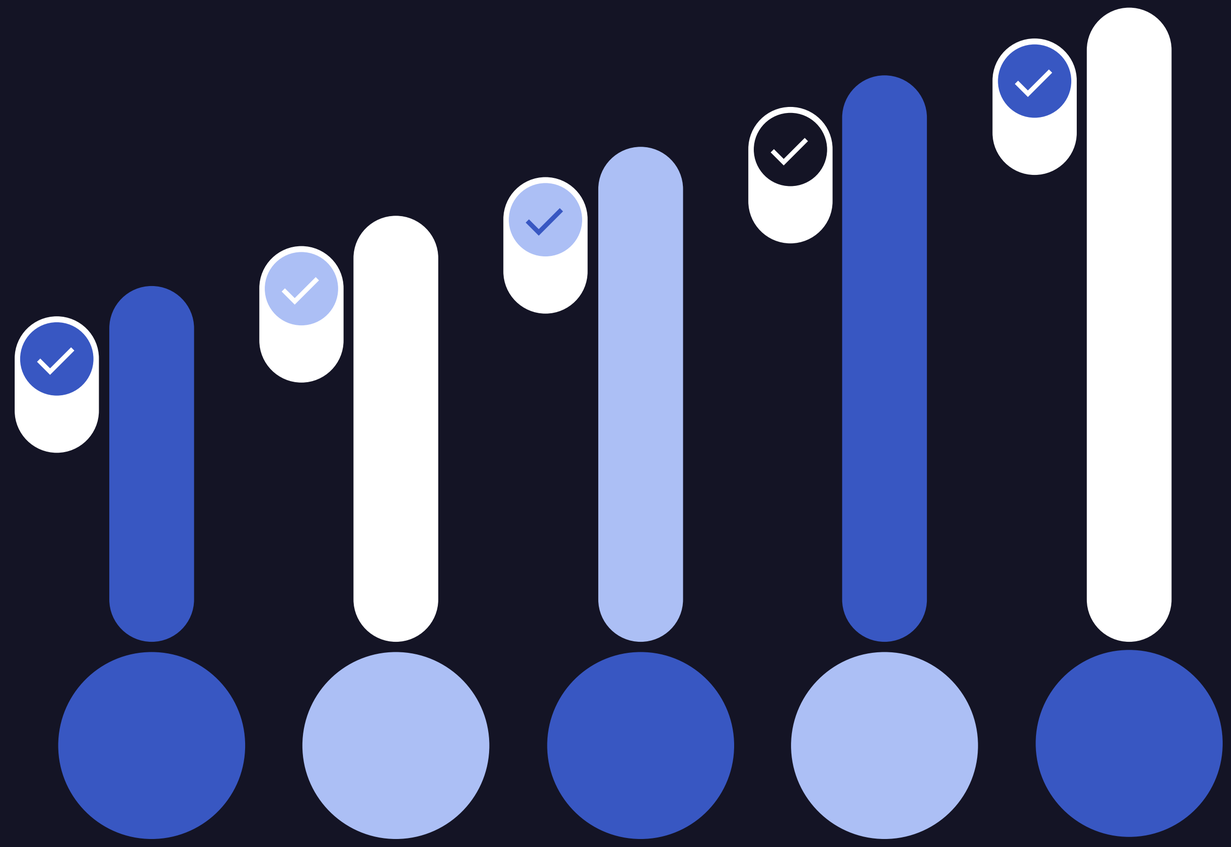
C3

eBOOK

Five Keys to CMMC Level 2 Success



About CMMC

The Cybersecurity Maturity Model Certification (CMMC) is a framework developed by the U.S. Department of Defense (DoD) to ensure that defense contractors implement the cybersecurity practices necessary to protect sensitive information. For those new to CMMC, we've developed an "Introduction to CMMC" eBook to get a basic understanding of the CMMC framework, including CMMC levels and the benefits of certification. This framework mandates third-party assessments to ensure the implementation and maintenance of strong cybersecurity standards, verifying that any contractors that handle Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) are protecting it appropriately. This both reduces the risk of cyber threats and increases alignment with federal regulations, helping to maintain national security through the protection of sensitive information.

Organizations seeking CMMC Level 2 certification or compliance with Defense Federal Acquisition Regulation Supplement (DFARS) 7012 cybersecurity requirements must follow the requirements laid out in the 110 security controls outlined in National Institute of Standards and Technology (NIST) Special Publication 800-171 rev 2, which are mandatory for protecting CUI. The companion document, SP 800-171A rev 2, breaks down these controls into 320 specific assessment objectives, providing clear criteria for compliance evaluation and delivering a structured framework for both self-assessment and third-party audits. It provides the "answers to the test," enabling organizations to prepare thoroughly for CMMC assessments because it details exactly how your security measures will be evaluated.

Introduction

As defense contractors seek to achieve and maintain Cybersecurity Maturity Model Certification (CMMC) Level 2 certification, they can be easily overwhelmed by the amount of advice—often conflicting—that exists in the market. This eBook is designed to break down the journey to (and beyond!) certification so organizations can navigate with clarity and confidence.

Whether you're at the beginning of your compliance journey or working toward final certification, this guide offers a practical, five-step approach to help you build a strong foundation, deploy the right technical solutions, manage compliance over time, implement effective security monitoring, and prepare for a successful assessment.

