# The OnShoreWave CMMC Readiness Framework

*A Hybrid Model for Achieving Affordable and Scalable Compliance*

The OnShoreWave CMMC Readiness Framework

*A Hybrid Model for Achieving Affordable and Scalable Compliance*

Prepared by David Haberland

OnShoreWave LLC

2025

OnShoreWave provides advisory services for public sector organizations and the companies that support them. This publication outlines a phased, hybrid approach to help micro and small businesses achieve CMMC readiness efficiently and sustainably.

www.OnShoreWave.com

## Table of Contents

## Executive Summary

The modern defense industrial base depends on thousands of small and micro businesses (generally under 100 employees). Many of these organizations lack dedicated cybersecurity staff, rely on lean IT budgets, and operate with tools and processes that have grown organically over time. As the Department of Defense strengthens its requirements for safeguarding information, these businesses face a growing challenge: cybersecurity is no longer optional. It is a prerequisite for winning and keeping federal contracts.

The Cybersecurity Maturity Model Certification (CMMC) establishes a unified standard for implementing security across the defense supply chain. It affects every organization that handles either Federal Contract Information or Controlled Unclassified Information (CUI). As contract language is updated, compliance becomes a condition of eligibility and participation. Businesses that cannot meet the standard will be removed from consideration no matter how strong their past performance or capabilities may be.

This white paper is written specifically for micro and small businesses that do not have the budget or staffing to pursue compliance with large scale enterprise programs. It recognizes the realities that these organizations face. Limited internal IT expertise. A need to control cost. The pressure to remain competitive. The desire to protect employees and customers while meeting federal expectations. The path to compliance must be practical, affordable, and achievable.

OnShoreWave proposes a hybrid and phased approach to CMMC readiness. This method blends automation, standardized templates, preconfigured enclaves, and targeted advisory support. It enables organizations to reach Level 1 compliance quickly and then progress toward Level 2 only when business needs require it. This structured progression lowers costs while allowing companies to scale their cybersecurity program as their contract profile evolves.

The hybrid model also reduces uncertainty by providing a clear roadmap for evidence collection, documentation, and system configuration. It gives organizations a predictable schedule for developing security controls and a repeatable process for maintaining them. The result is a program that is manageable, efficient, and aligned with the organization’s size, resources, and mission.

The organizations that succeed in the future defense marketplace will be those that understand these requirements early and develop a sustainable program. The purpose of this white paper is to provide the clarity, structure, and approach needed to become CMMC ready.

Figure 1: Modern Defense Supply Chain Landscape

These factors shape the environment in which small and micro businesses must operate. A clear understanding of the requirements and how they apply is essential before considering how to implement them. Section 2 introduces the structure of CMMC and the federal standards that underpin it.

## Understanding CMMC 2.0

Understanding the regulatory framework is the starting point for any compliance effort. This section explains how CMMC fits within existing federal requirements and how each certification level corresponds to the type of information a business handles.

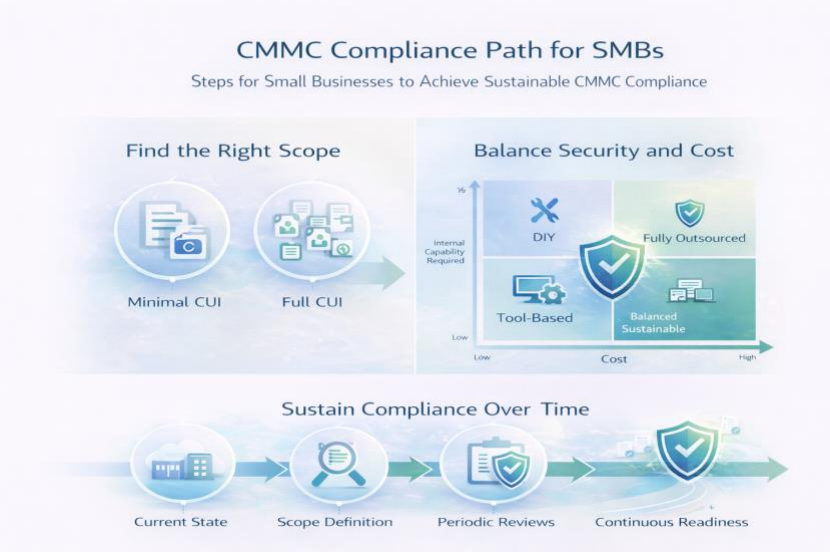

Figure 2: CMMC Compliance Path for Micro and Small Businesses

CMMC is the Department of Defense framework for improving the cybersecurity posture of companies that handle government information. It applies to organizations of all sizes that work within the defense supply chain. The model is built upon existing federal requirements including the Federal Acquisition Regulation safeguarding rules, DFARS clauses, and the security practices defined in NIST Special Publication 800-171.

CMMC establishes maturity levels that correspond to the sensitivity of data a contractor handles. Level 1 focuses on federal contract information and includes the basic security practices that all government contractors must follow. Level 2 includes the full set of NIST 800-171 requirements for protecting Controlled Unclassified Information (CUI). Level 3 applies to a smaller subset of companies performing critical or national security work and builds on the requirements from Level 2.

Understanding when each level applies is central to building a cost-effective compliance program. A company that handles only federal contract information often needs only Level 1. A company that handles Controlled Unclassified Information (CUI) must achieve Level 2. Some companies handle both types of information but can reduce their scope using a controlled enclave. This approach lowers cost and simplifies compliance by separating sensitive data from the rest of the organization’s systems.

CMMC 2.0 also introduces changes to the assessment process. Level 1 allows self-assessment. Level 2 requires a third-party assessment when required by contract for companies that handle certain categories of controlled information. All companies must submit their NIST 800-171 scores to the Supplier Performance Risk System. These scores are tied to contract eligibility and must be updated and maintained as part of the organization’s cybersecurity program.

A successful approach to CMMC begins with understanding not just the technical requirements but the regulatory and contractual context. Companies that understand the relationship between NIST 800-171, DFARS 252.204 7012, and the CMMC assessment process are better prepared to plan their compliance journey and avoid unnecessary cost.


Figure 3: CMMC Levels Overview


Figure 4: How Federal Requirements Fit Together

With the regulatory foundation established, the next step is to recognize the practical challenges that smaller organizations face when applying these requirements. Section 3 examines the realities that influence how micro and small businesses must approach compliance.

## Unique Challenges of Micro and Small Businesses

Compliance does not occur in a vacuum. It is shaped by the size, structure, staffing, and operational demands of the business. This section outlines why micro and small organizations require a different approach than larger enterprises.

