EXOSTAR

Surviving CMMC

8 Essential Takeaways SMBs Can’t Afford to Miss

TAKEAWAY ONE

If your organization handles Federal Contract Information (FCI)—basic non-public data needed to perform a government contract—or Controlled Unclassified Information (CUI)—more sensitive data that requires extra protection—CMMC compliance is required to win or renew defense contracts.

WHAT IS CMMC?

CMMC is a set of cybersecurity rules that make sure companies working with the government properly protect sensitive information.

Why Do You Need This Guide?

Small businesses keep the Defense Industrial Base (DIB) running. You deliver the components and services that primes depend on. This critical role also makes SMBs increasingly attractive targets for cyber adversaries. With CMMC 2.0 now being incorporated into defense contracts, compliance is nonnegotiable. It is becoming a condition for award, and many primes are already expecting suppliers to demonstrate readiness.

This guide breaks CMMC 2.0 into simple, actionable takeaways that help you understand what's required, how to prepare, and how to protect your contracts, without overwhelming your team or your budget.

TAKEAWAY TWO

CMMC readiness can be a competitive advantage as noncompliant suppliers will fall out of the supply chain.

WHAT IS CUI?

Controlled Unclassified Information is sensitive government information that isn't classified but still must be protected from unauthorized access.

CMMC 2.0 Simplified

CMMC 2.0 is the governments cybersecurity framework for protecting sensitive information across the Defense Industrial Base. It standardizes requirements and makes cybersecurity a shared responsibility for every contractor and subcontractor.

Unified Standard *Strengthens cybersecurity across all tiers of the DIB.*

Mandatory *Applies to primes and subcontractors; some require assessments.*

Security Baseline *Protects FCI and CUI at every level on the supply chain.*

Why SMBs Are Hit the Hardest

Attackers target SMBs because they often lack the resources of larger primes. CMMC ensures small businesses aren't the weak link in the chain.

National Security Risk *CUI (examples include: technical data, drawings, or specifications) is a target. Breaches threaten national security.*

Downstream Pressure *Primes demand compliance; noncompliant subs risk being replaced.*

Business Survival *Noncompliance means lost contracts and revenue.*

TAKEAWAY THREE

Knowing your correct CMMC level depends on the DFARS clauses in your contracts.

ASK YOUR PRIME:

Find out which CMMC level applies to you. Ask your prime or contracting officer which level applies to you.

TAKE THE QUIZ:

Find out which CMMC level applies to you.

Know Your CMMC Level

Good news: While there are three CMMC maturity levels, most small businesses only need to focus on Levels 1 or 2. Knowing where you fit saves time, money, and effort on your compliance journey.

CMMC Level 1 Protecting FCI	CMMC Level 2 Protecting CUI
17 Controls	110 Controls
Annual Self-Assessment	Self & C3PAO Assessments
Federal Contract Info	Controlled Unclassified Information
No POA&Ms	POA&Ms Allowed (Close in 180 Days)
Example Practices:	**Example Practices:**
• Secure Wireless Access • Limit User Access • Malware Protection • Physical Access Control • Media Sanitization	• Access Control • Encryption • System Monitoring • Logging • Documented SSP Evidence

TAKEAWAY FOUR

CMMC Level 2 requires full compliance with all 110 NIST SP 800-171 controls.

For organizations handling CUI, partial compliance is no longer acceptable. Even a small number of unmet controls can result in a failed assessment, despite being "mostly compliant."

WHAT IS NIST SP 800-171?

NIST SP 800-171 is a set of cybersecurity guidelines that explain how organizations should protect CUI.

From Barriers to Breakthroughs

Compliance is challenging, but every barrier has a solution.

LIMITED RESOURCES

Tight budgets and small IT teams make CMMC feel overwhelming.

SOLUTION

Use managed security services and automation to scale protection without adding headcount.

CONFUSING REQUIREMENTS

NIST SP 800-171 and CMMC controls are complex and easy to misinterpret.