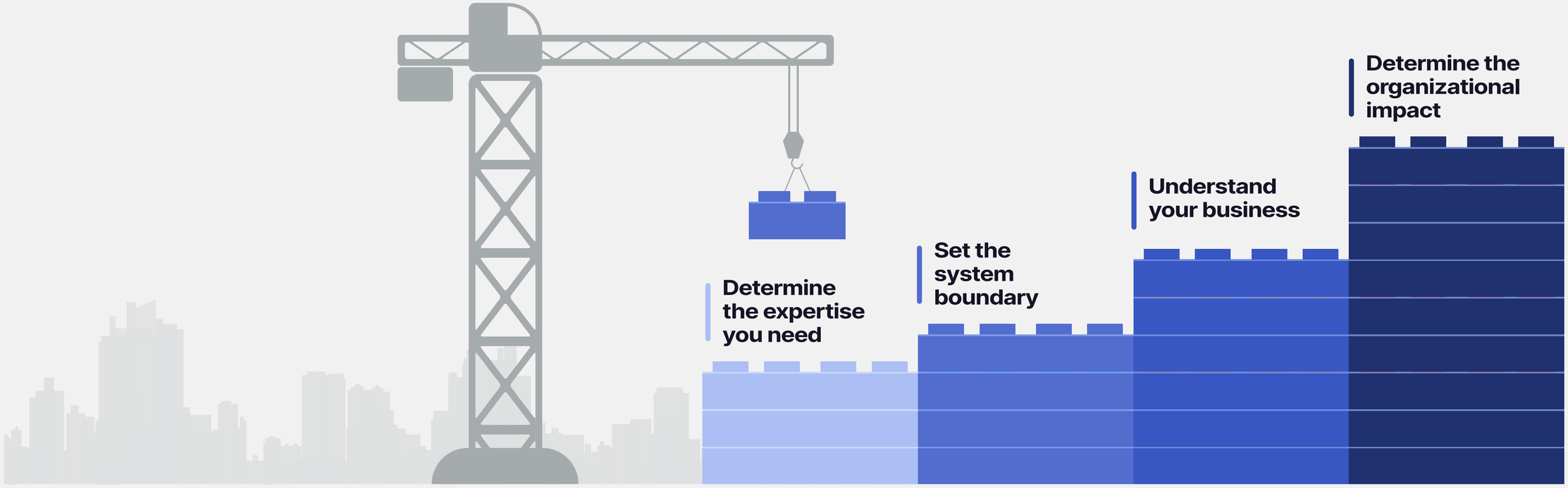
Each chapter walks through actionable strategies that reduce risk, clarify responsibilities, and streamline the path to certification—providing the insights and structure you need to meet CMMC Level 2 requirements and protect the sensitive information that keeps our nation secure.

FIRST KEY TO SUCCESS:

Building a Strategy for Success

Achieving CMMC Level 2 certification is now a requirement for organizations seeking to do business with the Department of Defense (DoD), and the stakes have never been higher. As prime contractors begin to incorporate CMMC expectations into contracts with their sub-contractors, more and more contractors face the need to prove their CMMC Level 2 status—or at least have a scheduled assessment—even in advance of the final 48 CFR rule.

Starting with a well-defined strategy for CMMC Level 2 is essential given these requirements. If you aren't yet ready (or aren't sure if you are), the following steps will help you avoid costly mistakes, wasted resources, and poor investment decisions that could put your certification at risk.



Analyze Your Business

The first key to success requires analyzing your business from a client, contract, and operational perspective. Understanding these aspects of the business will help clarify future steps. To build a strategy for CMMC compliance, you need to analyze both external and internal factors related to your business. This process provides a foundation for understanding your organization's unique challenges and opportunities so you can ensure you're putting effort into the right areas. This is a good time to tighten up your data flows and access as it will simplify the next steps in your certification process.

External factors that influence compliance requirements

The first step in understanding the external factors that will influence your compliance requirements is to determine which DoD contracts you currently hold or plan to pursue. Next make sure you understand the CMMC level requirements tied to these contracts. You'll also need to review your existing contracts to identify clauses related to CUI to ensure you meet those requirements.

Tip: If you currently have DFARS 252.204-7012 in your contracts, you will likely have CMMC requirements in the future.

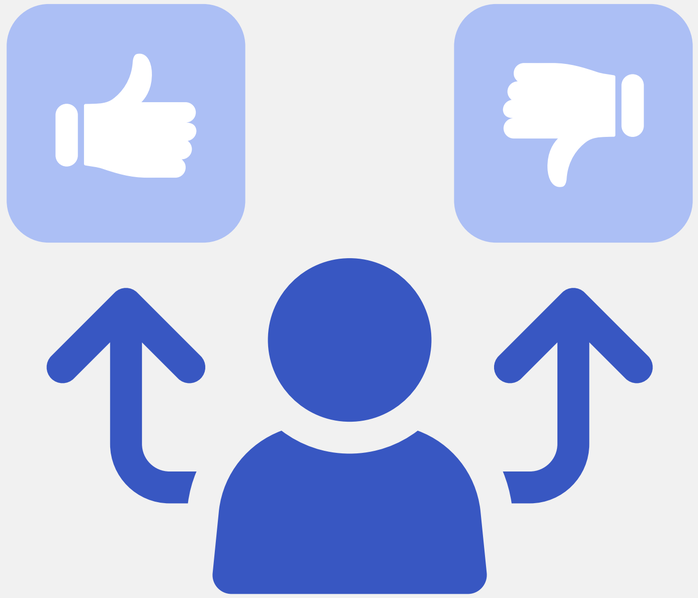
Part of this process includes assessing the cybersecurity posture of your subcontractors and partners: Any subcontractor, that receives CUI data, regardless of what tier in the supply chain they reside, must comply with the appropriate level of CMMC certification for that data. Their deficiencies could impact your ability to capture and retain contracts. This is also a good time to evaluate your business growth strategy and confirm it aligns with the certification level you are seeking.

