SIMPATICO.COM



The Defense Contractor's **CMMC** Guide

Navigating Compliance, Certification & Risk Management.



Table of **contents**

01 Why CMMC Matters

The Department of Defense created CMMC to protect sensitive data across the defense supply chain. This chapter explains the growing cybersecurity threats and why compliance is now mandatory.

02 CMMC and Levels

CMMC introduces a simplified model with three certification levels based on data sensitivity and contract requirements. Learn what each level requires and how it applies to your organization.

03 The Assessment Process

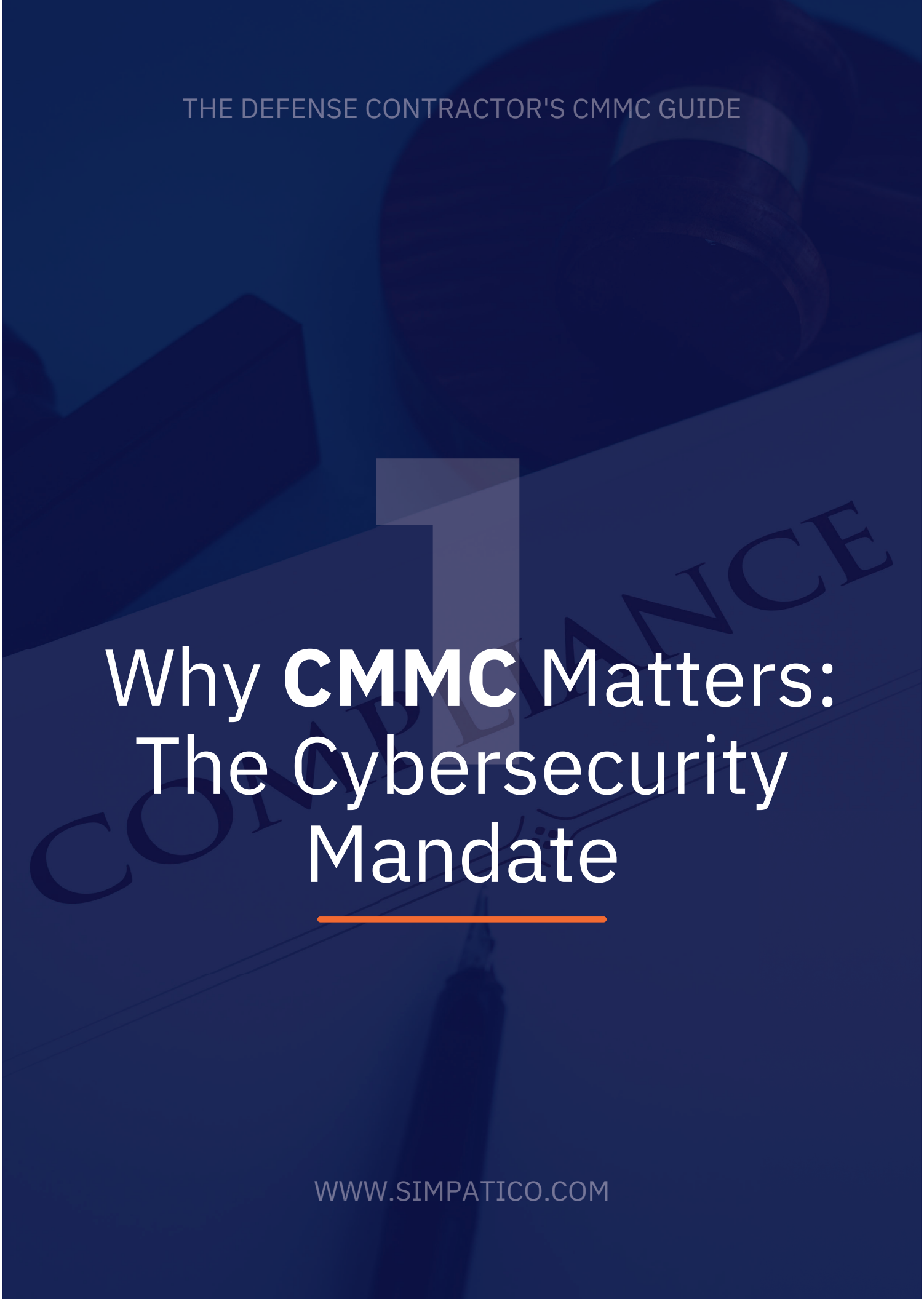
Whether you're doing a self-assessment or hiring a third-party assessor, preparation is key. This chapter walks through the process, timelines, and documentation needed to succeed.

