The Executive Brief

for

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

The Brief is located on OnShoreWave Website

OnShoreWave CMMC Readiness Framework

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

Executive Overview

CMMC compliance now directly determines whether a company can bid on, win, and retain Department of Defense contracts. For organizations supporting the defense industrial base, cybersecurity is no longer a future consideration. It is an operational requirement tied to eligibility, revenue continuity, and long-term competitiveness.

The Cybersecurity Maturity Model Certification framework applies across the supply chain, but its impact is felt most acutely by micro and small businesses (generally under 100 employees). These organizations often approach CMMC with limited internal resources, constrained budgets, and incomplete information. The result is frequently unnecessary cost, operational disruption, and delayed readiness.

This executive brief presents a practical, right sized approach to CMMC compliance designed specifically for micro and small businesses. It is based on real world implementation experience and emphasizes sustainability, clarity, and disciplined scope definition. The objective is not only to achieve compliance, but to do so in a way that can be maintained over time without overwhelming the organization.

This brief is intended for owners, executives, and senior leaders of micro and small businesses supporting the defense industrial base who must meet CMMC requirements without enterprise level staffing or budgets.

The Challenge Facing Micro and Small Businesses

Micro and small businesses represent the largest segment of contractors supporting the Department of Defense. They deliver specialized capabilities, agility, and innovation, yet they face unique challenges when implementing CMMC.

Staffing is the most common constraint. Many organizations rely on one or two generalists to manage all information technology responsibilities. Cybersecurity and compliance are often added on top of existing duties rather than supported by dedicated teams. When CMMC introduces documentation requirements, evidence collection, and formalized security controls, the workload can quickly exceed available capacity.

Budget limitations further complicate compliance efforts. Enterprise security tools and fully outsourced managed services are frequently priced beyond what smaller organizations can sustain. At the same time, attempts to minimize cost by relying solely on tools or internal effort often result in incomplete implementations or failed assessments.

Scope definition is another major challenge. Many organizations mistakenly assume that all systems, users, or data must be included within the compliance boundary. This expands the environment unnecessarily and drives higher licensing costs, greater complexity, and ongoing operational burden without improving compliance outcomes. Improper scope definition is the

single most common reason small businesses overspend on CMMC without improving audit results.

Finally, micro and small businesses must maintain daily operations while implementing CMMC. Extended downtime, disruptive migrations, or wholesale system changes are rarely feasible. A compliance strategy that does not align with real operating conditions is unlikely to succeed.

Understanding the CMMC Landscape

CMMC requirements are rooted in federal law, regulation, and established security standards. At a high level, requirements flow from the Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement through NIST Special Publication 800-171 and into CMMC certification and reporting through the Supplier Performance Risk System.

For most micro and small businesses, the primary focus is on CMMC Level 1 or Level 2. Level 1 emphasizes basic safeguarding practices for federal contract information. Level 2 introduces more comprehensive requirements for protecting controlled unclassified information and requires third party assessment when required by contract.

While the framework itself is consistent across organizations, its implementation must be scaled appropriately. Applying enterprise level solutions to small environments often introduces unnecessary friction, cost, and administrative overhead without improving compliance posture.

The Hybrid Compliance Model

For most micro and small businesses, neither a fully internal nor a fully outsourced compliance approach is sustainable. A hybrid compliance model provides the most predictable and manageable path to CMMC readiness and long-term sustainment.

Under a hybrid model, organizations retain ownership of their systems, data, and business decisions while leveraging structured guidance, standardized templates, automation, and targeted expert support where it adds the most value. Responsibilities are clearly defined, and implementation is phased to align with internal capacity and contract requirements.

Key characteristics of a hybrid approach include accurate scope definition so that only systems and users handling controlled information are included, phased implementation that prioritizes foundational controls before expanding scope, standardized documentation and evidence structures that reduce ongoing effort, and flexibility to increase or decrease external support as requirements evolve.

This approach reduces cost volatility, minimizes disruption, and supports sustainable compliance rather than one time certification efforts.

Managing Scope and Cost Effectively

Scope definition is the primary driver of CMMC cost and complexity. Expanding the compliance boundary beyond actual requirements increases licensing costs, documentation effort, training demands, and audit complexity. A disciplined review of contracts, data flows, and workflows allows organizations to focus compliance efforts only where required.

Cost modeling should distinguish between initial implementation and ongoing sustainment. While there is an upfront effort to establish controls and documentation, the long-term cost of compliance is driven by how efficiently those controls are maintained over time. Predictable, right sized sustainment is often more important than minimizing initial spend.

Organizations that adopt a hybrid approach are better positioned to balance cost and capability. They avoid the extremes of high-cost outsourcing and high burden internal execution, resulting in a more stable and defensible compliance posture.

Sustaining Compliance Over Time

CMMC compliance is not a one-time event. It is an ongoing operational commitment. Controls must be monitored, documentation maintained, and evidence collected consistently. Personnel changes, system updates, and new contracts all require periodic reassessment of the compliance environment.

Successful organizations assign clear ownership for compliance sustainment and treat CMMC activities as part of normal operating rhythm rather than as a special project. Repeatable processes, structured reviews, and practical tooling enable organizations to maintain readiness without excessive manual effort.

By incorporating sustainment into the compliance strategy from the beginning, organizations reduce risk, improve resilience, and maintain eligibility for future contracts.

Key Takeaways for Decision Makers

CMMC compliance is achievable for micro and small businesses when approached with discipline and realism.

- Accurate scope definition is critical to controlling cost and complexity.
- A hybrid compliance model offers the best balance of cost, capability, and sustainability.
- Compliance should be phased, structured, and aligned with actual contract requirements.
- Long term success depends on sustainment, not just certification.

About This Brief

This executive brief is derived from *The OnShoreWave CMMC Readiness Framework for Micro and Small Businesses*. It reflects practical experience supporting organizations across the defense industrial base and is intended to provide clarity, direction, and confidence to decision makers navigating CMMC requirements.

Organizations preparing for upcoming contracts, assessments, or SPRS updates should evaluate their current scope, platform readiness, and sustainment approach before committing to tooling, migrations, or assessments.

OnShoreWave LLC
www.onshorewave.com

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.

The Brief is located on OnShoreWave Website

OnShoreWave CMMC Readiness Framework