Internal factors drive compliance strategy

Once you've evaluated your external factors, it's time to look at the internal aspects of your business that may impact your strategy. Begin by identifying employees who currently interact with CUI. An understanding of who interacts with CUI will allow you to understand the breadth of your compliance scope within the organization.

Next, map out where CUI data is stored, processed, or transmitted within your IT infrastructure. Look at how this data flows across systems, applications, and organizational units. This process can also help you to identify vulnerabilities or gaps in security, but it's also a good time to think about how to minimize your CUI and who has access to it.

Determine Your Compliance Scope



Once you understand the people, systems, and processes that interact with CUI, you can now determine your compliance scope. In essence, this means mapping and documenting all locations and pathways of CUI data in your environment so that you can define exactly what must be included in your compliance efforts to meet regulatory requirements.

The compliance scope defines the boundaries of the systems that store, process, and/or transit CUI data. It also sets the stage for all the future steps and is a key parameter in your overall CMMC assessment scope.

Once you understand where CUI data exists and where it flows, your next decision is whether to choose an enclave or all-in approach for your compliance boundary. Each approach has pros and cons, so it’s important to consider which one makes the most sense for your organization.

Evaluating an enclave approach

The enclave approach specifically isolates systems that handle CUI into a separate environment. This approach is particularly beneficial for organizations seeking a more controlled scope rather than bringing everything within the system boundary.

- Smaller initial investment compared to an enterprise-wide solution.
- Reduced scope simplifies compliance efforts by minimizing the number of systems that need protection.
- A smaller attack surface may reduce cybersecurity risks.
- Minimal data migration decreases operational disruption during implementation.

PROS

- Swivel-seat users (that is, employees who work across both compliant and non-compliant systems) may face inefficiencies from having to switch back and forth between environments.
- Having dual administration requirements often creates additional overhead and operational complexity.
- You may experience higher costs than anticipated if you underestimate ongoing maintenance costs.
- Data spillage potential increases because users may inadvertently transfer sensitive data between compliant and non-compliant environments.

CONS

Evaluating an all-in approach

The all-in approach involves applying CMMC requirements across the entire organization, creating a unified environment where everything is contained within the system boundary.

- A single, unified environment eliminates the need for both dual administration and swivel-seat users.
- There's the potential to eliminate technical debt because moving to a single environment will probably involve replacing legacy systems.

PROS

- Data migration to a new environment can create challenges that disrupt operations and increase deployment costs.
- Every user in the organization must comply with stringent security requirements, which may impact productivity, especially at the beginning.
- Users may request non-approved applications, resulting in additional administrative controls and denial of such requests.

CONS

Choosing the right approach

When making the decision between the enclave or all-in approach, consider the percentage of DoD work your organization does. Organizations that provide commercial products and services with only a small percentage of revenue coming from the DoD tend to benefit from the enclave approach. Conversely, companies that focus on the DoD or have DoD contracts deeply intertwined with their commercial business may find an all-in approach is the best fit.

Tip: At C3, we have seen cases where a client's final objective is an all-in approach but they choose to start with an enclave. This allows the organization to move quickly to an initial, compliant posture, and then migrate additional users and systems over time.

Determine Organizational Impact

Even once you have chosen between an enclave and all-in approach, you must still evaluate the organizational impact, particularly in terms of your current and planned data flows. In small organizations especially, it’s not uncommon for teams to be unaware of how data flows between different systems. They may not understand how things are currently structured, thereby creating unintended business disruption if not properly analyzed.

Assess Operational Impact:

Compliance with CMMC may necessitate changes to workflows, policies, and day-to-day operations. Identify how implementing new security controls will alter existing processes to determine the operational impact. For example, stricter access controls or conditional access requirements may require employees to take additional steps to access systems. Will this impact productivity? Also, consider whether compliance measures are likely to slow down operations or create inefficiencies in areas such as data sharing or collaboration.

Evaluate Financial Impact:

Depending on your organization’s current cybersecurity efforts, achieving CMMC compliance may involve significant investments in technology, personnel, and third-party services. Your process should include estimating costs for system upgrades, consulting services, and ongoing maintenance.

Minimize CUI Footprint:

This step is essential for simplifying CMMC Level 2 compliance, reducing costs, and limiting risk. Start by thoroughly identifying all CUI, beginning with where it is received, processed, stored, and transmitted within your organization, and map the flow of this data across systems and users. Next, define and narrow your system boundary by restricting access to CUI only to those personnel, applications, and devices that absolutely require it. Part of this process should include minimizing the footprint of where CUI sits.

Implementing a segmented CUI enclave—an isolated environment dedicated to handling CUI—can further reduce your compliance scope, making assessments more manageable and cost-effective.

Analyze Technological Impact:

CMMC compliance will almost certainly require upgrades or modifications to your IT infrastructure. Do your current systems meet CMMC requirements, or do you need to make improvements in some areas, such as encryption, logging capabilities, or endpoint protection? Consider how any new tools or configurations will integrate with your existing systems and whether there will be any impact on performance.

