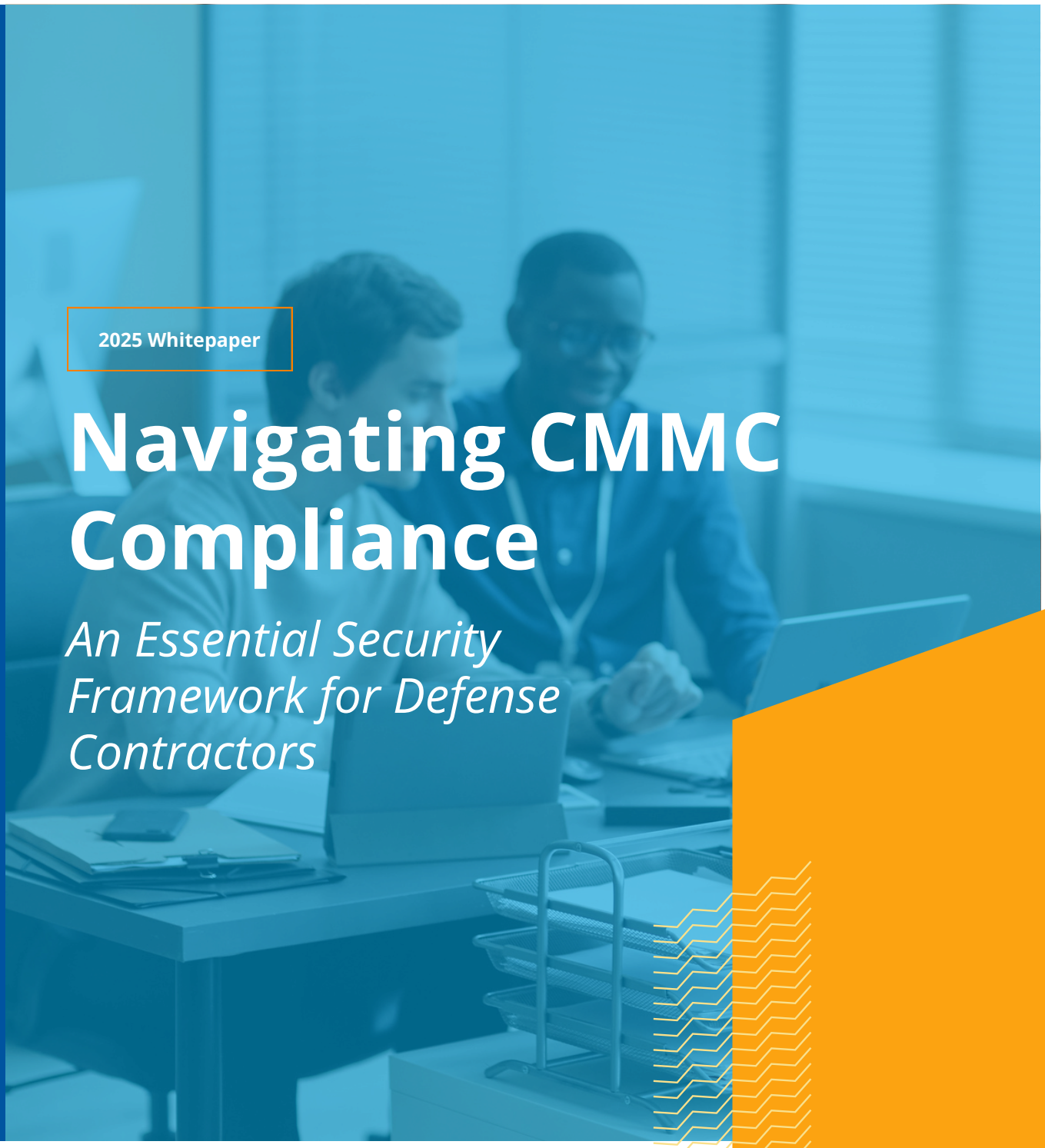
BARR ADVISORY



2025 Whitepaper

# Navigating CMMC Compliance

*An Essential Security Framework for Defense Contractors*

# Table of Contents


2 | Introduction

3 | What is CMMC?

5 | Who Must Comply with CMMC?

6 | What Are the Three Levels of CMMC Compliance?

7 | Where Do I Start?

8 | About BARR Advisory

# Introduction

**For organizations that want to do business with the U.S. Department of Defense (DoD), understanding the Cybersecurity Maturity Model Certification (CMMC) program is a crucial first step.**

Introduced by the DoD in 2020, CMMC is a program designed to safeguard national security by mandating that DoD contractors and subcontractors adhere to a series of baseline cybersecurity requirements for protecting sensitive government data.

So, what exactly is CMMC, who needs to comply, and what does it take to achieve compliance? In this whitepaper, we break it down.