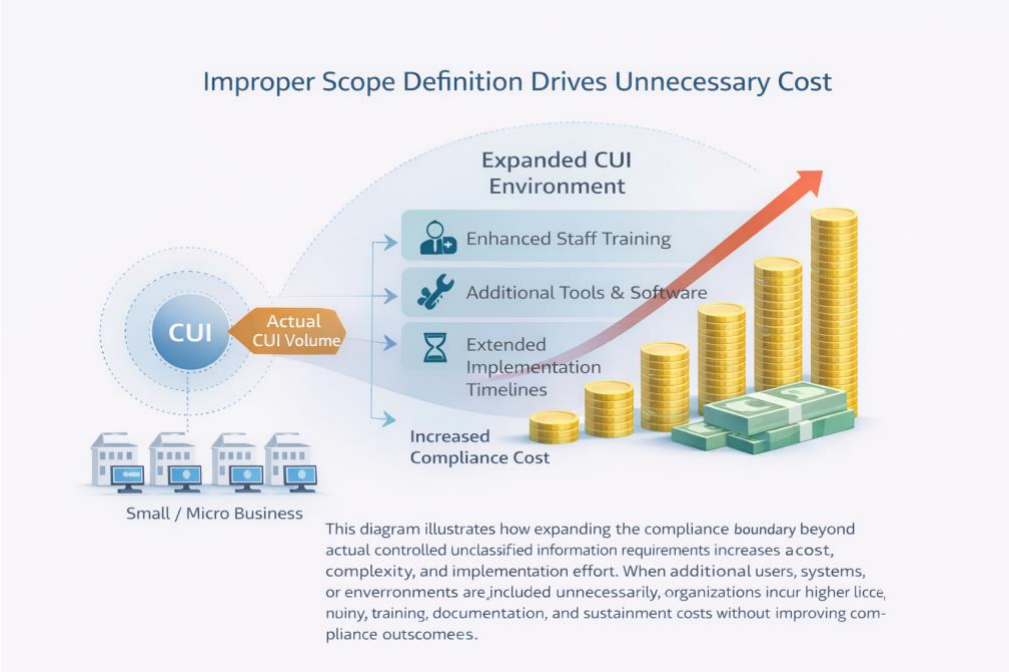


Figure 5: Improper Scope Definition Drives Unnecessary Cost

Micro and small businesses form the largest segment of contractors supporting the defense industrial base. These organizations bring specialized expertise, innovation, responsiveness, and strong mission alignment. Yet they face challenges in implementing CMMC that differ significantly from those encountered by larger companies. Understanding these challenges is essential for building a realistic and sustainable path toward compliance.

The most common challenge is staffing. Many small businesses operate with only one or two individuals responsible for all technology needs. These individuals are often generalists who support networking, email, hardware, software, and user support. Cybersecurity becomes an added responsibility rather than a dedicated function. When a regulatory framework such as CMMC introduces documentation requirements, evidence expectations, and system configuration obligations, the workload can quickly exceed available capacity.

Budget constraints add further pressure. Small businesses often avoid complex tools or enterprise configurations that require expensive licenses or long-term service commitments. Traditional managed service or managed security providers frequently charge fees that are out of reach for organizations with fewer than one hundred employees. As a result, these businesses require solutions that are appropriately scaled, predictable in cost, and maintainable without a specialized compliance team.

Small businesses also struggle with the volume and complexity of information associated with compliance. Terminology used in federal regulations may be unfamiliar, and technical control requirements can appear overwhelming. Many organizations attempt to identify a single product or tool that automatically delivers compliance. This leads to confusion and, in many cases,

unnecessary purchases. Compliance is not a tool. It is a combination of processes, people, technology, documentation, and consistent operational behavior.

Another challenge is maintaining daily business operations while implementing CMMC. Small organizations cannot afford prolonged downtime or disruptive system migrations. Employees often work remotely, access systems from multiple devices, or rely on cloud tools that have evolved organically over time. These real-world conditions must be incorporated into a compliance strategy that supports operations rather than disrupts them.

A final challenge is accurately defining the compliance boundary for controlled information. Many organizations mistakenly assume that all data they handle qualifies as Controlled Unclassified Information (CUI). This leads to an expanded compliance boundary that significantly increases cost, documentation effort, and operational burden without improving compliance outcomes. A careful review of contract requirements, data types, and information workflows is necessary to define an appropriate and defensible scope.

Small businesses need a compliance strategy that reflects these realities. They need clear direction, practical templates, simple automation, and a structured plan that can be executed incrementally. They also need the ability to elevate their level of compliance only when contract requirements demand it. A one-size-fits-all approach does not meet the needs of micro and small organizations.

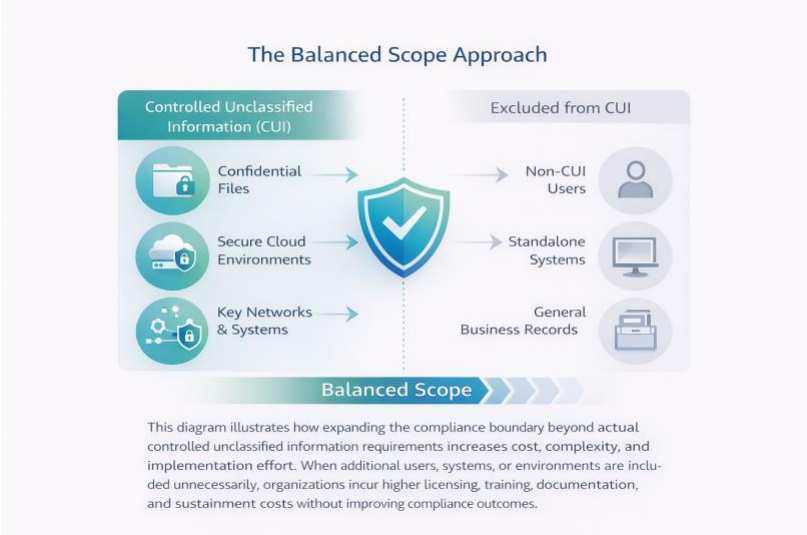

Figure 6: Balanced Scope Approach

These challenges demonstrate why smaller organizations need a structured and flexible approach to compliance. Section 4 introduces the hybrid model developed by OnShoreWave to address these needs in a practical and sustainable way.

## The OnShoreWave Hybrid Compliance Framework

A compliance strategy must be manageable, cost effective, and adaptable. The OnShoreWave hybrid framework provides these capabilities by combining phased implementation, standardized tools, and optional support tiers.