Note that with an enclave approach, technology upgrades are limited to the smaller footprint of the enclave. This can reduce implementation costs and accelerate deployment times.

Assess Personnel Impact:

CMMC compliance affects employees at all levels across your organization. Some personnel may need to take on additional responsibilities, such as managing compliance documentation or monitoring security controls. If tools and responsibilities have changed significantly, you may need to create a training program to ensure all employees understand their updated individual roles in maintaining compliance.

Many companies recognize the additional burden of managing a compliant environment and choose to outsource some, or as much of the effort as possible.

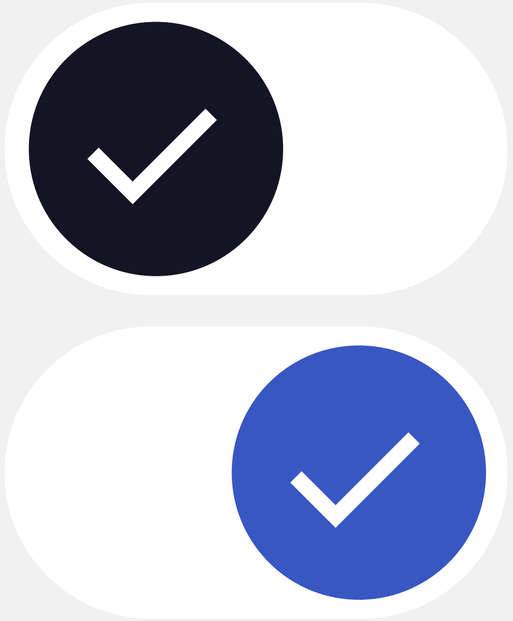
Consider Supply Chain Impact:

As evidenced by frequent breach announcements, your organization’s compliance is only as strong as the weakest link in its supply chain. Evaluate your subcontractors and suppliers to ensure they meet CMMC requirements and work with them to align their cybersecurity practices with yours.

Align Compliance with Business Goals:

CMMC compliance impacts your broader business objectives, so consider compliance a competitive advantage when pursuing new DoD contracts. Even in non-DoD contracts, strong cybersecurity practices reduce risks and protect sensitive information, which can help you achieve other business goals.

Determine the Expertise You Need



Getting certified under the CMMC framework takes a team with the right mix of skills. You'll need experts who can handle technical systems, manage daily operations, evaluate potential threats and vulnerabilities, and ensure compliance. While some of your current staff may already have experience with IT support or system design, it's unlikely that they also have the requisite expertise (or time!) to also manage threat monitoring or compliance documentation as well. That's why it's important to divide responsibilities—some people should focus on keeping your systems running, others on security, and others on meeting CMMC requirements. No matter your company's size, you'll need to assign roles across individuals, teams, or outside providers so no single person is responsible for everything.

Whether these roles are filled internally or through partners, you'll need coverage in the following key areas:

Systems Architect:

Design the overall architecture of the IT environment to ensure it aligns with CMMC requirements, including developing a secure architecture for handling CUI, creating segmentation strategies to isolate sensitive data within defined system boundaries, and ensuring scalability for future compliance needs as business operations change.

Systems Integrator:

Responsible for configuring the technical environment to meet CMMC requirements, including implementing security controls such as MFA, encryption, and access management; managing integrations between existing systems and new compliance tools; and addressing compatibility issues and minimizing downtime during system upgrades.

Managed Services Provider / IT Day-to-Day Support:

Provide ongoing IT support and maintenance for systems in scope for CMMC compliance, including monitoring system performance and addressing technical issues promptly; managing routine updates, patches, and backups to maintain security; and supporting end-users with troubleshooting and IT questions.

Managed Security Services Providers (MSSP) / Cybersecurity Team:

Focus on cybersecurity monitoring to detect threats and ensure adherence to security practices. Additional, proactive services include conducting vulnerability assessments, penetration testing, and threat monitoring; implementing advanced security solutions (such as intrusion detection systems (IDS) or endpoint protection); and providing incident response (IR) services in the case of a material incident.

CMMC Compliance Experts:

Guide organizations through the certification process by interpreting CMMC requirements and ensuring adherence. This includes conducting gap analyses to identify areas where current practices fall short of CMMC standards, preparing necessary documentation, including System Security Plans (SSPs) and Plans of Action & Milestones (POA&Ms), and advising on strategies to meet specific requirements efficiently.

When these roles work together effectively, your organization can address all aspects of CMMC compliance. In many cases, service providers can deliver some, or even all of these capabilities as part of their managed services offerings. The specific expertise needed depends on your organization's size, the complexity of your IT systems, and how much of your business is dedicated to DoD work.

Whether you have all the expertise in house or use one or multiple providers, you must consider how everyone works together cohesively. Clearly outlined responsibilities and a tightly integrated team can make the difference between passing your assessment and missing key assessment objectives.

SECOND KEY TO SUCCESS:

Deploying Technical Solutions

Deploying technical solutions for CMMC requires you to balance compliance requirements with operational efficiency.

Execute the strategy

Define in-scope systems

Identify all the systems, personnel, and processes that interact with CUI. Use the CMMC scoping guide to classify assets into:

- **Controlled Environments (CE):** Systems directly handling CUI.
- **Security Protection Assets (SPA):** Tools, such as firewalls, Endpoint Detection and Response (EDR) solutions, Security Information and Event Management (SIEM) systems, and MFA mechanisms, that safeguard CE.
- **Contractor Risk Managed Assets (CRMA):** These are assets that can store, process, or transmit CUI workflows, however, they are not intended to do so.