# What is CMMC?

The DoD works with a network of tens of thousands of private companies that collectively make up the defense industrial base (DIB). These companies handle sensitive government information, and if that data falls into the wrong hands, it could threaten national security. To mitigate this risk, CMMC was developed to ensure all DoD contractors follow cybersecurity best practices based on the level of risk their work involves.

CMMC was specifically designed to protect two types of sensitive information:

**Federal Contract Information (FCI):**
This includes communications related to government contracts, such as contract details, RFPs, and other collaborative documents.

**Controlled Unclassified Information (CUI):**
This includes sensitive but unclassified government information, such as technical schematics, research data, and procedural documents. While not technically classified as "secret" or "top-secret," CUI still presents a national security risk if exposed.

By enforcing cybersecurity maturity across the DIB, CMMC ensures that companies working with the U.S. military take cybersecurity seriously.

# Who Must Comply with CMMC?

Any company that handles FCI or CUI, or that works directly or indirectly on a DoD contract, is likely required to comply with CMMC. This includes contractors, subcontractors, and third-party vendors that support defense projects. If your business is involved with the DoD in any capacity, you should expect to comply with CMMC requirements.

CMMC uses a tiered system to match security requirements with the sensitivity of the information a company handles. Under the program's tiered model, companies that handle higher-risk information or data that is especially critical to national security are subject to stricter standards.

Regardless of your risk level, CMMC compliance is an important requirement for doing business with the DoD and a key step toward securing future government contracts.

# What Are the Three Levels of CMMC Compliance?

The CMMC framework establishes three levels of compliance, each incorporating security requirements from existing regulations and guidelines:

**Level 1** requires organizations to complete an annual self-assessment and an annual affirmation of compliance with the 15 security requirements outlined in FAR clause 52.204-21.

**Level 2** requires an annual affirmation and verification of compliance with the 110 security requirements in NIST SP 800-171. Organizations at this level must also undergo a self-assessment or external assessment by a CMMC Third-Party Assessor Organization (C3PAO) every three years, depending on what the DoD requires in their contract.

**Level 3** requires organizations to undergo an assessment every three years by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). Organizations at this level must also provide an annual affirmation verifying compliance with the 24 identified requirements from NIST SP 800-172, which expand on the requirements outlined in NIST SP 800-171.

Depending on your organization's level of risk, a third-party attestation may not be required to achieve CMMC compliance. However, businesses planning to pursue DoD contracts should be proactive about compliance.

# Where Do I Start?

Even if you don't yet have a government contract, beginning the CMMC readiness process now—including conducting a gap assessment and understanding how your environment aligns with the DoD's requirements—can help you secure future opportunities.

With deep expertise in cybersecurity and government contracting, BARR Advisory simplifies the CMMC process with end-to-end consulting, including gap analysis, implementation support, and ongoing compliance maintenance. Our expert CMMC consultants guide you every step of the way, helping you meet DoD standards and grow your government contracting opportunities.

## *How It Works*

### STAGE 1

CMMC Architecture & Business Process Mapping: At this stage, we work with you to assess your business processes and data flows and define scope, determining which parts of your business are subject to CMMC requirements. This helps set the foundation for compliance and align your internal processes with the current and future expectations of government agencies.

### STAGE 2

CMMC Gap Analysis: At this stage, we conduct a thorough analysis of your systems against CMMC requirements, including the NIST SP 800-171 baseline for organizations pursuing Level 2 compliance. You'll walk away with a clear roadmap for securing contracts and strengthening your position in government sectors.

### STAGE 3

CMMC Implementation Support: Once you understand the requirements that your organization must adhere to under CMMC, we'll help you implement the required controls with security architecture and engineering support. This could include unique solutions like building out a fully compliant cloud meant to isolate and minimize in-scope systems. Limiting the exposure of sensitive data to the custom-built cloud environment allows business processes that are out of scope to remain unaffected, so you can achieve compliance with as little disruption as possible to business as usual.

### STAGE 4

CMMC Sustainment: After you've achieved initial compliance, we'll continue offering support to help your team maintain audit readiness and reduce risk.

Whether you're actively working with the DoD or positioning yourself for future contracts, now is the time to take action. With evolving government regulations, staying ahead of compliance expectations can give your business ***a competitive edge***.

# About BARR Advisory

BARR Advisory is a security and compliance solutions provider specializing in cybersecurity and compliance for organizations with high-value data that serve regulated industries such as healthcare, financial services, and government. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements.

## Our Services

**SOC Examinations**
SOC 1, SOC 2, SOC 3, SOC for Cybersecurity

**Healthcare Services**
HIPAA/HITRUST

**ISO/IEC Certifications**
ISO 27001, ISO 42001

**FedRAMP Security Assessments**

**PCI DSS Assessment Services**

**Penetration Testing and Vulnerability Assessments**

**Cybersecurity Consulting**
GRCaaS, CMMC, Security Engineering Services

**Compliance Program Assistance**

## Connect with BARR

Need help navigating compliance in the age of AI? Contact us today for a free consultation.