CMMC Compliance Checklist

Kickstart Your Compliance Journey with Egnyte

EGNYTE

Introduction

As part of a wider effort to protect its supply chain and the Defense Industrial Base (DIB) against cybersecurity threats, the U.S. Department of Defense plans to implement the Cybersecurity Maturity Model Certification in 2025.

As you probably know, CMMC is an extremely comprehensive IT Security initiative that can take the average company up to 18 months to achieve, even when they have the required skill-sets in place. As a result, if your company does work with the U.S. Department of Defense, the time to prepare for CMMC is now. The goal of this checklist is to help you to get the process started.

Why You Need to Take Action Now

Here's the most recent CMMC update: In October 2024, the US DoD issued a Final Rule for CMMC, which confirmed its planned 2025 implementation date. The rule also codified when CMMC will become a formal DoD contractual requirement. That's why it's in your best interest to take action now, so that your company can proactively safeguard the revenue that it generates from DoD contracts.

As you familiarize yourself with CMMC, you may see clauses referencing:

- DFARS 252.204-7012 (Safeguarding Covered Defense Information & Cyber Incident Reporting)
- DFARS 252.204-7019 (Notice of NIST SP 800-171 DoD Assessment Requirements)
- DFARS 252.204-7020 (NIST SP 800-171 DoD Assessment Requirements)
- DFARS 252.204-7021 (Cybersecurity Maturity Model Certification Requirements)

These DFARS clauses collectively formulate the core requirements of CMMC.

The Next Step in Your CMMC Journey

Thankfully, the DoD's benchmarks are all achievable with proper planning and execution by your company. This ebook contains:

- A detailed CMMC checklist—which includes practical IT Security and project-related recommendations—so you can build a CMMC project plan of your own.
- A listing of common pitfalls that you should avoid.
- Convenient resources and ways that Egnyte can help.

Let's begin with the CMMC checklist on the following page.

Your Compliance Checklist

- [ ] Verify that CMMC Applies to Your Organization
- [ ] Decide on Maturity Level
- [ ] Select a Project Lead
- [ ] Define Scope of CMMC Environment
- [ ] Engage Your Executive Team and Confirm Budget for CMMC
- [ ] Document Your Environment and Controls (System Security Plan: SSP)
- [ ] Deploy A Secure Data Enclave for Handling CUI
- [ ] Identify and Move CUI into the Secure Data Enclave
- [ ] Develop Policies and Train Employees
- [ ] Define Compliance Review-and-Approval Workflows
- [ ] Conduct Your Self-Assessment
- [ ] Create and Submit Plan of Action and Milestones (POA&M)

VERIFY THAT CMMC APPLIES TO YOUR ORGANIZATION

The first step is to determine whether you are required to comply with CMMC at all. In general, if you are a contractor or subcontractor to the U.S. Department of Defense, then you are part of the Defense Industrial Base (DIB) and are likely to be subject to CMMC requirements as part of your contract if you handle Controlled Unclassified Information (CUI) and/or Federal Contract Information (FCI). In the future, how will you know for sure? Compliance requirements, including level, will appear as language in your contract. (See the Final Rule in the U.S. government's Federal Register for more details).

Even if the DoD does not represent a majority of your business, you may still handle FCI in flow-down contracts, and CUI such as specifications and delivery schedules for products and services supplied to the DoD.

DECIDE ON MATURITY LEVEL

The CMMC levels represent an escalating set of commitments for certification, so you'll want to determine which one is appropriate for your business needs. If you only handle FCI, you'll need to comply with Level 1. If you handle both FCI and CUI information, you will need to comply with Level 2. Finally, if you are participating in larger contracts with more sensitive products and services, you may need to comply with Level 3.

Typically, your responsibility for compliance and the appropriate level will be explicitly spelled out in contracts and purchase agreements, either directly from the DoD, or via a flow-down contract if you are a subcontractor. You'll want to confirm with the contracting authority if it's not clear.

SELECT A PROJECT LEAD

Once you determine the level you will need to comply with, you'll need to identify or appoint a CMMC Lead within your organization, and provide the lead with significant executive support. They will be the champion for the project and work with outside consultants as necessary. The person in that role will need to develop a high-level of understanding of the CMMC requirements.