Map configurations to NIST 800-171A

Align in-scope systems with the 320 assessment objectives outlined in NIST SP 800-171A rev. 2, which underpins CMMC Level 2. (For a clarified view of the 320 assessment objectives, download this eBook.) For example, the control AC.L2-3.1.11 in the Access Control domain dictates the need to "Terminate (automatically) a user session after a defined condition," and is measured via two related assessment objectives:

- Defining the conditions that would result in an automatically terminated user session (which needs to be clearly documented)
- The technology that will perform the automatic termination when such conditions are met.

In most cases, a given control has multiple assessment objectives. For example, CM.L2-3.4.7 in the Configuration Management domain requires the organization to "Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services." This control has 15(!) associated assessment objectives that all need to be met and documented.

Use the NIST 800-171A assessment objectives to validate whether your controls meet required standards, then document and resolve any gaps you discover during this process.

Catalog operational technology (OT) & Internet of Things (IoT)

OT and IoT devices, such as industrial sensors and smart cameras, frequently lack built-in security, making them vulnerable entry points. Mitigate these risks by cataloging all OT and IoT assets and their data flows, isolating OT and IoT systems from CUI environments using firewalls or virtual local area networks (VLANs). Track vulnerabilities in these devices and apply updates promptly.

Deploying enclaves

Enclaves can be an effective approach to move quickly while managing implementation costs. Start with a Pilot Program approach, where you use a small, isolated environment (for example, a cloud enclave) to test your CMMC controls. Once you have tested this pilot well, you can bring your other systems into the enclave. Watch for an inflection point when it makes sense to transition to an all-in approach.

Tip: In our experience, when over 30% of company employees need access to the enclaves, its time to reevaluate whether an all-in approach is more effective.

All-in deployment

If you've chosen an all-in deployment model, you'll need to budget time and money for data migration, and potential downtime. Once your operations move to this restricted environment, you'll need to enforce strict access controls, prohibit unencrypted transfers of CUI, and conduct continuous monitoring and quarterly audits for the entire IT environment to ensure ongoing compliance with CMMC requirements.

Follow secure by design best practices

Adopting Security by Design best practices ensures cybersecurity is prioritized at every stage of system development. For example, zero-trust architecture (ZTA) eliminates implicit trust by continuously validating user and device access through micro-segmentation and strict access controls. Similarly, implementing the least privilege principle in NIST 800-160 restricts users and processes to the minimum access required for their roles, reducing your attack surfaces and mitigating the risks of lateral movement. Continuous improvement, another key component of Secure by Design practices, includes regular audits, ongoing updates to security protocols, and proactive threat hunting to ensure alignment with key standards, including CMMC and NIST SP 800-171.

THIRD KEY TO SUCCESS:

Ongoing Management

Ongoing management to maintain CMMC compliance requires organizations to do all the “basics” of traditional IT management but also adds the complexity of ensuring compliant IT management in every environment.

Traditional IT management

Traditional IT management consists of all of the actions you expect in operating any IT system regardless of compliance requirements. For example, traditional IT management includes:

- Routine hardware and software updates.
- Support desks addressing user-reported issues in a timely manner.
- Routine moves, adds, and changes to the system.
- Business planning involves budgeting for regular hardware and software upgrades.

Compliant IT management

Compliant IT Management adds a lot more complexity to existing IT management processes. This is driven by the level of maturity in operations required to meet and maintain compliance. For example, compliant IT management includes:

- Standard processes that align workflows with NIST 800-171.
- Artifact collection, which includes maintaining records of access logs and incident reports for assessors.
- Reporting and reviews, such as quarterly compliance reviews with stakeholders and annual self-assessments against CMMC Level 2 controls.
- Change management, including assessing the security impact of every system modification and documentation of approvals.

Traditional IT Management vs. Compliant IT Management

	Traditional IT Management	Compliant IT Management
Reactive troubleshooting	✓	✓
Ad-hoc change approvals	✓	✓
Basic user support	✓	✓
General system maintenance	✓	✓
Proactive monitoring aligned with NIST 800-171A controls		✓
Formalized change management workflows		✓
Role-specific training on CUI handling		✓
Continuous artifact collection for audits		✓

Beyond these basics, staying aligned with the DoD's changing requirements is also important. Key ways to do this include:

- Subscribing to DoD newsletters, CyberAB (the official accreditation body for CMMC) announcements, and NIST publications to track changes in compliance standards. Do note that sometimes standards and regulations are on different cycles. For example, NIST 800-171 is currently on revision 3; however, the CMMC rule is specifically designed around revision 2.
- Updating system baselines and security policies in response to new threats or regulatory changes, such as revised NIST guidelines or CMMC scoping rules.

FORTH KEY TO SUCCESS:

Security Monitoring

Effective security monitoring is a key aspect of CMMC compliance, but sometimes, teams are not sure what tools to use or who is responsible for which activities. Proper security monitoring requires both reactive and proactive activities to ensure the health of the environment. This is one area where all but the largest companies outsource this function. Some things to consider include when choosing a security provider:

Security monitoring

Conduct continuous monitoring (SC.L2-3.13.1), using security tools, such as Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR), to aggregate and analyze logs from firewalls, endpoints, and access controls for real-time threat detection. Store audit logs (such as access attempts and configuration changes) for at least 24 months to support incident investigations and compliance audits.