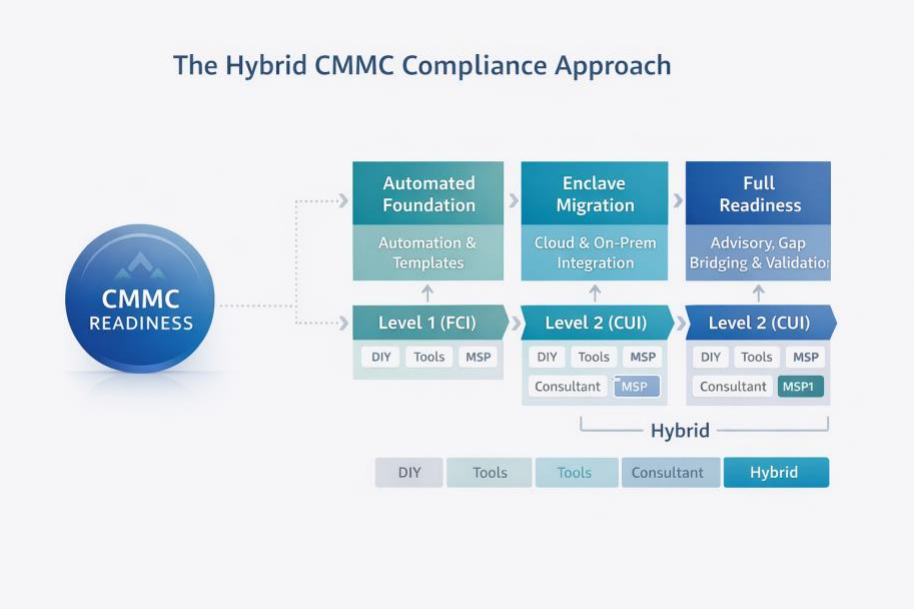


Figure 7: Hybrid CMMC Compliance Approach

A successful path to CMMC for micro and small businesses must be flexible, staged, and supported by both technology and guidance. The OnShoreWave hybrid compliance framework is designed around these principles. It reduces the cost and complexity of compliance while enabling organizations to adopt the technical and administrative controls needed to meet federal expectations.

The hybrid approach begins with establishing foundational safeguards aligned with CMMC Level 1. These foundational controls include basic access control, authentication, data protection, and documentation. This initial phase provides a structured cybersecurity baseline and prepares the organization for federal contract requirements without forcing immediate adoption of the full Level 2 practice set. It also builds confidence within the organization by demonstrating that compliance is achievable with the right structure.

The second element of the hybrid framework is a focus on automation and standardization. Rather than requiring every organization to build its own set of policies, procedures, and templates, OnShoreWave provides standardized artifacts and preconfigured technical settings that align with federal requirements. This reduces time to compliance and decreases the risk of inconsistencies between policy, practice, and evidence.

The framework also introduces three tiers of service options that align with different organizational needs. The first tier, which can be described as a light internal approach, provides templates, checklists, and guidance for organizations with some internal IT capability. The second tier provides a shared responsibility model in which OnShoreWave assists with system configuration, evidence collection, and periodic reviews. The third tier is a more comprehensive managed model for organizations that want the highest level of support. Each tier builds on the same core structure, enabling organizations to scale support as requirements increase.

To illustrate how different solutions, services, and internal responsibilities align across micro and small business environments, the following diagram shows how tools, external support, and internal effort work together within a hybrid compliance model.

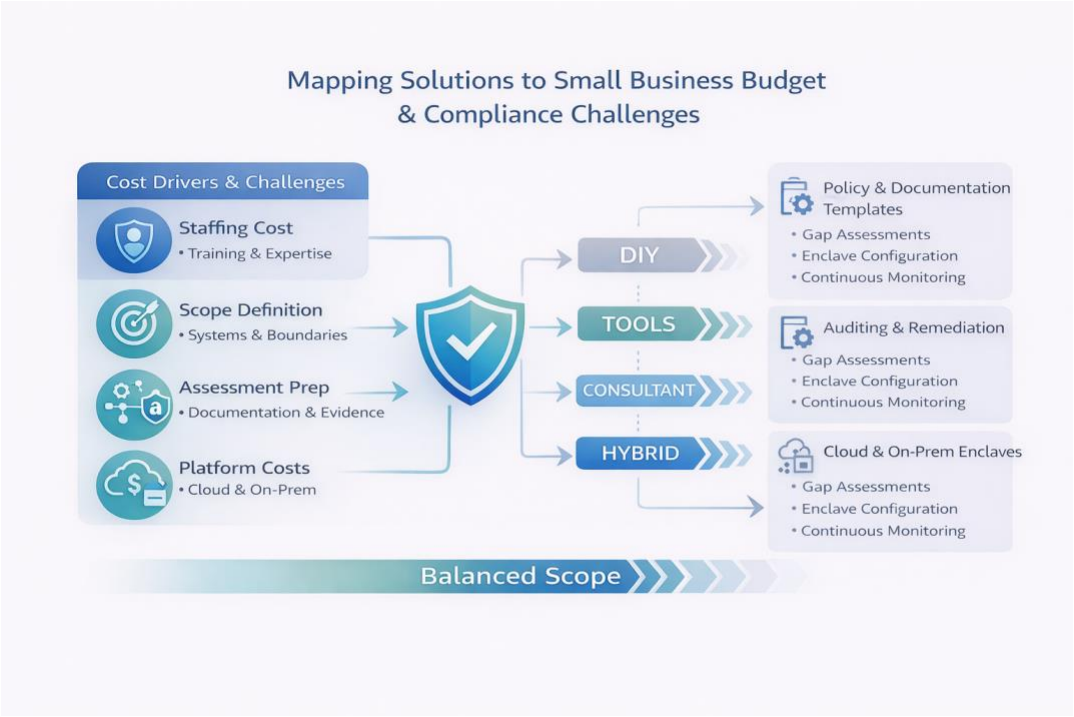


Figure 8: Mapping Solutions to Micro and Small Business

Another key component of the hybrid model is the concept of phasing. Instead of attempting to implement all 110 practices required for CMMC Level 2 at once, the organization adopts controls in stages. Level 1 controls are implemented first. Additional technical safeguards such as device management, logging, monitoring, and data loss prevention can be added gradually. When the organization wins work involving Controlled Unclassified Information (CUI), it can transition seamlessly to the full set of Level 2 controls without rework.

The hybrid framework also emphasizes reducing the scope of assessment when appropriate. For small organizations, isolating Controlled Unclassified Information (CUI) within a purpose built enclave simplifies compliance and reduces the number of systems that require documentation and evidence. This approach lowers cost, reduces audit complexity, and creates clear visibility into the systems that must meet specific requirements.

OnShoreWave's hybrid model is designed to be repeatable, scalable, and sustainable. It supports micro and small businesses that want to remain competitive in the defense marketplace without taking on unnecessary risk or expense. It replaces uncertainty with structure, and it transforms compliance from a one time project into an ongoing capability that grows with the organization.


Figure 9: The Hybrid Approach Capabilities and Benefits

With a strategic framework in place, the next consideration is understanding the specific technical controls that CMMC requires. Section 5 provides an overview of the control domains and why each is important for compliance.

## Technical Requirements of CMMC for Micro and Small Businesses

Technical controls form the backbone of CMMC. Although the terminology can appear complex, each domain serves a clear purpose in protecting information. This section introduces the key domains in accessible terms.

CMMC defines a series of technical and administrative safeguards that organizations must implement to protect federal contract information and Controlled Unclassified Information (CUI). For many small and micro businesses, these safeguards represent a new level of formality and control. While the requirements can appear complex, they become manageable when organized into clear categories and implemented gradually.

