Top 7 Ways to Make CMMC Less of a Burden to Your Organization

The Cybersecurity Maturity Model Certification (CMMC) is a rigorous set of security requirements that organizations must meet to be eligible for certain U.S. Department of Defense contracts. Achieving compliance with CMMC can be a significant burden for many businesses, particularly ones that lack the necessary resources and expertise.

The Cybersecurity Maturity Model Certification (CMMC) is a rigorous set of security requirements that organizations must meet to be eligible for certain U.S. Department of Defense contracts. Achieving compliance with CMMC can be a significant burden for many businesses, particularly ones that lack the necessary resources and expertise.

To help contractors navigate the complex process of CMMC compliance, our Certified CMMC Professionals (CCPs) have put together the top 7 strategies designed to advance your progression towards certification. By adopting these methods and incorporating compliance-leaning procedures into your working operations and security posture, your organization can focus on its core business objectives, while **reducing the challenges of CMMC compliance and increasing chances of success.**

1 Define the Scope of CUI

The **single most overlooked step** in building a CMMC program is defining the scope of the Controlled Unclassified Information (CUI). Organizations must understand the flow of CUI into and through their organization. Once that is completed, security boundaries **specific to CUI** can be established. Subjecting your entire organization to the cost and burden of CMMC compliance might be considered impractical and financially prohibitive. Mapping CUI in your environment will allow for considerable scope and cost reductions tied to CMMC compliance.

Ensuring that all CUI is restricted to the CMMC security boundary reduces the cost of CMMC compliance, while minimizing risk to the organization. The most impactful ways to reduce the scope of your CUI and CMMC assessment are by:

- Limiting the number of users who can access CUI
- Segmenting systems that contain CUI
- Confining physical CUI media

EXAMPLE

SP6 has personnel who's performed CMMC readiness services for a large, international firm with 40,000 employees. By taking the time to map and understand where CUI lived on that organization's network, it was identified that only 3,000 employees had access to CUI. The organization established security boundaries tied to these users through techniques including network segmentation.

Rather than subject the entire organization to CMMC requirements, it was determined that over 90% of the organization's network and systems were not in scope for CMMC. **By focusing the NIST 800-171 controls to the 10% of the organization that did touch CUI, the organization was able to both significantly reduce the time, cost, and complexity of the CMMC requirement while simultaneously ensuring that the DoD's sensitive data was being thoroughly protected, as intended.**

Where Do I Start?

To understand the flow of your CUI, one must understand the products and services your organization provides to the DoD and the Federal Government. It's critical to ensure the business development function of your organization is involved in this process. They are the bodies making full contact with the government client via www.SAM.gov, industry events, or government-specific marketplaces.

Defining the scope and understanding the flow of your CUI can begin as soon as you secure a contract. Once an opportunity goes through the business development process, and the client has been identified as the DoD, validate that DFARS 252.204-7012 is present as this may imply CUI will be part of the product or service.

The Effect of Mapping CUI

From there, you can validate whether this is true or not with the Contract Officer. If valid, **make a note of the people, processes, and tools that will support that opportunity.** Do you need to start making some changes to reduce exposure, and therefore, risk? Likely. Document the end-to-end process identifying the non-negotiable steps – steps that if removed, your organization will not be successfully delivering the services committed. This is going to be part of your future CUI dataflow and CMMC ecosystem.

Think about how CUI enters your organization, how it is shared internally, and how it is shared with your critical suppliers. This is what we mean by documenting the flow and defining the scope.

NOTE: Do not forget your critical suppliers. This is your supply chain that needs visibility into the government specifications to provide you with the material required to finish the DoD goods/services.

While this process takes time, it's time extremely well-spent. **Don't lose sight of why your organization undertakes this task.** Mapping CUI is the only way that you can benefit from reducing the scope of the CMMC, while simultaneously ensuring the protection of critical data.

CUI data mapping is an exercise that can be executed without the assistance of a third party. If your organization does require additional assistance, SP6 offers CUI Data Mapping as part of our overall CMMC professional services.