SOLUTION

Leverage expert guidance, proven templates, and structured training to reduce risk and rework.

HEAVY DOCUMENTATION BURDEN

Manual, time-consuming documentation and evidence.

SOLUTION

Adopt compliance platforms that centralize documentation and automate evidence tracking.

TAKEAWAY FIVE

CMMC Level 2 compliance depends not only on your internal controls, but also on the vendors and third parties that can access CUI. Understanding your scope means knowing who touches CUI and ensuring every in-scope partner meets CMMC requirements.

WHAT IS SCOPE?

Scope defines which systems, users, and connections must meet CMMC requirements because they can access CUI. It sets the boundary for compliance, cost, and assessment impact.

Knowing Your Scope Matters

Most CMMC failures occur due to poor scoping, when organizations either include too many systems or miss systems that touch CUI. Clear scope reduces cost, risk, and complexity while speeding compliance. Use this simple path to define your CMMC scope:

Where is CUI?

Identify where controlled data is created, stored, processed, or transmitted (for example: technical data, drawings, and contracts).

Who touches it?

List all users, roles, vendors, and third parties with access to CUI.

What systems are involved?

Document email, endpoints, cloud apps, file storage, backups, and identity systems that handle or protect CUI.

What's connected?

Map integrations, remote access paths, and data flows into and out of in-scope systems.

What's in scope?

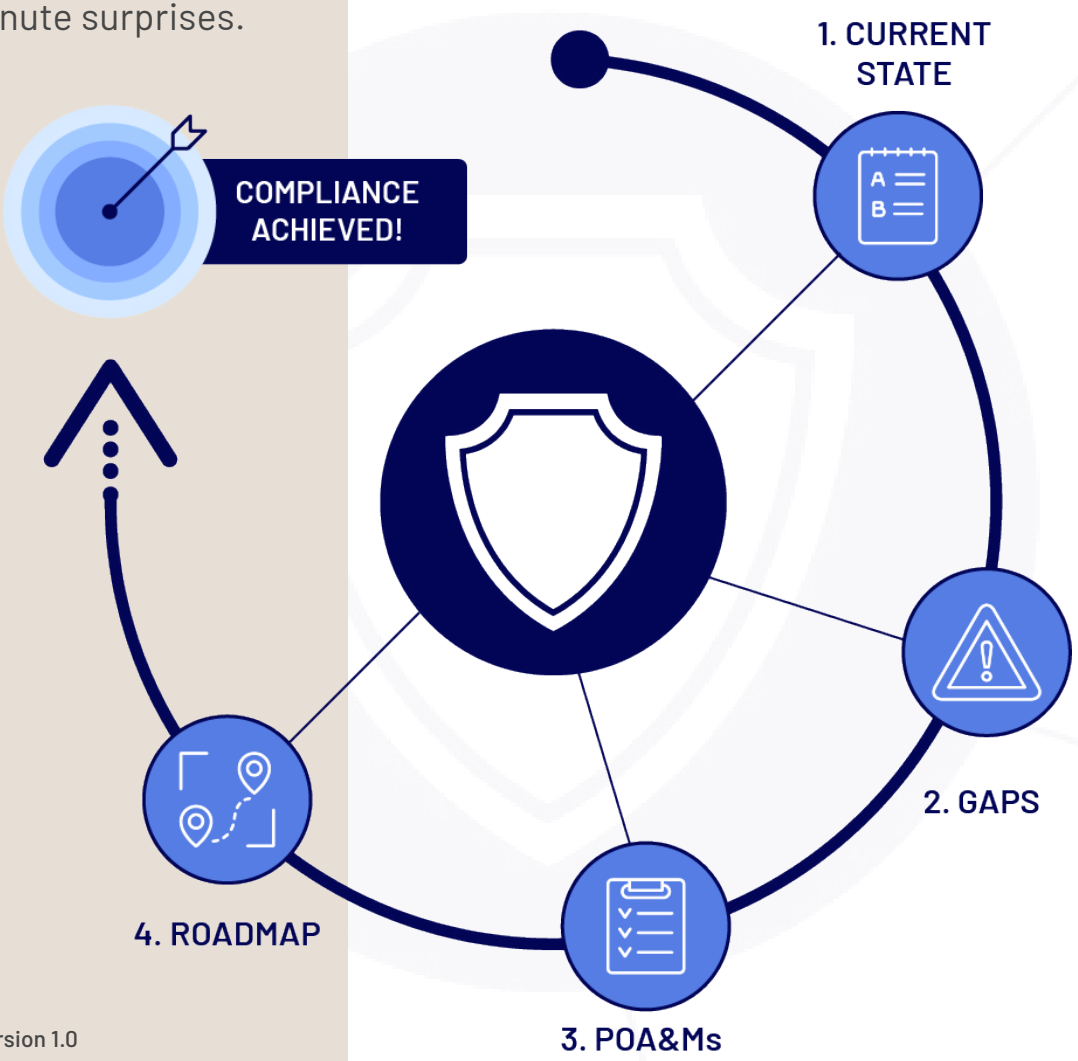
Clearly define what is and is not in scope to control cost, complexity, and assessment risk.