The following subsections summarize the core technical domains of CMMC that impact micro and small organizations. This overview provides a foundation for the deeper guidance that appears in later sections of the white paper and in the accompanying toolkit.

Access control is one of the most important requirements for all businesses. Access must be limited to individuals who need information to perform their duties. This includes the use of

multifactor authentication, limiting administrative privileges, eliminating shared accounts, and establishing processes for removing access when employment or job duties change. For small organizations, understanding who has access, why they have access, and how that access is managed is a central part of compliance.

Identification and authentication requirements govern how individuals log in and how credentials are protected. Strong passwords, the separation of administrative accounts, and consistent credential policies are essential. Many small companies allow users to operate with administrative privileges or rely on informal password practices. These behaviors conflict with CMMC expectations and must be replaced with standardized controls.

Audit and logging requirements ensure that activities within systems can be tracked. Logs must record actions that could affect security, such as login attempts, file access, changes to settings, or security events. Logs must also be protected from unauthorized alteration. Small businesses often rely on cloud provider defaults without understanding what events are captured or how long logs are retained. A simple plan for enabling logs, reviewing them periodically, and retaining them for the required period is necessary.

Configuration management includes establishing a standard configuration for devices and systems and documenting changes. This includes keeping operating systems and applications updated, removing unnecessary software, and tracking modifications. Small organizations frequently allow devices to be configured informally or differently across users. This inconsistency increases security risk and complicates compliance.

Incident response requirements introduce the need for a documented plan describing how the organization identifies, responds to, reports, and recovers from security incidents. Even small organizations must know who to contact, how to preserve evidence, and how to meet federal reporting timelines. Tabletop exercises and periodic plan reviews help ensure readiness.

System and communications protection focuses on securing the movement of information and protecting data through encryption. Information must be encrypted both when stored and when transmitted. Small organizations often assume encryption is automatic within cloud platforms, but they must verify that these protections meet federal expectations and document how they are configured.

System integrity includes safeguarding devices against malware, monitoring for unauthorized software, and applying patches in a timely manner. Automated tools can help ensure consistency, but even basic processes for ensuring updates and monitoring are essential for Level 1 and Level 2 readiness.

Documentation is the unifying requirement across all technical domains. Organizations must describe their policies, procedures, and configurations. They must also maintain evidence that demonstrates how those requirements are implemented. For small organizations, the creation of a System Security Plan (SSP), a Plan of Action and Milestones (POA&M), and an evidence binder provides structure and reduces confusion during audits.

Once the technical domain requirements are understood, organizations must evaluate the cloud platforms that support these controls. Section 6 provides guidance on selecting environments that meet federal expectations while remaining manageable for small businesses.

## Cloud Strategy and Platform Selection

Selecting the right cloud platform is one of the earliest and most important decisions in a compliance journey. The choice influences cost, complexity, and the organization's ability to produce evidence for an assessment.

Cloud platforms play a central role in CMMC compliance, especially for small and micro businesses that lack dedicated infrastructure. Choosing the right platform is one of the most important early decisions an organization will make. The platform influences cost, complexity, evidence requirements, and the ability to meet federal expectations for protecting Controlled Unclassified Information (CUI).

Federal requirements shape cloud selection. Systems handling controlled information must rely on platforms that meet specific security standards such as FedRAMP Moderate, FedRAMP High, or Department of Defense Impact Levels. These standards ensure that cloud providers meet baseline security expectations. Organizations must document which cloud services they use and verify that those services are authorized for their intended purpose.

Microsoft 365 is one of the most common platforms used by defense contractors. It includes environments such as Microsoft 365 Commercial, Microsoft 365 GCC Low, and Microsoft 365 GCC High. Each environment has different security and compliance capabilities. Small businesses that handle only federal contract information often remain in a commercial or GCC Low environment. Organizations that handle Controlled Unclassified Information (CUI) frequently need GCC High or a dedicated enclave. Understanding the distinctions helps align technical capabilities with contract obligations.

Google Workspace is another option, particularly for micro-organizations that prefer a simpler administrative model. When combined with Assured Workloads, Google offers configurations designed to support workloads that must meet certain federal security expectations. This approach may reduce complexity for very small organizations, although it may not meet all requirements for certain categories of controlled information. A careful review of contract language is necessary to determine whether Google Workspace is sufficient or whether a shift to Microsoft is required.

Amazon Web Services plays a more specialized role. AWS GovCloud provides capabilities for highly sensitive workloads, and some businesses choose hybrid models that combine Microsoft for productivity and AWS for infrastructure. This is more common in larger organizations but can apply to small businesses with specialized software or development environments.

Selecting a platform involves balancing several factors. Cost must be predictable and appropriate for the size of the organization. Administrative complexity must be manageable without an in

house security team. Evidence collection must be practical and supported by available features. Finally, the platform must align with future contract requirements to avoid costly migrations.

A structured decision model helps organizations identify their best fit. Micro organizations may prioritize administrative simplicity and cost efficiency. Small organizations may focus on audit readiness and evidence capabilities. Organizations pursuing or expecting controlled information contracts may evaluate enclave or GCC High options that reduce audit scope while meeting federal security expectations.