04 Ecosystem and Risk

The CMMC ecosystem includes assessors, consultants, and support organizations. We'll explore their roles and how to build a risk management strategy that aligns with compliance.

05 How Simpatico Helps

Simpatico simplifies CMMC compliance with expert guidance, tools, and support. From readiness to implementation, we partner with you every step of the way.



1

Why **CMMC** Matters: The Cybersecurity Mandate



Why CMMC Matters

THE CYBERSECURITY MANDATE

Cybersecurity is no longer optional for organizations working with the U.S. Department of Defense (DoD). With rising threats from nation-state actors, cybercriminals, and insider threats, the Defense Industrial Base (DIB) has become a prime target. In response, the DoD developed the Cybersecurity Maturity Model Certification (CMMC) to ensure standardized and enforceable cybersecurity practices across its contracting ecosystem.

CMMC represents a transformative shift in the way the DoD views cybersecurity compliance. Rather than relying on a contractor's word or assumptions of good practice, CMMC requires concrete evidence that proper cybersecurity measures are in place. It replaces "trust but verify" with "verify then trust."

Contractors must demonstrate they have implemented adequate cybersecurity controls before being awarded contracts involving Federal Contract Information (FCI) or Controlled Unclassified Information (CUI). This certification process ensures that only organizations with a secure posture are entrusted with sensitive data that could impact national security.

LEGACY COMPLIANCE FOUNDATIONS

The need for CMMC stems from more than a decade of regulatory evolution. While CMMC is relatively new, it stands on the shoulders of earlier mandates designed to protect sensitive but unclassified government data:

- 2010: Executive Order 13556 establishes the Controlled Unclassified Information (CUI) program to create uniformity in how unclassified information is safeguarded.
- 2015: DFARS 252.204-7008 requires contractors to comply with NIST SP 800-171 security requirements.
- 2016: DFARS 252.204-7012 mandates reporting of cyber incidents and protection of CUI.
- 2019: A DoD Inspector General report reveals widespread non-compliance across the DIB.
- 2020: Section 1648 of the NDAA prompts the DoD to develop a formal assessment framework.
- 2024: Title 32 CFR Part 170 is published, officially codifying CMMC.

Who Must Comply

CMMC requirements apply to all contractors and subcontractors that process, store, or transmit FCI or CUI on behalf of the DoD. Organizations dealing only in Commercial Off-The-Shelf (COTS) products and contracts below the micro-purchase threshold are generally exempt. Importantly, the DFARS 252.204-7021 clause requires compliance to be passed down to subcontractors, ensuring that the entire supply chain is secure.

TIMELINE FOR IMPLEMENTATION

CMMC is being implemented in phases, allowing organizations time to prepare:

- **Phase 1 (0–12 months):** Contractors can perform self-assessments for Level 1 and Level 2 (non-critical CUI).
- **Phase 2 (12–24 months):** Third-party assessments become mandatory for contractors dealing with critical CUI.
- **Phase 3 (24–36 months):** Level 3 assessments begin, conducted by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).
- **Phase 4 (36+ months):** CMMC is fully integrated into all contracts, including renewals and option years.