Larger organizations may want to dedicate a small team to CMMC compliance. As you assign members to the team, a best practice is to do it along the lines of the DoD's CMMC practice areas.

DEFINE SCOPE OF CMMC ENVIRONMENT

Defining the scope of the infrastructure included for CMMC compliance is critical. If defined too broadly, you'll incur additional costs and complexity, but if defined too narrowly, your users will be unable to work effectively. The best approach is to work with a CMMC partner like Egnyte to discuss your CUI processing environment and to determine where there may be opportunities to reduce your overall assessment scope.

ENGAGE YOUR EXECUTIVE TEAM AND CONFIRM BUDGET FOR CMMC

CMMC certification can be complex and expensive, so you'll want to begin the process with your executive team at this point to establish a budget for CMMC compliance.

This will likely depend on the value of current and future DoD contracts to your organization. However, because CMMC compliance consists of best practice cybersecurity processes, there will be intangible benefits as well. As your team learns and implements CMMC best practices, you'll reduce cybersecurity risk to your organization at large.

DOCUMENT YOUR ENVIRONMENT AND CONTROLS (THE SSP)

According to NIST, the System Security Plan (SSP) "..describes: the system boundary; operational environment; how security requirements are implemented; and the relationships with or connections to other systems." In other words, it is a formal, written plan that documents the infrastructure (within scope), associated risks, and security controls in place (or planned) to mitigate those risks.

When it comes time for your assessment, you will need to produce complete documentation on the system under control. This calls for clearly defined and documented boundary diagrams, network architecture, services descriptions, and data flows for CUI, as well as documented processes and procedures for dealing with it. Getting started with the security control review early provides a baseline for the project and an early indication of your largest gaps.

Virtually no small- or mid-sized company has existing documentation to the depth and complexity required. Most often major components of the architecture are outsourced, and little to no formal documentation may exist. Larger companies may have the people and documentation in-house, but the information can be spread across multiple IT teams rather than consolidated into a comprehensive document. Whether big or small, the key point here is that you need a comprehensive inventory of exactly what falls into scope, who is responsible for each control, and how it's managed.

DEPLOY A SECURE ENCLAVE FOR HANDLING CUI

Because the scope of the infrastructure is so critical to successful CMMC compliance, most organizations deploy a separate, highly secure system referred to as a "Secure Data Enclave" within their larger environment to store CUI/FCI information. This allows more careful control and monitoring of the way the information is accessed and used by limiting the cyberattack surface area. Most importantly, this greatly simplifies the burden of demonstrating compliance. From a practical standpoint, a Secure Data Enclave can be achieved by working with a Cloud Service Provider (CSP) like Egnyte, or on-premises via network segmentation.

IDENTIFY AND MOVE CUI INTO THE ENCLAVE

Based on the contractual and standard definitions, you'll need to identify what CUI data is (likely) in your organization. At this stage, make sure the obvious CUI is marked appropriately. You'll know which contracts and projects generate CUI data so that will be your starting point.

However, it's quite likely that CUI data has "leaked" into other parts of your organization, so you will need to perform a mapping exercise to find that data, and then move it into the secure data enclave. A data classification solution may be required to help locate CUI in repositories such as Microsoft SharePoint sites, file servers and email systems (Egnyte provides such solutions as a complement to its secure data enclave offering).

DEVELOP POLICIES AND TRAIN EMPLOYEES

CMMC is not just about protecting data, it's also about how to use that data safely. You'll need to develop internal policies that cover who/how/when CUI data can be accessed. You'll need to define how it is to be used and modified, and most importantly, what is not allowed. For example, some organizations find it necessary to limit printed copies. They also need to limit replication of the data on unsecured laptops. Once employees who deal with CUI data have been identified, you will need to train them on proper procedures for safe handling and management of CUI data. It's also helpful to train all employees to be aware of CUI even if they are not expected to handle it. This training should be performed on a routine basis—not just for new employees, but to help reinforce best practices for existing employees, too.