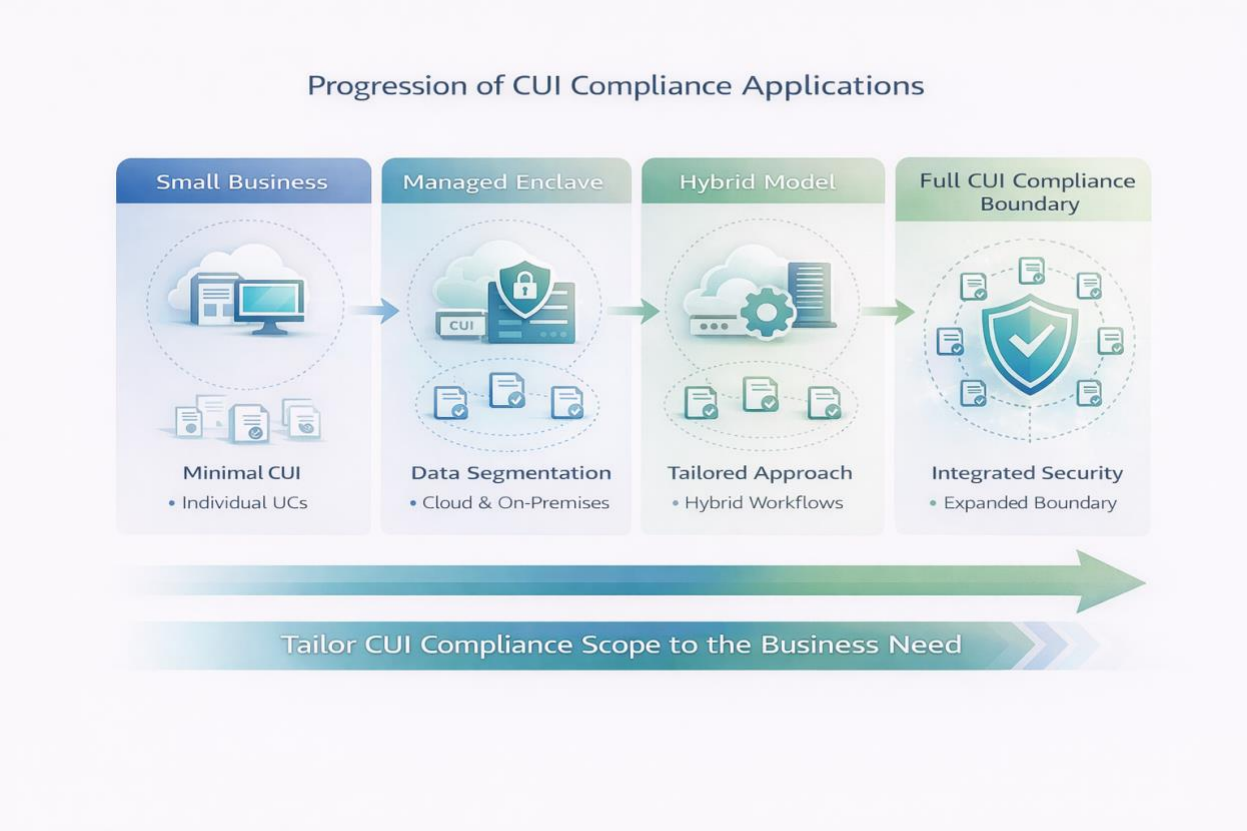


Figure 10: Progression of CUI Compliance

Platform selection naturally leads to planning how the organization will transition into an appropriate environment. Section 7 explains migration paths and the role of enclave architecture in simplifying compliance.

## Migration Paths and Enclave Architecture

A well-designed environment supports compliance and reduces assessment scope. Understanding migration options helps organizations adopt secure architectures without disrupting daily operations.

A core challenge for many micro and small businesses is determining how to transition from their current environment to one that satisfies CMMC requirements without disrupting day to day operations. The goal is to create a secure environment that protects controlled information while allowing the business to function efficiently. Enclave architecture plays an important role in achieving this balance.

An enclave is a dedicated, well-defined environment where controlled information is stored, processed, and accessed. By isolating this information from the rest of the organization's systems, the business reduces the number of devices, applications, and workflows that must meet the full set of security requirements. This approach is particularly attractive to small organizations because it lowers cost, simplifies evidence collection, and reduces the resources required during an assessment.

Migration into an enclave can be approached in several ways. The simplest scenario involves organizations that are already using cloud productivity platforms such as Microsoft 365 or Google Workspace. In these cases, the migration may involve creating a separate tenant or purpose-built configuration for handling controlled information. Users who require access to controlled information can be moved into the enclave environment while other users remain in a general operating environment with less restrictive settings.

Organizations using Google Workspace may migrate controlled information workflows into a Microsoft enclave when contract requirements dictate the use of GCC High or equivalent environments. This type of migration often involves separating file storage, email, device management, and identity controls so that only the users who handle controlled information are transitioned. This reduces the cost of licensing while maintaining appropriate security controls.

For organizations already using Microsoft 365 Commercial or GCC Low, the transition to a GCC High enclave may involve establishing a new tenant with the appropriate security boundary. The enclave becomes the location where controlled information is stored, and collaboration tools within that tenant are configured to meet federal expectations. Users can operate across both tenants depending on job responsibilities, provided identity and device controls are implemented in a consistent manner.

Some organizations may require a hybrid approach that combines cloud environments with dedicated infrastructure. This is more common among businesses that operate specialized software or engineering systems. In these cases, the enclave may be a combination of a cloud environment for collaboration and a secure infrastructure segment for technical workloads. The key principle remains the same: controlled information is handled only within the identified enclave.

A well-designed enclave architecture enables organizations to scale their compliance as contract requirements evolve. It also provides clarity during audit preparation by clearly defining what systems are in scope. This reduces uncertainty and helps ensure consistent configuration and documentation.

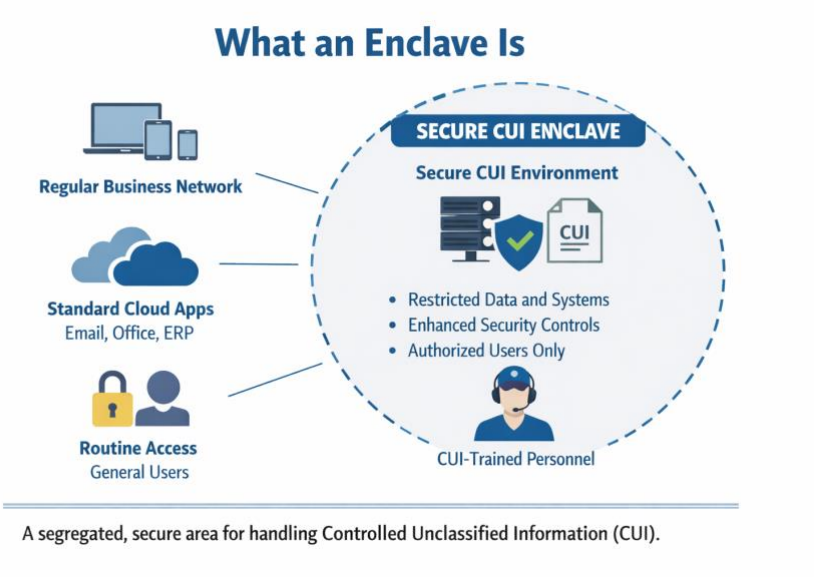


Figure 11: What an Enclave Is

With architectural options established, organizations can plan their compliance journey using a phased approach. Section 8 outlines a structured roadmap that enables steady progress toward readiness.

## The Phased Roadmap for CMMC Readiness

Compliance becomes more achievable when approached in manageable stages. This section provides a practical timeline for implementing controls and maturing documentation.


Figure 12: Building and Maintaining CMMC Compliance

CMMC compliance requires the implementation of specific controls, documentation, and technical safeguards. Attempting to complete all requirements at once can overwhelm small organizations and create unnecessary cost. A phased approach provides structure, predictability, and steady progress without disrupting operations. This section outlines a roadmap that organizations can use to move from basic readiness to full compliance.

The first phase focuses on establishing a Level 1 foundation and typically spans the first three months. During this phase, the organization adopts basic access control, authentication standards, password policies, and endpoint protections. Documentation is introduced through the creation of policies and the initial System Security Plan (SSP). Evidence collection begins in a simple, manageable form. This foundational work strengthens the security posture and prepares the organization for future requirements.

The second phase emphasizes the development of stronger security controls. Over the next several months, the organization introduces device management, structured logging, administrative account separation, periodic access reviews, and improved data protections. This period also includes maturing the System Security Plan (SSP) and beginning the development of a Plan of Action and Milestones (POA&M). These steps bridge the gap between Level 1 and Level 2 expectations.