Legal Ramifications

Contractors must be aware of the legal consequences of non-compliance. The Department of Justice's Civil Cyber-Fraud Initiative leverages the False Claims Act (FCA) to hold contractors accountable for cybersecurity failures. Legal action can result from:

- Knowingly providing insufficient cybersecurity.
- Submitting false affirmations or scores.
- Failing to report cyber incidents as required.

Penalties for FCA violations can include fines in the millions, debarment from government contracting, and reputational damage. It is essential that organizations maintain accurate records, submit truthful affirmations, and take corrective actions when needed.



2

CMMC Framework and Certification Levels



CMMC Framework & Certification Levels

CMMC FRAMEWORK

CMMC simplifies the certification structure while maintaining rigor. It aligns closely with existing NIST standards, creating a streamlined path to compliance and reducing duplicative efforts for organizations already following federal guidelines.

LEVEL 1: FOUNDATIONAL

Level 1 is intended for contractors that handle only FCI. It requires implementation of 15 basic cybersecurity practices derived from FAR 52.204-21. These controls are considered fundamental to safeguarding data such as names, addresses, contract performance dates, and other general federal contract information.

- **Assessment Method:** Annual self-assessment.
- **Reporting:** Results must be submitted in the Supplier Performance Risk System (SPRS).
- **Limitations:** No use of Plans of Action & Milestones (POA&Ms) permitted; all controls must be fully implemented.

LEVEL 2: ADVANCED

Level 2 is for organizations handling CUI. The requirements include full implementation of all 110 security controls from NIST SP 800-171 Rev 2. Level 2 introduces differentiated assessment paths based on the criticality of the work.

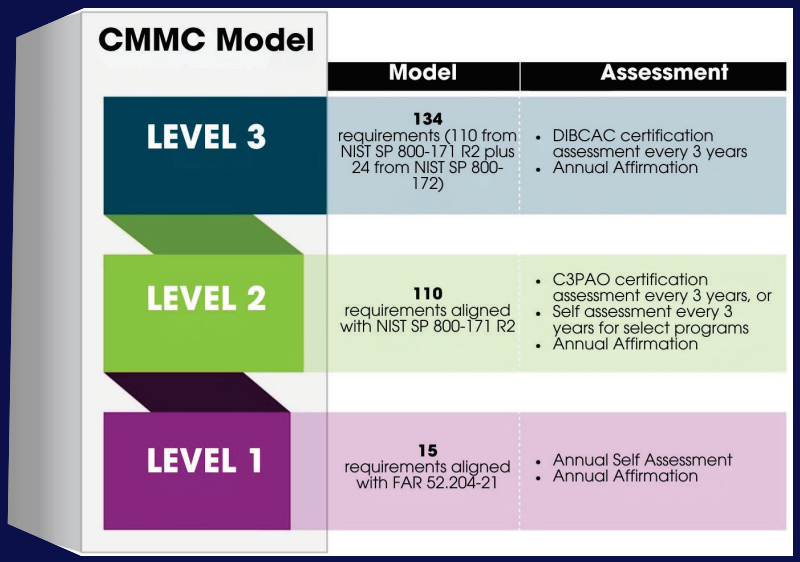
- **Self-assessment:** Permitted for non-priority programs (non-critical CUI).
- **Third-party assessment:** Required for priority programs (critical CUI), conducted by a Certified Third-Party Assessment Organization (C3PAO).
- **Conditional Certification:** Contractors scoring 88/110 or higher may receive conditional approval, provided missing controls are addressed within 180 days.
- **POA&Ms:** Permitted for select controls under strict conditions.

Level 3: Expert

Reserved for contractors supporting critical DoD missions, Level 3 builds upon Level 2 with an additional 24 controls derived from NIST SP 800-172.

- **Assessment:** Must be conducted by DIBCAC.
- **Requirements:** Must have a perfect Level 2 score and achieve a score of at least 20/24 for Level 3.
- **POA&Ms:** Allowed under limited conditions; remediation must be completed within 180 days and verified through a closeout assessment.