DEFINE COMPLIANCE REVIEW-AND-APPROVAL WORKFLOWS

As you get closer to completing your assessment, you'll need to set up the workflow for reviews and approvals of the various components of the project. Identify who will be responsible for capturing the actual compliance artifacts, who will review them, and who will provide final approval. Note that there are at least 110 practices to comply with at Level 2 and 3, so compliance with the practices will represent a significant resource commitment.

CONDUCT YOUR SELF-ASSESSMENT

Once the System Security Plan (SSP) has been documented, it will be necessary to perform a self-assessment. This is the point where you'll identify the gaps in your coverage of security controls, as you fill out the assessment document. Note that some items may not be applicable to your situation.

In the event your solution does have controls in place to meet a requirement, you'll need to demonstrate that with documentation including screenshots, written policies, or other information (admins of Egnyte's secure data enclave solution can auto-generate that information from an optional dashboard within Egnyte's solution). This is true whether you assemble the control yourself, or whether it is inherited from a solution you purchased. Finally, almost all organizations discover gaps in coverage of security controls that will need to be addressed in the future. These need to be carefully documented with a plan to address them including a budget and schedule.

CREATE AND SUBMIT PLAN OF ACTION AND MILESTONES (POA&M)

A Plan of Action and Milestones (POA&M) will be your response to any gaps in control coverage discovered during the self assessment. It details resources (People, Process, Technology) required to address the missing control. In the case of a complex project, it should include intermediate milestones with scheduled completion dates for the milestones.

Prior to your engagement with the Certified Third-Party Assessor Organization, or C3PAO, your organization must address all compliance and operational POA&Ms, leaving no incomplete CMMC controls. During the CMMC Assessment process, the Assessor may determine that there isn't objective evidence that one of your CMMC controls has been met. In that case, you will be placed into a POA&M, but you could unfortunately fail the assessment.

Common Pitfalls to Avoid

When implementing the CMMC checklist, here are the common pitfalls to avoid.

1. WAITING TOO LONG

Many organizations assume that CMMC compliance can be achieved in a short period, perhaps as little as several months, because they already have cybersecurity policies and practices in place.

However, experience has shown that even the most sophisticated organizations can take many months , if not years, to achieve and document compliance. This is because CMMC compliance is more than just an IT exercise and requires more than just a technological fix. First, detailed planning is required, often leading to additional technology purchases. Additionally, remember that all employees will need to be trained, while new processes and procedures will need to replace old ones. This all requires executive level engagement, not just spending approvals.

2. SCOPING TOO BROADLY

Out of an abundance of caution, security engineers can sometimes be more inclusive than they need be in defining the scope of the infrastructure to fall under CMMC. In rare cases, they may mis-define CUI too broadly, so data is listed as CUI when it isn't. More often, they simply don't know where their CUI is, so they include more infrastructure than is necessary. This can lead to including multiple repositories in scope, and associated infrastructure and network capabilities like Identity and Access Management (IAM) services across many different systems. A broader scope results in a much more complex and expensive path to CMMC.

Likewise, engineers sometimes target a higher CMMC level than necessary, striving for Level 2 when Level 1 is sufficient for their FCI data. Like scoping the infrastructure too broadly, striving for unnecessary levels of CMMC compliance multiplies cost, complexity, and resources. Even if Level 2 compliance is necessary, it might be more practical and less disruptive for some companies to attain Level 1 compliance first before attempting Level 2 compliance.

Another, even more subtle, scoping problem is a failure to include partners and supply chain participants in planning for CMMC compliance. For example, unique specifications sent to a supplier may contain CUI data. Therefore, that partner should be notified that they may need to comply with CMMC requirements as well. At the very least, the information needs to be passed in a secure way and employees need to be trained on proper handling.†

3. LACK OF DETAIL

When working through checklists, companies sometimes don't spend enough time documenting the details on key focus areas in the requirements. For example, logging should be documented to show not only that logs are collected, but also how often they are collected, how they are stored, and most importantly, how they are reviewed and analyzed. Likewise, access controls may be neglected in detailed documentation because they are complex and cross many different internal system boundaries. Documentation of access controls should include not only how they work, but the processes for how they are maintained and verified.