The third phase prepares the organization for handling Controlled Unclassified Information (CUI) and typically spans a longer period. This phase includes establishing or migrating into an enclave, enabling advanced security settings, and implementing monitoring practices that satisfy the full NIST 800-171 controls. The organization refines incident response, formalizes backup and recovery procedures, and conducts rehearsals to validate readiness. Evidence processes become more structured, and the organization prepares for a third party assessment if required by contract.

The final phase focuses on ongoing compliance and continuous improvement. CMMC is not a one time event. Organizations must maintain access reviews, review logs, update documentation, and evaluate changes in the technical environment. Quarterly reviews ensure that policies remain aligned with daily operations and that evidence remains organized and current. This ongoing work supports audit readiness and preserves the organization’s eligibility for federal contracts.

The phased roadmap allows micro and small businesses to adopt CMMC at a manageable pace. Each phase builds on the previous one, reducing rework and avoiding the confusion that often arises when organizations attempt to implement requirements without a structured plan. The result is a clear and effective compliance journey that aligns with organizational size, resources, and mission.


Figure 13: Sustaining CMMC Compliance Over Time

A phased roadmap helps organizations understand what to do and when. The next step is selecting the level of support that aligns with internal capacity. Section 9 presents a decision model for choosing the appropriate hybrid tier.

## The Hybrid Decision Model for Clients

Organizations vary in their internal capabilities and resource availability. This section helps readers evaluate which support model best aligns with their needs.

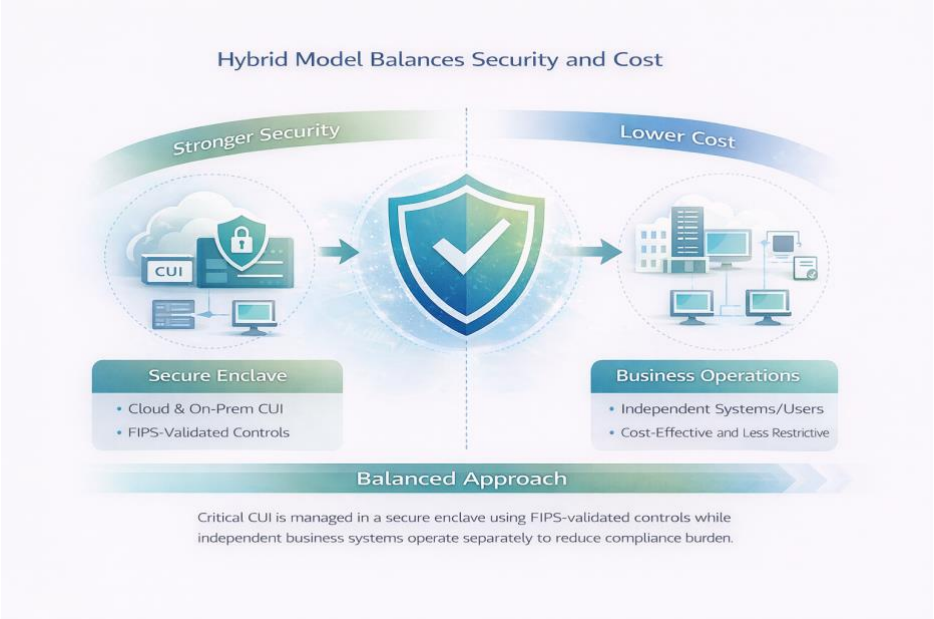


Figure 14: Hybrid Model Balance Security and Cost

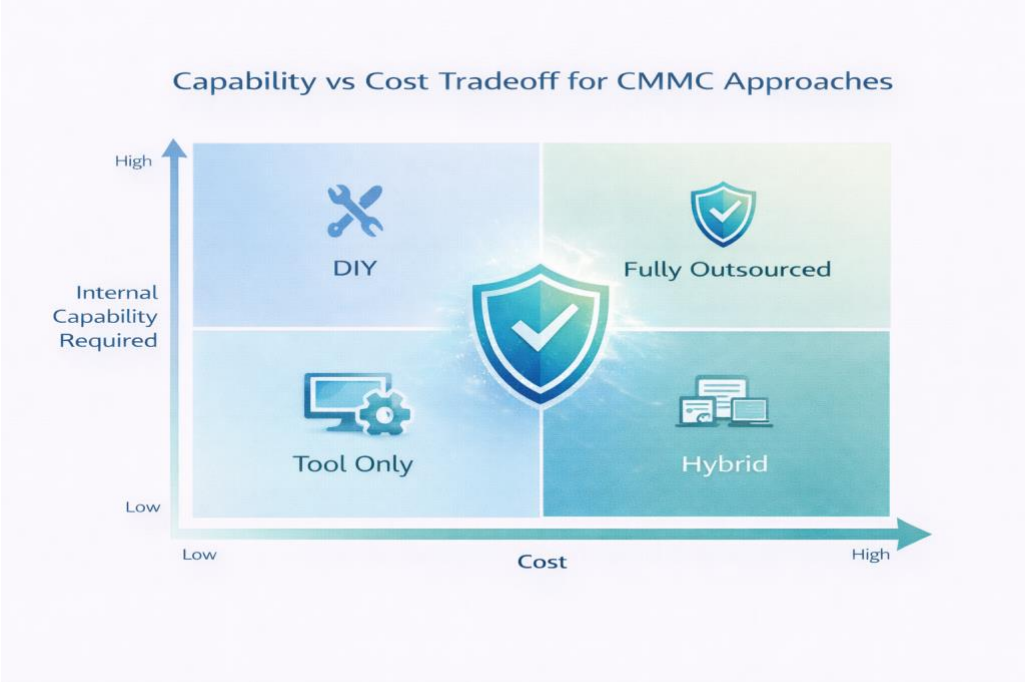


Figure 15: Capability vs Cost Tradeoff for CMMC Approaches

Selecting the right approach to CMMC compliance is not a one size fits all decision. Micro and small businesses differ widely in their contract profiles, staffing levels, technology environments, and financial capacity. A structured decision model helps organizations understand their options and choose a path that aligns with both operational needs and budget realities. The hybrid model offered by OnShoreWave provides flexibility while maintaining a consistent framework for progress.

An organization with some internal IT capability may be able to follow a light internal approach that relies on standardized templates, checklists, and periodic guidance. This approach is well suited for businesses where a staff member can dedicate part of their time to implementing controls, updating documentation, and coordinating with OnShoreWave as needed. It minimizes cost and allows the organization to build internal familiarity with compliance requirements.

Some businesses require more involvement due to limited staffing or more complex environments. In these situations, a shared responsibility model becomes a better fit. In this model, OnShoreWave supports the design of the technical environment, assists with configuration, reviews documentation, and helps organize evidence. The business maintains daily operations while relying on structured oversight to ensure controls are implemented correctly and consistently. This option provides balance by reducing internal workload without shifting full control to an external organization.