TAKEAWAY SIX

Most organizations overestimate their readiness. A gap analysis creates clarity, reduces wasted spend, and helps avoid failed assessments and last-minute surprises.

Conducting a Gap Analysis

A gap analysis shows how your current security practices compare to CMMC requirements and highlights what must be addressed to achieve compliance. It provides a realistic view of your readiness, helps prioritize effort and budget, and prevents surprises during an assessment.



1. **Current State**
   Document existing controls and security practices.
2. **Identify Gaps**
   Compare controls to CMMC requirements and note what's missing.
3. **POA&Ms**
   Track unresolved gaps with actions, owners, and timelines.
4. **Roadmap**
   Prioritize remediation based on risk and deadlines.
5. **Compliance Achieved**
   Validate controls, finalize evidence, and confirm CMMC readiness.

TAKEAWAY SEVEN

CMMC compliance protects sensitive data, reduces cyber risk, and keeps your business eligible for defense contracts.

SMBs that prepare early lower costs, avoid assessment failures, and gain a competitive advantage.

WHO CMMC APPLIES TO

CMMC applies to any company in the defense supply chain that handles FCI or CUI, including primes, subcontractors, and small businesses.

The Benefits of Being CMMC Compliant

Win More Contracts

Certified SMBs stand out as low-risk partners, opening the door to more and bigger opportunities.

Reduce Cyber Risk

Compliance practices actively reduce risks from ransomware, phishing, and insider threats.

Earn Trust with Primes

Demonstrates commitment to security, leading to smoother onboarding and stronger relationships.

Build Long-Term Resilience

Embedding compliance creates a scalable framework that adapts to evolving defense requirements.

TAKEAWAY EIGHT

Maintaining compliance with 110 CMMC controls requires ongoing monitoring and documentation—not a one-time effort.

The right solution reduces risk, lowers long-term costs, and helps keep your business assessment-ready over time.

GET CMMC ASSESSMENT-READY.

Speak to an expert today about your compliance plan.

The CMMC Ready Suite

CMMC LEVEL 2 SOLUTION FOR IMPLEMENTING 110 CONTROLS

A fully managed, assessment-ready solution that delivers CMMC Level 2 certification as an outcome, aligned to all 110 NIST SP 800-171 controls, designed to protect CUI and preserve defense contract eligibility.

Fast Time to Certification

Purpose-built to achieve CMMC Level 2 assessment readiness quickly.

Low Total Cost of Ownership

Reduces scope and cost compared to MSP and DIY approaches.

Expert Guidance

Assessment-ready support to help you prepare for CMMC and sustain compliance over time.