Alignment with audit policies

Configure your systems to “enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.” (Audit & Accountability domain). This should include recording many different types of events, including user logins (IA.L2-3.5.1 & IA.L2-3.5.2) and privilege escalations (AC.L2-3.1.5) as mandated by NIST SP 800-171. Conduct quarterly audits to validate that monitoring aligns with documented policies, including roles for log analysis and escalation procedures.

Separation of duties

Separation of duties (AC.L2-3.1.4) ensures no single individual has unchecked access or control over critical security processes. This reduces the potential risks of insider threats and errors. For CMMC compliance, this separation includes both access to systems as well as dividing responsibilities between teams handling threat detection, threat analysis, and IR.

Threat hunting

Though not specifically required by NIST 800-171a, threat hunting is a best practice by proactively searching for potential issues. Use behavioral analytics and manual investigations to identify advanced threats (such as lateral movement or credential misuse) that evade automated detection. Cross-reference internal data with external feeds, such as CISA cybersecurity alerts and advisories, to prioritize risks related to CUI.

Tabletop exercises

NSIT 800-171 requires companies to conduct regular exercises to test your IR plans (IR.L2-3.6.3). These exercises may include IT, legal, and executive personnel to validate each team's role during a material incident. Document any issues identified during these exercises, such as communication delays or unclear protocols, and update your incident plans accordingly.

Vulnerability scanning

Perform automated scans regularly (and after significant system changes) to identify vulnerabilities, document your findings, and remediate critical flaws within 14 days of identification (RA.L2-3.11.2). This includes all assets in the CMMC enclave, including cloud environments and third-party services.

Evidence and documentation

For both compliance, and cybersecurity reasons, it is important to maintain records of monitoring alerts, scan reports, threat-hunting findings, and exercise results. It is also prudent to store these in a centralized repository for C3PAO assessments. Make sure your policies explicitly define monitoring responsibilities, escalation workflows, and the tools used.

Remember that different security monitoring aspects can be done internally or externally. If you outsource, you may find that your internal IT team or your IT services provider does not have the necessary expertise and personnel to adequately meet your security needs, requiring you to hire a separate security services firm. If that's the case, you'll need to make sure there is close coordination and understanding of responsibilities so that no assessment objective is dropped accidentally.

If you work with an outside provider, make sure they have experience with NIST 800-171 and NIST 800-171A, experience with clients in the defense sector, and have experience using the tools and frameworks necessary to help you achieve and maintain CMMC compliance.

FIFTH KEY TO SUCCESS:

Compliance Management

Maintaining compliance with CMMC requires consistent management efforts throughout the year. A mature compliance management program will require you to:

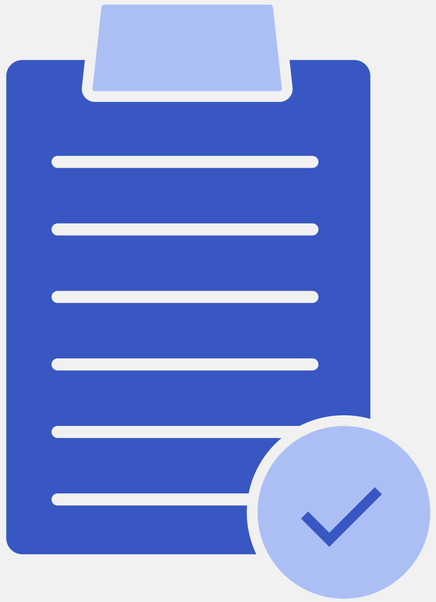
1. Develop and follow designated policies and procedures, including an Incident Response (IR) Plan that defines roles, communication protocols, and recovery steps for breaches involving CUI. Update these policies and procedures at least biannually or after any change to the environment.
2. Conduct periodic risk assessments to identify new threats or control gaps using NIST SP 800-30 as a framework. Maintain written policies and make sure they are accessible to all personnel who handle CUI.
3. Develop a System Security Plan (SSP) that includes the boundaries of in-scope systems and data flows and a map showing implemented controls. After assessment, it may also include a POA&M for unresolved gaps, with deadlines and responsible parties listed.
4. Conduct regular reviews and ensure documentation is up to date. Validate the accuracy of your SSP against current infrastructure quarterly. If you have a POA&M, review progress and adjust timelines if necessary. Reassess against CMMC Level 2 requirements at least once a year.
5. Maintain ongoing efforts throughout the year, including:
    - Conduct evidence gathering, which involves collecting artifacts such as system logs, audit trails, configuration reports, and screenshots to demonstrate the implementation of security controls
    - Organizing and storing these artifacts systematically using tools, such as compliance management platforms, to ensure they are readily accessible for audits.
    - Keep your documentation updated through periodic reviews of policies, procedures, and plans to ensure they reflect changes in operations or security environments.
    - Conduct regular internal audits to identify gaps in compliance, address vulnerabilities, and ensure ongoing alignment with NIST SP 800-171 requirements.
    - Update network diagrams, data flow maps, and risk assessments to account for new technologies or processes introduced during the year.