The third option is intended for organizations that prefer a more comprehensive level of support or have limited internal capability. In this model, OnShoreWave manages key aspects of configuration, evidence management, documentation updates, and periodic reviews. The organization focuses on daily mission activities while receiving guidance, monitoring, and

structure to maintain compliance. This approach is often appropriate for companies expecting to handle Controlled Unclassified Information (CUI) or preparing for third party assessments.

These three paths provide flexibility for different types of organizations, but the importance of choosing the correct approach cannot be overstated. A business that overestimates its capacity for internal work may struggle to meet deadlines, maintain documentation, or prepare evidence for audits. A business that invests in more support than it needs may face unnecessary costs. The hybrid decision model addresses these concerns by aligning needs, capacity, and resources into a clear pathway.

Organizations can evaluate their situation by considering factors such as the number of employees requiring access to controlled information, current IT staffing, technology maturity, contract requirements, and anticipated growth. The decision model is not static. As organizations expand or take on new contracts, they can move between tiers and increase or decrease support accordingly.

Selecting the right support model helps organizations plan budgets, resources, and timelines with confidence. Section 10 expands on these considerations with cost modeling and time to compliance.

## Cost Modeling, Return on Investment, and Time to Compliance

Budgeting and scheduling are central to managing compliance effectively. This section provides a realistic view of costs, timelines, and value.


Figure 16: Cost Drivers and Budget Pressure Points

Understanding the cost of compliance is essential for micro and small businesses that operate with limited budgets and tight resource constraints. While CMMC introduces new requirements, the financial impact can be manageable when approached methodically. The key is to structure the compliance journey in phases and select a level of support that aligns with the organization's operational needs.

Costs typically fall into several categories. Licensing expenses include cloud platform subscriptions, identity tools, device management solutions, and other basic capabilities. Technical implementation costs may include configuration work or assistance with setting up an enclave. Documentation and evidence management require time and potentially external support. Finally, organizations that must undergo third party assessments incur costs related to audit preparation and the assessment itself.

Micro organizations often require only a small number of licenses and minimal migration support. Their costs are concentrated in the configuration of foundational controls, the introduction of basic documentation, and periodic guidance. Because these organizations typically have fewer devices and simpler workflows, a phased approach allows them to achieve readiness at a reasonable cost while maintaining operational continuity.

Small businesses with more users or more complex workflows may incur higher costs, particularly when preparing for Level 2 certification. Device management, logging, access reviews, and enclave configurations may require more extensive work. However, by applying a phased roadmap and scoping controlled information appropriately, these businesses can avoid unnecessary expenses. Clear separation of environments and well planned migrations reduce complexity and prevent costly rework.

Return on investment becomes evident when organizations consider contract eligibility, competitive advantage, and reduced risk. CMMC is increasingly required for participation in defense contracts. Organizations that achieve compliance strengthen their position within the industrial base and increase their ability to win future work. Compliance also reduces the likelihood of security incidents, which carry both financial and reputational costs.

Time to compliance varies based on the maturity of the organization and the level of support selected. Micro organizations with well organized cloud environments can often reach Level 1 readiness within three months. Businesses transitioning to Level 2 readiness may require additional time for enclave configuration, documentation maturity, and internal process development. The structured roadmap described earlier in this paper ensures predictable progress and helps organizations anticipate future milestones.

The most important financial consideration is the avoidance of rushed or reactive compliance efforts. Businesses that plan early, adopt phased improvements, and select appropriate support options minimize long term costs. CMMC becomes not just a federal requirement but an investment in operational resilience and competitiveness.


Figure 17: Year One versus Sustainment

Understanding cost and investment prepares organizations to evaluate consulting partners and strategic options. Section 11 describes how OnShoreWave delivers a practical and scalable approach tailored to small and micro businesses.

## The OnShoreWave Advantage

A successful compliance journey often requires both guidance and structure. This section highlights the unique value that OnShoreWave provides to help organizations meet CMMC requirements confidently.

Micro and small businesses need an approach to CMMC that is realistic, structured, and aligned with their resources. Many organizations struggle because they attempt to navigate complex federal requirements without the guidance or support necessary to make informed decisions. OnShoreWave's hybrid model addresses this gap by combining practical experience, public sector expertise, and a deep understanding of the needs of smaller organizations.

OnShoreWave offers a framework that simplifies compliance without diminishing the rigor required to meet federal expectations. The phased approach allows organizations to begin with the foundational controls of Level 1 and grow steadily toward Level 2 only when contract requirements demand it. This prevents unnecessary investment while ensuring that each step is aligned with documented guidance and technical standards.

Another advantage of the OnShoreWave approach is the focus on templates, evidence structure, policy clarity, and repeatable processes. Documentation plays a central role in CMMC, and many

businesses find it difficult to translate technical requirements into understandable and actionable language. OnShoreWave provides structured documents that help organizations implement, track, and verify controls in a consistent manner.

The hybrid support tiers allow organizations to select the level of involvement that matches their internal capability. Companies with some IT capacity can leverage guidance and tools to manage most of the work internally. Others may rely more heavily on shared responsibility or comprehensive support to ensure proper configuration and documentation. This flexibility reduces friction and ensures that each organization receives the right level of assistance.

OnShoreWave also emphasizes the importance of scoping controlled information effectively. By helping organizations determine what data is considered controlled, where it lives, and who needs access to it, the overall compliance footprint is reduced. This leads to lower implementation costs, simpler documentation, and clearer audit boundaries.

The overarching goal of OnShoreWave's method is to transform CMMC from an obstacle into a predictable and manageable capability. By providing structured guidance, practical tools, and a clear roadmap, OnShoreWave enables micro and small businesses to strengthen their security posture and maintain eligibility for federal contracts with confidence.


Figure 18: End to End CMMC Readiness Journey for Small Businesses

# Appendices

CMMC readiness is attainable when organizations follow a structured, phased, and well supported approach. By combining technical controls, operational discipline, and clear documentation, micro and small businesses can meet federal expectations while strengthening their overall security posture. The following appendices provide reference material, definitions, and resources that support the guidance presented in this white paper.

## Appendix A - Official References

This appendix contains a curated collection of authoritative links from the Department of Defense, NIST, and related agencies. These links provide the formal basis for CMMC and support the guidance offered in this white paper.

Department of Defense CMMC Overview
https://dodcio.defense.gov/CMMC/About

CMMC Assessment Guides
https://dodcio.defense.gov/CMMC/Assessment-Guide

NIST Special Publication 800-171
https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

DFARS 252 dot 204 dash 7012
https://www.acquisition.gov/dfars/252.204.7012

Cyber AB Marketplace
https://portal.cyberab.org/marketplace

## Appendix B - Glossary of Terms

Organizations that are new to CMMC often encounter terminology that may be unfamiliar. This glossary provides definitions of commonly used terms within the context of CMMC and federal cybersecurity requirements. It is intended to help organizations that may be unfamiliar with regulatory terminology.

Federal contract information
Information provided by or generated for the government under a contract that is not intended for public release.

Controlled Unclassified Information (CUI)
Information that requires safeguarding or dissemination controls according to law, regulation, or government policy but is not classified.