Finally, many security engineers often leave out detailed documentation on procedures, both for admins configuring and monitoring the system as well as users handling CUI data itself. It's important to document proper procedures so that deviations from normal processes can be detected quickly before data is put at risk.

4. LACK OF CONTINUOUS MONITORING

Many organizations struggle to "climb the CMMC compliance mountain" only to relax and become complacent at the top. CMMC requires continuous review, monitoring and improvement. The best way to do this is to choose tools and architecture (like Egnyte) that allow you to automate as much of the ongoing monitoring and maintenance as possible.

5. VIEWING CMMC AS JUST A ONE-TIME EVENT

CMMC compliance is not a one-time event or checkbox exercise. In reality, it affects people, processes, and technology, often profoundly. Your people may need significant training, cultures need to be modified, new processes and procedures and even business workflows may need to change.

Technology needs to support the new requirements, but these deployments should never be regarded as a static state. Over time, your business will change, which changes your risk profile and attack surface. Meanwhile, new security risks will continue to emerge, and cybersecurity solutions will evolve with them. Therefore, your SSP will need frequent review and updating to meet those risks.

This is why the DoD plans for CMMC assessments to be performed on a regular basis rather than one time. CMMC compliance truly is a journey, not a destination.

How Egnyte Helps Companies On Their CMMC Journey

Egnyte provides a simple, secure data environment specifically designed to make compliance practical and affordable for small- and mid-sized businesses.

The Egnyte Gov Enterprise solution will save your IT and compliance teams weeks, if not months, of time each year. Meanwhile, business stakeholders will appreciate that it's easy to use and enables them to win/maintain DoD contracts while minimizing the amount of overhead (including third-party consulting hours) required to do so.

Egnyte's secure data enclave satisfies many CMMC requirements by default. The solution also includes proven data governance capabilities and the optional ability to discover CUI/FCI in third-party repositories, allowing you to limit the scope of your assessed environment. When it comes time to prepare for your next assessment, you simply click a few buttons in the optional Egnyte reporting interface to auto-generate much of the documentation that will be needed.

1	Secure Data Enclave With Inherited CMMC Controls (see Shared Responsibility Matrix on the following page)
2	Detailed Technical Implementation Guide
3	Optional Tools to Locate and Label Data in 3rd Party Repositories
4	Access to Practitioner Community
5	Access to Egnyte's CMMC Experts
6	Partner Recommendations to Address Skill-Set Gaps

EgnyteGov Enterprise Shared Responsibility Matrix

CMMC Practice / NIST SP 800-171 Security Requirements	Egnyte Provided	Provided by the Customer	Shared between Egnyte and the Customer	Total Number of Controls Required by NIST SP 800-171
Access Control	10	8	4	22
Awareness and Training	0	3	0	3
Audit and Accountability	2	2	5	9
Configuration Management	0	6	3	9
Identification and Authentication	9	2	0	11
Incident Response	0	2	1	3
Maintenance	0	6	0	6
Media Protection	0	8	1	9
Personnel Security	0	2	0	2
Physical Protection	0	6	0	6
Risk Assessment	0	1	2	3
Security Assessment	0	3	1	4
System and Communications Protection	3	6	7	16
System and Information Integrity	0	2	5	7
TOTALS	**24**	**57**	**29**	**110**

If you have questions about any of the practices that are referred to above, please reach out to your Egnyte contact.

Appendix: Additional Links and Resources

Information in this checklist is current as of December 2024.

Authoritative guidance for CMMC comes from the Department of Defense. You can find a link to the complete text of the CMMC Final Rule here: https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

The NIST document that the DoD uses as the basis for CMMC is NIST SP 800-171 (Rev 2), which can be accessed here: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Below you'll find more beneficial Egnyte resources on CMMC, including the following:

- Model Overview
- CMMC Requirements
- CMMC Assessment Guide

Schedule a CMMC Workshop

If you have additional questions about CMMC compliance, Egnyte is here to help.
Reach out to your Egnyte representative to schedule a CMMC Workshop, where we can discuss your company's CMMC journey in further detail, or click here.

Contact Us

+1-650-968-4018

1350 W. Middlefield Rd.
Mountain View, CA 94043, USA

www.egnyte.com