CMMC provides a realistic and enforceable framework that raises the cybersecurity baseline while accounting for practical implementation timelines and resource constraints.



CMMC Clauses to Look for in DoD Contracts

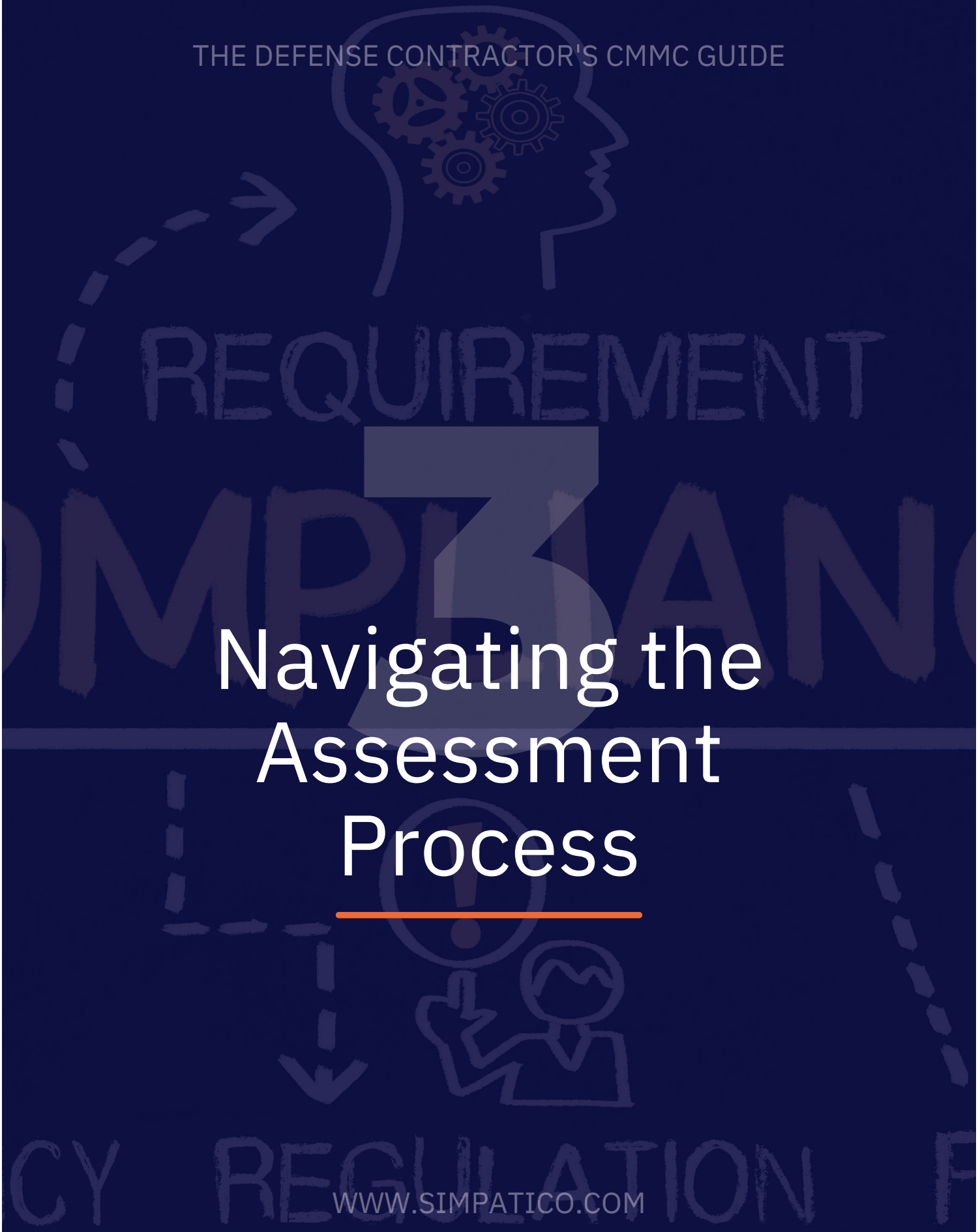
Understanding which clauses to watch for in DoD contracts is essential for identifying when CMMC requirements apply. Here are the most common and critical clauses contractors should look for:

- **DFARS 252.204-7012:** Requires implementation of all 110 NIST SP 800-171 controls and mandates reporting cyber incidents within 72 hours. Cloud services must meet FedRAMP Moderate standards if storing Covered Defense Information (CDI).
- **DFARS 252.204-7019:** Requires a NIST SP 800-171 assessment (Basic, Medium, or High) with results uploaded to SPRS—even if CMMC isn't yet required for the contract.
- **DFARS 252.204-7020:** Gives the DoD the right to verify your self-assessment and conduct its own review. Ensures your reported scores are accurate and verifiable.
- **DFARS 252.204-7021:** Specifies the required CMMC certification level (1, 2, or 3). Determines if self-assessment or third-party certification is needed based on contract risk.

Tips for Contract Review

- Review the SOW: CMMC may apply only to certain project components.
- Check Flowdown Requirements: Subcontractors may inherit CMMC obligations.
- Verify Level Match: Your CMMC level must match what's required in the contract—no exceptions.





Navigating the Assessment Process

Navigating the Assessment Process

The CMMC assessment process is a critical milestone on the path to certification. It's not just about putting cybersecurity measures in place—it's about proving that those measures are effectively implemented, documented, and maintained over time. The goal is to ensure that contractors handling Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) meet the necessary cybersecurity requirements appropriate to the sensitivity of the data they manage. Organizations must prepare to demonstrate the maturity and consistency of their cybersecurity practices through either self-assessments or independent third-party audits, depending on their assigned CMMC level.

ASSESSMENT TYPES BY CERTIFICATION LEVEL

• **Level 1:** Organizations handling FCI must complete an annual self-assessment. This involves reviewing the 17 required practices for basic cyber hygiene and uploading results into the Supplier Performance Risk System (SPRS). No third-party validation is required at this level, but documentation and accuracy are still essential.

• **Level 2:** For contractors managing CUI, assessment requirements vary based on the nature of the work:

- If the CUI is considered non-critical to national security, a self-assessment is allowed once every three years.
- If the environment involves critical CUI, a triennial assessment must be conducted by a Certified Third-Party Assessor Organization (C3PAO).

These Level 2 assessments are far more rigorous, requiring detailed evidence, documentation, and scoring against the 110 practices in NIST SP 800-171.

• **Level 3:** This level applies to organizations working with the most sensitive or mission-critical information. Assessments are carried out by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) and are reserved for high-impact contractors. Level 3 evaluations assess not only compliance with NIST SP 800-171 but also with selected elements of NIST SP 800-172 for advanced cybersecurity capabilities. Each level of assessment is designed to ensure that organizations are not just checking boxes, but actively embedding cybersecurity into their operational fabric. It's an evaluation of readiness, resilience, and risk management.

Plans of Action & Milestones (POA&Ms)

A POA&M is a formal document outlining how an organization plans to remediate specific cybersecurity gaps identified during the assessment. It enables companies to move forward with a contract even if they haven't fully met all requirements, provided that critical elements are in place and a clear plan exists to close the gaps.
To qualify for conditional approval using a POA&M:

- A minimum score of 88 out of 110 is required for Level 2 assessments.
- A minimum score of 20 out of 24 is required for Level 3 assessments.
- No high-priority (critical) controls may be missing.
- All identified deficiencies must be remediated within 180 days, followed by a closeout assessment to verify completion.

This structured approach offers some flexibility, but it also ensures accountability and a firm deadline for achieving full compliance.