System Security Plan (SSP)
A document describing the security environment, system architecture, responsibilities, and the implementation status of required controls.

Plan of Action and Milestones (POA&M)
A document that identifies gaps between required and implemented controls and provides a plan for addressing them, including timelines and responsibilities.

Assessment guide
A document published by the Department of Defense that explains how each CMMC requirement is evaluated and what evidence must be provided.

Enclave
A defined environment where sensitive information is stored or processed, allowing organizations to limit the systems that fall within the scope of a security assessment.

Identity and access management
The processes and technologies used to ensure that only authorized individuals can access systems, applications, and data.

Configuration baseline
A defined and approved set of system configurations that establish a secure operating state across devices or systems.

Security control
A safeguard or protection measure required to meet federal expectations for the protection of information.

Evidence
Documentation, screenshots, logs, and other materials that demonstrate a security requirement has been implemented and is functioning as expected.

Multifactor authentication
A login method requiring more than one form of verification, typically a password combined with a code or authentication prompt.

Impact level
A categorization used by the Department of Defense to describe the sensitivity of information stored or processed in a cloud environment.

## Appendix C - Controlled Unclassified Information (CUI) Categories

This appendix summarizes the structure of Department of Defense Controlled Unclassified Information (CUI) categories. It is intended to help organizations correctly identify which information qualifies as controlled and ensure that compliance efforts are aligned with actual contractual and regulatory requirements. By clearly distinguishing controlled information from non-controlled data, organizations can define an appropriate compliance boundary and avoid unnecessary cost, complexity, and operational burden.

Controlled Unclassified Information (CUI) includes information that is not classified but must be protected according to federal policy. Understanding what qualifies as controlled information helps organizations define the appropriate scope for their compliance programs.

The Department of Defense maintains a registry of controlled information categories, organized into groups such as critical infrastructure, export control, financial information, intelligence sources or methods, law enforcement information, defense operations, personnel information, proprietary information, and privacy information.

- Examples of information that may be considered controlled include
- Technical drawings
- Engineering data
- Weapon system specifications
- Sensitive contract requirements
- Detailed performance reports
- Medical or personnel records protected under privacy rules
- Export controlled data subject to the International Traffic in Arms Regulations

Organizations should review their contracts and the DoD CUI Registry to determine which categories apply to them.

A link to the DoD CUI Registry is provided for reference
https://www.dodcui.mil/Home/DoD-CUI-Registry

## Appendix D - SPRS Scoring Overview

This appendix describes the scoring model used for reporting NIST 800-171 assessment results to the Supplier Performance Risk System. It provides a simplified explanation of scoring calculations, common deductions, and how organizations should approach self-assessment.

The Supplier Performance Risk System is used to track self-assessment scores for NIST Special Publication 800-171. Contractors must calculate their score according to the Department of Defense assessment methodology and submit it to the system before work can begin on many contracts.

The scoring model contains 110 security requirements. Each unmet requirement deducts a specific number of points. The highest possible score is 110, and the lowest is negative 203. Organizations begin at 110 and subtract points for each unimplemented requirement according to the weighting described in the assessment methodology.

A typical example
Failure to implement multifactor authentication results in a five-point deduction.
Failure to restrict administrative privileges may result in a three-point deduction.
Failure to encrypt information when transmitted results in a four-point deduction.

Organizations must maintain documentation to justify their score. If a requirement has not been fully implemented, the organization must describe the deficiency and the planned remediation activities in a Plan of Action and Milestones (POA&M).

SPRS scores are considered sensitive contract information. They must be updated when significant progress has been made toward remediation or when required by contract renewal.

Submitting an accurate and well documented score reduces risk during a future third party assessment and provides contracting officers with visibility into an organization’s cybersecurity posture.

Organizations should retain their scoring worksheet and supporting evidence for at least three years to support future reviews.

## Appendix E - Sample Evidence Items

This appendix provides examples of the types of evidence organizations may need to collect as part of a CMMC readiness effort. Examples include access control lists, screenshots of settings, configuration exports, policy documents, audit logs, and incident response test records.

Evidence is used to demonstrate that a requirement has been implemented. It must be clear, organized, and readily accessible during an assessment. The following examples represent common types of evidence small and micro businesses should prepare.

Access control lists showing which users have access to specific systems
Screenshots demonstrating multifactor authentication configuration
User account inventories showing separation between standard and administrative accounts
Device management configuration screens showing baseline security settings
Exported logs showing successful and failed login attempts
Records of access reviews and the removal of inactive accounts
Backups of configuration files showing encryption settings
Policy documents describing how the organization manages passwords, incidents, or changes
Incident response test records documenting tabletop exercises
Training records showing that users have been briefed on cybersecurity responsibilities
System Security Plan (SSP) updates showing implemented and planned controls
Plan of Action and Milestones (POA&M) entries showing remediation steps and timelines

Screenshots of encryption-in-transit settings for email and file storage.
This helps SMBs understand that encryption evidence is more than just “it exists.”

Evidence should be stored in a structured binder either digitally or physically. Each item should be labeled clearly and linked to the control it satisfies. This approach simplifies audits and helps organizations maintain readiness over time.

## Appendix F - Checklist Index

This appendix provides a concise index linking each section of the white paper to the corresponding tools found in the OnShoreWave CMMC Toolkit. It helps organizations understand which checklist or template should be used at each stage of the compliance journey.

Section 2
Requirements summary checklist
Determines whether the organization must meet Level 1 or Level 2 requirements.

Section 3
Organizational readiness assessment
Evaluates staffing, budget, and operational constraints prior to beginning compliance work.

Section 4
Hybrid model selection guide
Assists with selecting the appropriate support tier.

Section 5
Technical controls checklist
Provides practical items for access control, identification, logging, configuration, and other technical domains.

Section 6
Cloud platform decision matrix
Supports platform selection for compliance.

Section 7
Migration and enclave planning workbook
Outlines tasks, data flows, and system boundaries for enclave creation.

Section 8
Phased roadmap implementation checklist
Lists activities required for each phase of the compliance journey.

Section 9
Support tier evaluation worksheet
Helps match organizational capacity with appropriate service levels.

Section 10
Cost model estimator
Provides a structure for estimating initial and ongoing compliance costs.

Section 11
Engagement readiness checklist
Prepares organizations for working with OnShoreWave toward implementation or sustainment.

OnShoreWave provides advisory services for public sector organizations and the companies that support them. The firm focuses on practical readiness frameworks, cybersecurity preparedness, operational assessment, and strategic planning. Through a structured hybrid approach, OnShoreWave helps micro and small businesses achieve cybersecurity maturity, meet federal expectations, and maintain competitiveness within the defense industrial base.

This publication presents a phased model and practical toolkit designed specifically for organizations pursuing Cybersecurity Maturity Model Certification (CMMC) readiness in a cost effective and sustainable way.


Contact
OnShoreWave LLC
www.onshorewave.com