2 Start Generating CMMC Evidence as Part of the Implementation Project

CMMC validates the implementation of the applicable NIST 800-171 controls and **part of the validation process is providing a C3PAO assessment team with "adequate and sufficient" evidence** that your controls meet the intent of the security requirements.

EXAMPLE

You have deployed FIPS-Validated encryption to protect the confidentiality of CUI at rest. Your policy and SSP both mentioned you have; however, CMMC requires that you "convince" the assessment team you are doing what your documentation says you are doing.

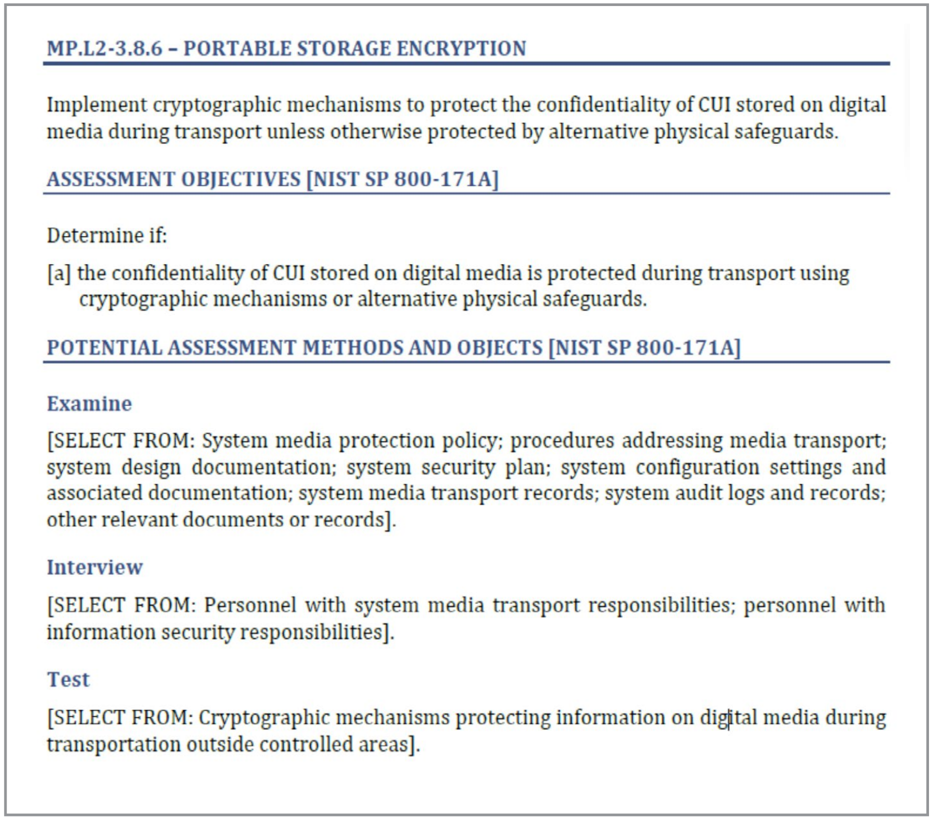
To do this, you generate evidence and provide the assessment team with:

- Information from the vendor stating their encryption module meets the FIPS-Validation standards
- Information from the NIST's cryptographic validation program page (i.e. Cryptographic Module Validation Program)
- Proof of the configuration setting, validating the FIPS mode is enforced. Having a FIPS-Validated compliance is one thing, enforcing the mode is another.

Compiling this evidence to a consolidated evidence folder, as you build your Security program, has many benefits, including:

- Assuring that security controls are properly implemented
- Being prepared and organized for your CMMC assessment
- Having a higher likelihood of passing your CMMC assessment, reducing the costs associated with needing to be re-assessed, and ensuring your organization's ability to deliver on contracts

Also, leverage the CMMC Assessment Guide:
The CMMC Assessment Guide provides your organization with exactly what an assessor will examine, pointing towards appropriate evidence to collect. For example:



MP.L2-3.8.6 – PORTABLE STORAGE ENCRYPTION

Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

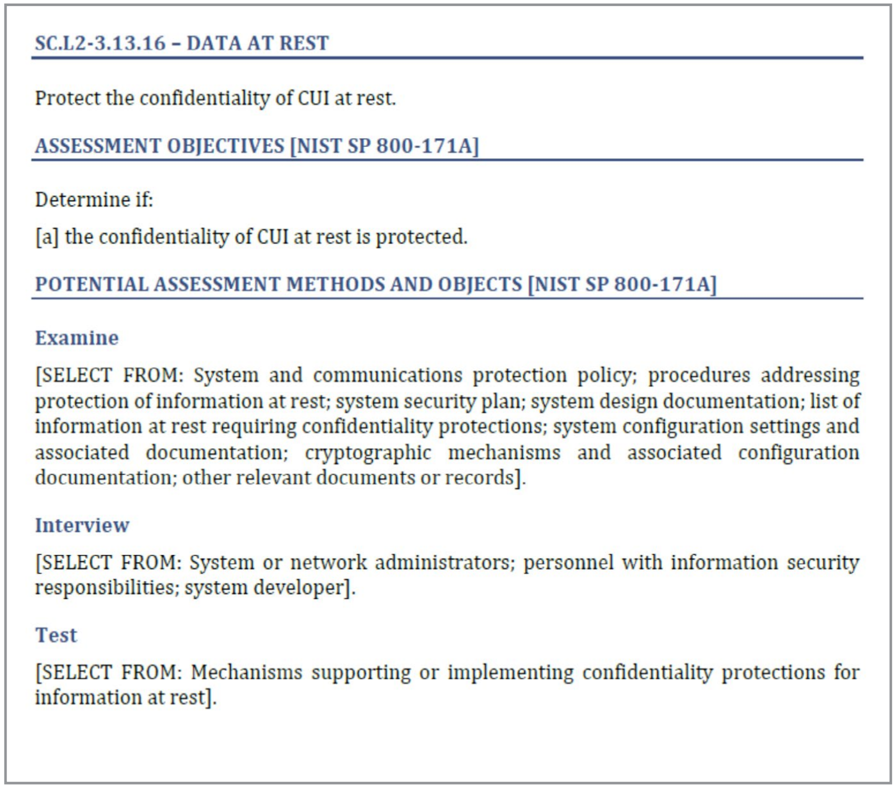
[SELECT FROM: System media protection policy; procedures addressing media transport; system design documentation; system security plan; system configuration settings and associated documentation; system media transport records; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system media transport responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Cryptographic mechanisms protecting information on digital media during transportation outside controlled areas].



SC.L2-3.13.16 – DATA AT REST

Protect the confidentiality of CUI at rest.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the confidentiality of CUI at rest is protected.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: System and communications protection policy; procedures addressing protection of information at rest; system security plan; system design documentation; list of information at rest requiring confidentiality protections; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; system developer].

Test

[SELECT FROM: Mechanisms supporting or implementing confidentiality protections for information at rest].

3 Consolidate Existing Organizational Technical Capabilities

When reading through the CMMC 2.0 control listings (as of May 1, 2023), there are **35 required technologies that need to be deployed and managed in your organization. That number is down from 47** technologies in what was CMMC 1.0.

Any new tool that is acquired brings the overhead of:

- Cost
- Deployment
- Integration with other tools
- Ongoing administration

There is a strategy that helps remediate this tool burden. Many security solutions are becoming more feature-rich and going beyond the functionality of a single point solution. Where possible, leverage one tool to satisfy multiple NIST 800-171 controls.

Consolidation of security tools can reduce licensing costs, minimize the scope of CUI, and streamline security operations to increase efficiency and objectivity for CMMC compliance. In many cases, certain tools can satisfy multiple requirements.

There may be a tradeoff in bypassing a single-purpose, best-of-breed solution, for the same tech that is built into another product. There are lots of tools with varying degrees of asset management functionality. The question becomes if the technology that's included is "good enough" to pass or if you need to, or prefer to, purchase and manage a dedicated point solution that may be more feature rich.