Affirmation and Legal Responsibility

Beyond the assessment itself, CMMC requires ongoing accountability. Every certified organization must submit an annual affirmation of compliance, signed by a senior executive, to the SPRS. This declaration confirms that the organization continues to uphold the CMMC standards it was certified against.

This isn't just a formality—false affirmations or misrepresentations can result in serious consequences, including penalties under the False Claims Act (FCA), breach of contract allegations, and potential disqualification from future government contracts. The affirmation requirement reinforces that cybersecurity compliance is not a one-time achievement but a continuous responsibility led from the top.



The CMMC Ecosystem & Risk Management

The CMMC Ecosystem & Risk Management

Achieving CMMC certification is not a solo effort. A robust ecosystem of stakeholders, guidance bodies, assessors, and technology providers support organizations throughout the process.

KEY STAKEHOLDERS

CMMC is governed by a well-defined structure, with each participant playing a distinct role in policy enforcement, training, and certification.

- **DoD CIO / CMMC PMO (Program Management Office):** The top-level authority that develops the CMMC framework, issues policy guidance, and provides updates based on evolving cybersecurity threats and defense needs.
- **DCMA DIBCAC (Defense Industrial Base Cybersecurity Assessment Center):** Responsible for conducting Level 3 assessments, DIBCAC ensures that organizations with the highest security requirements are held to strict standards. They also audit the performance of other assessment entities to enforce quality.
- **Cyber AB (Accreditation Body):** Formerly the CMMC Accreditation Body, Cyber AB oversees the certification ecosystem. It accredits third-party assessment organizations (C3PAOs), manages the Cybersecurity Assessor and Instructor Certification Organization (CAICO), and ensures assessor quality and consistency.
- **C3PAOs (Certified Third-Party Assessment Organizations):** These independent, certified entities are authorized to conduct official Level 2 CMMC assessments. They evaluate an organization's compliance against the NIST SP 800-171 standards and report findings to the DoD.
- **CAICO (Cybersecurity Assessor and Instructor Certification Organization):** Under Cyber AB, CAICO designs and delivers assessor training programs that meet ISO/IEC 17024 accreditation standards. This guarantees a consistent, professional level of auditing expertise across the board.

Together, these stakeholders ensure that assessments are fair, standardized, and rooted in cybersecurity best practices. For contractors, understanding the role of each entity helps demystify the process and supports more effective engagement at every step.

CYBERSECURITY RISK MANAGEMENT BEST PRACTICES

While CMMC provides a structured framework, true cyber resilience goes beyond checking compliance boxes. Risk management is an ongoing process of evaluating threats, reducing vulnerabilities, and building a culture of security that extends from leadership to frontline employees.
Here are core risk management strategies aligned with CMMC expectations:

- **Maintain an Up-to-Date System Security Plan (SSP):** Your SSP is the foundation of your cybersecurity posture. It must be accurate, living documentation that reflects your current technical environment and controls.
- **Enforce Multi-Factor Authentication (MFA):** MFA is required across most access points, especially for administrators, remote users, and systems handling CUI. It significantly reduces the risk of unauthorized access.
- **Implement Access Controls:** Adopt the principles of least privilege and role-based access. Only authorized personnel should have access to sensitive systems or data, and access should be regularly reviewed.
- **Encrypt Sensitive Data:** Ensure that data at rest and in transit is encrypted using FIPS-validated cryptographic solutions. Encryption is a core expectation under both CMMC and NIST 800-171.
- **Train Personnel Regularly:** Ongoing cybersecurity awareness and role-specific training reduce the risk of user-driven breaches. Everyone in the organization should understand their responsibilities and the consequences of non-compliance.
- **Track and Update POA&Ms (Plans of Action & Milestones):** Active tracking of POA&M progress ensures that security gaps are addressed within allowed timelines. Make sure to document progress and closeout activities accurately.

By embedding these practices into your daily operations, you're not just preparing for an audit—you're building a security-first culture that enhances trust, reduces liability, and supports long-term business sustainability.