Customer Responsibility Matrix

As the Organization Seeking Certification (OSC), you are responsible for maintaining a master Customer Responsibility Matrix (CRM) that outlines the internal and external parties that help to satisfy a given assessment objective. Every external vendor you work with on CMMC compliance must provide a Customer Responsibility Matrix (CRM) that clearly outlines at the assessment objective level the extent to which they help you meet the objective. This matrix is required in the final rule (defined in 32 CFR Part 170). The matrix specifies whether your organization, a vendor (or multiple vendors), or a combination are responsible for implementing each NIST 800-171 control and documents how compliance will be validated.

BONUS:

Tips to prepare for a CMMC assessment



The CMMC program went into effect in December 2024 and C3PAO assessments officially started the following month. As the industry gains experience and the program matures, we've developed the following tips to help prepare for an assessment.

Preparing for a CMMC assessment requires planning, documentation, and alignment with DoD requirements. Keep in mind that CMMC Level 2 certification typically requires 12–18 months from initial scoping to assessment readiness. In addition, assessors expect a minimum amount of time (typically between 3-6 months), in which the final system design and configuration has been operating to ensure consistency and adherence to the policies, processes, and configurations outlined in your documentation. That means that you can't expect to sit for the assessment the day after you deploy your system. Organizations already aligned with NIST 800-171 may reduce timelines by 3–6 months, while third-party dependencies (such as FedRAMP cloud providers) can accelerate or delay progress based on their compliance status. Below is a guide so you know what to expect in this process.

Maturity does not equal assessment readiness

Achieving and maintaining compliance does not equate to assessment readiness. Even the most mature organizations will need to take steps to ensure they experience a successful assessment.

Preparing for an assessment

Scheduling your assessment

Currently, there aren't enough C3PAO assessors available to conduct assessments, which means there's a backlog. Schedule your assessment, but make sure you're ready when the time comes. Assessment failures are logged and will impact your ability to secure contracts. Also, it's important to check the availability of your vendors when scheduling an assessment. Similar to assessors, many vendors are overloaded with assessment requests, straining capacity and the availability of personnel.

If third-party vendors are part of your approach, ensure that they are available during your preferred assessment window. Like C3PAOs, many providers are capacity-constrained with respect to assessment scheduling.

Pick an assessor

Select a C3PAO accredited by the CyberAB. When choosing an assessor, consider finding one familiar with your industry and situation (for example, a vendor familiar with professional services vs. manufacturing), check to see if they have worked with defense contractors with similar scoping needs in the past, and look at their availability. Remember, many assessors are overwhelmed in the early stages of the program and are currently scheduling assessments 6–12 months in advance.

Assessment prep

Your prep includes validating all your documentation and diagrams to gain an understanding of your system boundaries. The documentation must be accurate and defensible; be prepared to answer questions from your assessor. Your diagrams should show your data flows and how data is being protected, and make sure your customer responsibility matrix is accurate and defensible. Test all of this by doing a tabletop assessment that includes all of the vendors involved in managing your compliance. This exercise should walk through a mock assessment to make sure everyone, including all vendors involved, knows what their roles are and can answer to the objectives they are responsible for.

Assessment process

Every C3PAO has their own process, but generally speaking, the assessment process will follow this path:

1. The first step of the process is a scoping call that walks through your compliance boundary and data flow diagrams so they can quickly assess your strategy. You will not proceed to the assessment stage if this information is not ready. You'll need to go back and reschedule for a time when you are better prepared for the assessment.
2. Submit your documentation, including your SSP, evidence, and reports, such as access logs and training records, for review.
3. The actual assessment which includes interviews with IT staff and leadership to validate your policies and technical testing to verify your controls. This may be done on-site or remotely.
4. Post-assessment, you'll receive a score that determines your next steps.

What to expect during an assessment

During a CMMC Level 2 assessment, you should expect a multi-day evaluation conducted by a C3PAO to verify compliance with all 110 controls outlined in NIST SP 800-171. The assessor will use the 320 assessment objectives in NIST 800-171a as their reference and require detailed evidence and documentation demonstrating proper implementation.

A key purpose of the assessment is that the documentation aligns exactly to the actual implementation and management of the environment.

Common assessment challenges

1. The first one is obvious and unavoidable. High demand for C3PAOs has resulted in backlogs that can delay your assessment. This has led to many organizations "pre-scheduling" their assessment before they're ready. Doing so introduces the risk of rushing preparation, putting their achievement at risk. **Schedule your assessment early but only *after* you are certain to be prepared.**

2. Many organizations have documentation gaps, such as incomplete SSPs, resulting in conditional scores. **Review your SSP to ensure it's up to date before your assessment.**

3. Legacy systems often lack the ability to apply encryption or log activity as required. **Address technical debt before you get to the assessment stage.**

4. If you don't have all your supporting documentation in order, you'll have trouble with your assessment. **Your supporting documentation should include policies, procedures, network diagrams, and CUI data flow diagrams.**

5. Don't be disorganized. **Follow C3PAO submission guidelines on organizing your evidence and ensure you have the documents signed and dated if required.**

Conditional certification & POA&Ms

There are a limited number of controls that can be addressed through a POA&M, and many assessment objectives constitute an "instant failure" if not met at the time of the assessment, with no ability to put them on a temporary POA&M. For assessment objectives that are not an "instant failure," a "conditional" certification may be granted. In this situation, a POA&M is developed and all POA&M items must be closed out within 180 days before a final certification is issued. If you are issued a POA&M, be sure to have a detailed plan for how to remediate these gaps and have clearly assigned responsibilities to ensure all POA&M items have been fully addressed.