Reducing Tech Overlap Increases Efficiency

EXAMPLES

1. Most next generation firewalls (Palo Alto, CheckPoint, new Cisco) will do: Network Firewall, Content / DNS Filtering, Remote Access / VPN, Access Control List (ACL), Intrusion Detection/Prevention (IDS/IPS) all in one; though they have a patchwork of licenses (sometimes you have to buy extra licenses for that feature).
2. Most organizations use a directory service capability such as Active Directory (AD). Within AD, you could create groups for CUI-specific users and processes acting on behalf of those users. This is an excellent group object for CUI-specific devices, which can then be used to identify authorized users. Leverage these groups to enforce security settings that meet the NIST 800-171/CMMC standard. This modification immediately generates greater functionality from your current tool while utilizing something that's already in your tech stack for compliance.
3. Additionally, you could leverage your existing Remote Monitoring & Management (RMM) capability to build your asset inventory and categories (to identify CUI Assets, Security Protection Assets, Contractor Risk Managed Assets) which can help with risk-based decisions and investigation. If your SIEM or endpoint detection and response have this information, leverage those instead or validate all your systems until you identify an authoritative source.

When security tools are successfully consolidated, the organization can more easily benefit from automated security workflows, improved incident response, monitored compliance status, and reduced security tool sprawl.

4 Assess Organizational, Functional, or System Risk – Often

The DoD's assessment team, the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), has developed a list of the Top 10 "Other Than Satisfied" Requirements from their DIBCAC High Assessments. This is a list of the topmost failed NIST 800-171 security requirements. **At the top of that list is RA.L2.3.11.1, Periodically Assess Risk.**

To meet this security requirement, the DoD will validate that your organization has:

1. Implemented a policy that establishes and communicates organizational guidance for performing risk assessments, inclusive of its frequency (at least once per year).
2. Supporting processes and procedures for enforcing the policy to conduct periodic/annual risk assessments.
3. Performed at least one (formal or informal) risk assessment at the enterprise level, functional unit level, or system level within the last 12 months.

Some organizations are failing to realize they are already performing some type of "periodic risk assessment," to meet this control – ranging from security, privacy, safety, or all the above as part of their change management or configuration management process. Regardless, for

CMMC compliance, it's necessary to formalize and document proof of this practice (policy, processes, and procedures).

Risk Assessments Are a Common Business Practice

EXAMPLE

Users submit a change request to gain access to new systems or a cloud application, to open a firewall port, or to install a new program. After you receive the change request, you will likely verify its legitimacy, the business reason, if the user or system meets the access requirements, or if the change request aligns with existing policy or practices. This "informal" process assesses the potential adverse effect the change request may have on your common practices and procedures, that hopefully align with your policies.

If the change request is associated with changing a configuration item, such as allowing access to a new IP address range, opening a communication port, or enabling a protocol, do you validate the potential effect this will have on your System Security Plan (SSP) prior to executing the change?

Do you validate the cloud meets the DFARS 252.204-7012 requirements, ensuring it is FedRAMP moderate or equivalent? You likely do. These are all examples of your organization assessing "the risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational."

What Does CMMC Explicitly Require?

CMMC wants you to perform **periodic risk assessments, meaning at least once per year.** If your organization does not have an existing risk assessment process, CMMC suggest organizations use NIST SP 800-30, Guide for Conducting Risk Assessments. You can also visit SP6's CMMC Resources page for a usable example on how to conduct a risk assessment, in alignment with NIST SP 800-30.

To make sure you're achieving the official risk assessment requirement, and joining the DIBCAC's positive statical trend, follow these steps:

1. Establish a policy communicating and providing guidance to perform risk assessments at least once per year.
2. Identify the Risk Methodology you will use, likely in alignment with NIST 800-30, following a qualitative model – keep this simple.
3. Identify the scope of the risk assessment (Organization Level, Function or business unit or manufacturing plant level, or even System Level e.g., think SSP or those systems that generate the goods and services that pay the bills.
4. Identify the common threats (bad actors) and non-adversarial (misconfiguration items, users' mistakes, vulnerabilities, etc.) with solutions like:
   – Vulnerability Scans
   – Penetration Testing
   – Breach and Attack Simulation (BAS)
   – Threat Intelligence
   – Etc...