5

Partnering for Compliance: How **Simpatico** Helps



Navigating the Assessment Process

Navigating the CMMC landscape can be overwhelming—especially for small and mid-sized defense contractors who lack the internal expertise or resources to manage complex compliance requirements. That's where Simpatico comes in. We don't just guide you through the CMMC certification process—we empower your organization to build a sustainable, future-ready cybersecurity program that aligns with business objectives and DoD expectations.

Simpatico serves as a strategic partner at every stage of your compliance journey, from initial readiness assessments to long-term managed cybersecurity services. With a team of certified experts and a deep understanding of the defense industry, Simpatico ensures you stay on track, avoid costly delays, and meet all CMMC obligations with confidence.

OUR END-TO-END CMMC COMPLIANCE SERVICES

Simpatico offers comprehensive services tailored to your business's maturity level, risk profile, and certification goals:

- **Readiness Assessments:** Identify existing gaps between your current security posture and CMMC requirements. Our team conducts a detailed analysis to help you understand your starting point and what it will take to become compliant.
- **System Security Plan (SSP) & POA&M Development:** We help you build accurate, audit-ready documentation—your SSP, Plan of Action & Milestones (POA&M), Incident Response Plan, and more. These documents are foundational to passing your assessment.
- **SPRS Score Calculation & Submission:** Simpatico helps calculate and validate your NIST SP 800-171 score, ensuring it meets DoD expectations for submission into the SPRS.
- **Endpoint Protection, Monitoring & Incident Response:** We offer enterprise-grade security tools and 24/7 monitoring to detect, respond, and recover from threats, ensuring you're covered before, during, and after certification.
- **Managed Compliance-as-a-Service:** Stay secure and compliant with ongoing patching, backup, MFA enforcement, access controls, and continuous documentation updates—all managed by Simpatico's expert team.

Why Simpatico?

Compliance is about more than passing an audit. It's about protecting your organization, maintaining eligibility for defense contracts, and building a cybersecurity strategy that scales with your business. Simpatico goes beyond checklists—we deliver strategic value:

- **Risk Reduction:** We help reduce your attack surface with layered defenses, threat detection, and continuous monitoring tailored to your unique environment. From endpoint protection and vulnerability management to secure system architecture, we proactively identify and mitigate risks before they become liabilities. Our team stays ahead of emerging threats to ensure your infrastructure remains secure, resilient, and ready for audit at all times.

- **Contract Eligibility:** Our services ensure that you meet all certification and reporting requirements to remain competitive in the DoD contracting space. Whether you're bidding on new contracts or renewing existing ones, Simpatico helps you demonstrate compliance in a way that builds trust with prime contractors, subcontractors, and government agencies. We help maintain your SPRS score, manage your documentation, and prepare you for audits—so you never miss an opportunity due to a lapse in compliance.

- **Simplicity and Support:** We turn the complexity of CMMC into a clear, manageable process through end-to-end project planning, dedicated support, and straightforward communication. With Simpatico, you're never navigating compliance alone. You'll have a dedicated partner to answer questions, guide decisions, and keep you informed and confident every step of the way—from gap assessments to final submission.

- **Cybersecurity Alignment:** Our approach isn't just about passing a certification—it's about aligning cybersecurity with your broader business goals. We help you make smarter investments in security technologies that reduce operational risk, improve customer confidence, and ensure long-term scalability. As your needs grow, Simpatico scales with you—delivering the right level of protection, governance, and operational support at every stage.

With Simpatico, you're not just meeting minimum standards—you're building a resilient, audit-ready organization that's positioned for long-term success in the defense supply chain. We understand what's at stake—your contracts, your reputation, and your future. That's why we offer more than services—we offer a partnership built on trust, expertise, and a shared commitment to cybersecurity excellence.

Call or visit our website
for more information
about CMMC

855-672-4800 SIMPATICO.COM