Conclusion

This eBook provides clear guidance on the five critical steps that will set your organization on the path to success in CMMC Level 2 compliance. CMMC Level 2 is no longer a distant requirement—it has already become a reality for many contractors and subcontractors in the DIB. Organizations that postpone compliance risk losing out on critical contracts and falling behind competitors who have already completed the CMMC assessment process successfully.

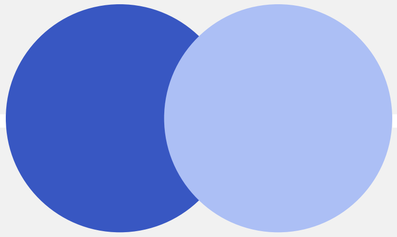
Next steps

The time to achieve CMMC compliance is now. Take these steps to get started:

- Identify the people, processes, and systems that interact with CUI.
- Build a strategy to define your planned compliance scopeand required investments.
- Work with your leadership team to get buy-in and resources for this initiative.
- Develop a detailed project plan that identifies key milestones and responsibilities.
- Consider partnerships with experienced CMMC consultants or solution providers to accelerate your journey.

Remember, achieving CMMC Level 2 is not just about meeting a regulatory requirement—it's about strengthening your organization's cybersecurity posture, protecting sensitive information, and positioning your business as a trusted partner in the defense supply chain.

Visit us at: c3isit.com



Appendices

Glossary of Key Terms

Cybersecurity Maturity Model Certification - The U.S. Department of Defense developed this program to enforce cybersecurity standards across the Defense Industrial Base. It ensures contractors and subcontractors protect sensitive unclassified information, such as Federal Contract Information and Controlled Unclassified Information, through compliance with defined maturity levels.

Federal Contract Information - Information generated for or provided by the government under a contract to develop or deliver a product or service. FCI does not require special safeguarding but must be protected under basic cyber hygiene practices specified in FAR 52.204-21 and is not intended for public release.

Controlled Unclassified Information - Information requiring safeguarding or dissemination controls pursuant to federal law, regulations, or government-wide policies. Examples include technical drawings, financial data, and research results critical to national security. The National Archives and Records Administration (NARA) oversees the CUI program.

Defense Federal Acquisition Regulation Supplement - A supplement to the Federal Acquisition Regulation (FAR) that governs DoD procurement processes. DFARS clauses, such as 252.204-7012, mandate cybersecurity requirements for contractors handling CUI, including compliance with NIST SP 800-171 controls.

Federal Risk and Authorization Management Program
A government-wide program providing standardized security assessments for cloud services used by federal agencies. Cloud providers must meet FedRAMP Moderate or equivalent standards to handle CUI under DFARS 252.204-7012.

Plan of Action & Milestones - A document outlining how an organization plans to address gaps in its cybersecurity practices. POA&Ms are required for CMMC compliance when certain controls are unmet during assessments. Organizations must close POA&M items within 180 days to maintain certification.

Certified Third-Party Assessment Organization - An independent organization accredited by the Cyber AB to conduct formal CMMC assessments. C3PAOs validate whether contractors meet the required cybersecurity practices for their designated maturity level.

NIST SP 800-171 - This National Institute of Standards and Technology publication defines 110 security requirements for protecting CUI in non-federal systems. These requirements form the basis of CMMC Level 2 compliance.

Zero Trust Architecture (ZTA) - ZTA is a cybersecurity model that assumes no user or system is inherently trustworthy. It requires continuous verification of access requests, segmentation of networks, and encryption of data in transit and at rest.

Customer Responsibility Matrix - A document required under 32 CFR Part 170 that outlines which entity—contractor, vendor, or both—is responsible for implementing specific cybersecurity controls.

CMMC Resources

eBook: An Introduction to Cybersecurity Maturity Model Certification

This comprehensive eBook breaks down the CMMC framework, CMMC levels, and the benefits of certification for organizations in the Defense Industrial Base (DIB).

eBook: CMMC Level 2 Controls & Assessment Objectives

CMMC Level 2 compliance is crucial for DIB organizations handling CUI, involving 110 controls from NIST SP 800-171 and 320 assessment objectives in NIST SP 800-171A to ensure cybersecurity readiness.

Webinar: Learn How to Fast-track CMMC Compliance with the C3 Suite

CMMC is now the reality for nearly every company that works with the DoD. The rule is complex, and the timeline is tight: many primes are already enforcing adherence to CMMC standards. Watch our webinar on-demand to learn the critical steps necessary for CMMC compliance.

About C3

C3 accelerates CMMC cybersecurity compliance by designing, implementing, and managing IT & cybersecurity solutions purpose-built for the U.S. Defense Industrial Base.

C3 offers a wide range of compliance-centric managed IT services—from targeted services customized to fit within a client's existing environment to the C3 Suite, a set of packaged solutions, including fully managed CMMC offerings purpose-built to meet compliance requirements.

By rooting our prescriptive solutions in cybersecurity best practices and an intimate understanding of CMMC assessment requirements, the C3 Suite minimizes the risk of non-compliance and accelerates compliance timelines, enabling defense contractors to more easily achieve and maintain CMMC Level 2 compliance with confidence.

A leading provider of Microsoft 365 GCC High and Azure Government, C3 is a leading AOS-G Partner, a CMMC Registered Provider Organization (RPO), and one of the few companies to successfully support the DIBCAC assessment of a CMMC Third-Party Assessment Organization (C3PAO).

Visit us at: c3isit.com