5. Identify the risk with your subject matter experts by calculating #4 and using best judgement towards the relevance of the threat to the system (or identified scope of the risk assessment).
6. Document some basic assumptions about the environment and the threats and vulnerabilities.
7. Conduct the assessment and report the results.
8. Review the results and take action – specifically towards opportunities for improvement.
9. Update your risk assessment process and methodology as needed, then move to continuous monitoring and compliance.

5 CMMC Is a Business Problem and Potential Opportunity

A majority of organizations force CMMC to be "championed" within the IT department, often creating a snowball effect that spreads CUI into unnecessary, far-reaching places. As a result, CMMC implementation quickly loses steam after all of the technical requirements are implemented within the scope of the IT team. Safeguarding CUI requires a change in business processes and the education of users. Effective organizational change starts at the top with an informed workforce.

While Cybersecurity is at the core of CMMC, there are two aspects every organization needs to account for. The primary being CMMC helps organizations protect US Government sensitive data (CUI). Secondarily, failing to meet this safeguarding requirement is a business risk.

Contractors Are at the Forefront of CMMC

The business risk of failing to achieve CMMC is especially true if your organization generates more than 25 percent of its revenue from doing business with the DoD and other federal agencies. At that level of significance, your organization must continue to generate revenue through existing federal contracts. If your organization's strategy is to do more business with the DoD and federal government, CMMC is also a business risk and potential opportunity.

It's important to remember, organizations that have achieved full NIST SP 800-171, which is the existing regulatory standard, have established strong partnerships between business and technical leaders. Again, this stems from acknowledging that safeguarding CUI requires a change in business processes and the education of users. Effective organizational change starts at the top with an informed workforce.

6 Leverage Free Resources from Various Online Sources

The CISA (Cybersecurity and Infrastructure Security Agency), the NARA (National Archive and Records Administration), and the DoD (Department of Defense) are reliable organizations who offer free CMMC-related resources. From these websites, courses, and training materials, organizations can find information regarding a large expanse of topics from building a security program to running a tabletop exercise and more.

If you're not sure where to start, we've put together a few comprehensive resources that can lift organizations off the ground and start the process of defining, scoping, and mapping their CUI. While these aren't the end-all and be-all, they're a good place to start.

Cybersecurity Awareness and Training
(CUI Program Training and Awareness Products)

CUI TRAINING

- DoD CUI 101 – The lifecycle of CUI.
- DoD Mandatory CUI Training
  – Video/CBT: DoD Mandatory Controlled Unclassified Information (CUI) Training
- Insider Threat Awareness
  – Recognizing and Reporting Insider Threats
- CISA Tabletop Exercises

If you're past the point of mapping CUI, and further along in your CMMC compliance maturity, visit SP6.io/Resources for a comprehensive list of categorized resources pertaining to every stage of the certification process.

7 Partner with an Experienced RPO

Registered Provider Organizations (RPOs) offer consultation services to government contractors and other Organizations Seeking Certification (OSC) to prepare for CMMC assessments or assist during assessments if any issues are discovered. This partnership ensures your organization receives guidance and support throughout the certification process.

What Are the Benefits?

RPOs are specifically trained and authorized to provide pre-assessment consulting to help organizations have a clear understanding of the requirements and processes involved in achieving compliance. This support can potentially include: identifying areas of non-compliance, developing a plan of action to address them, and providing ongoing support throughout the certification process.

In addition, RPOs can assist during assessments in the event that any findings are uncovered, quickly and effectively resolve any issues, and eventually achieve compliance. Overall, working with an RPO can help organizations navigate the complex CMMC certification process and ensure they are fully prepared to meet the requirements and achieve certification.

SP6 Leverages 8+ Years of Compliance Expertise

As for a specific RPO that can assist your organization, SP6 is a reliable provider for CMMC advising. As an RPO, we leverage expertise in security, cyber risk, and compliance. Our professionals have worked on critical programs for the DoD throughout the last 18 years – with this experience and a passion for compliance and client success, our staff of RPs (Registered Practitioner) and CCPs (Certified CMMC Professionals) are more than happy to aid you.