RICHEY MAY | Cyber

CMMC 2.0:

Your Comprehensive Guide to Certification and Compliance

You don't need to build fighter jets to be subject to the rigorous requirements of the Cybersecurity Maturity Model Certification (CMMC 2.0). Whether you are a large aerospace provider or a small screw manufacturer, if you work with the Department of Defense (DoD) and handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI), you are required to meet the cybersecurity standards outlined in CMMC 2.0.

The data handled by the DoD—and its contractors—is among the most sensitive and critical in the nation. From defense strategies to advanced technology designs, any breach of this data could have catastrophic consequences for U.S. national security. Incidents like the SolarWinds supply chain attack, which impacted nearly 40 federal contractors, are powerful reminders that these breaches do happen - and their impacts can be far-reaching.

Given the critical nature of this data, it's clear why robust frameworks like CMMC 2.0 are necessary to strengthen security. Understanding the framework and achieving full compliance with the help of qualified providers is crucial to ensuring continued DoD partnership, driving business continuity, and, significantly, safeguarding the nation's sensitive data. However, this framework's broad scope and complexity give rise to various challenges.

Understanding the CMMC 2.0 Framework

The original CMMC launched in 2020, and an updated CMMC 2.0 was announced late in 2023 ahead of a phased rollout. Based on the NIST 800-171 standards, CMMC 2.0 simplifies the original CMMC framework, offering a more streamlined compliance journey.

Small and medium-sized businesses benefit from this latest version for several reasons. First, the number of levels was reduced from five to three (as we explain below). Companies requiring Level 1 can now self-assess instead of hiring a third-party provider to conduct their compliance audit. Plus, with the process being more straightforward and practical, companies can save costs and speed up the implementation of new security practices.

CMMC 2.0 covers critical cybersecurity areas, including Access Control, Incident Response, and Risk Management to protect operations comprehensively. It is divided into three certification levels based on the sensitivity of the information handled:

LEVEL 1: **FOUNDATIONAL**

Level 1 covers companies managing Federal Contract Information (FCI), which typically involves data related to contracts, procurement, and financial transactions. For example, an office supplies provider that handles procurement orders and billing information would fall under this level.

Compliance at this level requires implementing 17 basic cybersecurity practices and can involve a self- or third-party assessment. While self-assessments are allowed, organizations benefit from the guidance and technical knowledge of compliance experts.

LEVEL 2: **ADVANCED**

Level 2 is intended for organizations handling Controlled Unclassified Information (CUI), which refers to unclassified data that requires protection under law or government policy. It could include military blueprints, research data, or specific technical data related to defense projects.

A company designing software for managing military supply chains would fall under this category, as it handles specific technical information related to defense operations. At this level, companies must adhere to 110 practices aligned with NIST SP 800-171, with prioritized CUI requiring a third-party audit and non-prioritized CUI allowing self-assessment.

The distinction between prioritized versus non-prioritized CUI is nuanced, but you can find more information in the latest official updates. If you handle both FCI and CUI, you can also conduct two separate CMMC activities: one self-assessment for Level 1 and one external assessment for Level 2.

LEVEL 3: **EXPERT**

Lastly, level 3 focuses on entities dealing with critical national security data like classified technical specifications and defense-related research. Consider an aerospace and defense contractor that builds highly sensitive systems like space technologies - they would fall under this category. Compliance demands additional practices and collaboration with the DoD and must be assessed by a third party.

RICHEY MAY | Cyber

Five Steps to Achieve CMMC 2.0 Certification

Achieving CMMC 2.0 certification is a layered process that can take nine months to two years. The goal isn't just to meet regulatory requirements and continue doing business with the DoD but to strengthen your cybersecurity posture in the long term by implementing the right solutions. Companies can remove some of the complexities of CMMC 2.0 by following these five common steps:

STEP ONE: INITIAL ASSESSMENT AND GAP ANALYSIS

Begin by evaluating your organization's cybersecurity posture through a comprehensive audit that covers security controls, data handling procedures, and risk management policies.

You can then identify gaps between current practices and CMMC requirements to establish a roadmap for improvements, which industry experts often refer to as a Plan of Action and Milestones (POA&M).

This assessment clarifies your certification-level needs and prioritizes actions based on risks and compliance objectives. You should adopt a phased approach to your compliance journey, starting with the high-risk areas (systems and activities that handle critical national security data).

STEP TWO: DOCUMENTATION AND POLICY CREATION

Develop or update policies and procedures to align with CMMC requirements. Comprehensive and tailored documentation ensures clear governance structures and consistent implementation of security controls.

This step could include drafting formal documents like an Incident Response Plan for Level 2 or an Access Control Policy for handling Controlled Unclassified Information (CUI) following NIST SP 800-171. While required for CMMC, following NIST SP 800-171 is also a best practice for organizations across all industries, making it a smart approach regardless of your CMMC level.

STEP THREE: IMPLEMENTATION OF SECURITY CONTROLS

Deploy the necessary security controls—such as policies, procedures, and risk management practices—to meet CMMC standards. Key security controls include multifactor authentication (MFA), endpoint security, and network segmentation.

In some cases, modernizing legacy systems may be required to enable the application of mandatory controls. If updating legacy infrastructure is too costly or complex, adopting cloud-based platforms with built-in security features could be a more efficient solution.

If your scope falls under CMMC Level 2, your cloud services must be **FedRAMP** (Federal Risk and Authorization Management Program) certified.

The goal isn't just to meet regulatory requirements and continue doing business with the DoD, but to strenghen your cybersecurity in the long term by implementing the right solutions.

A comprehensive third-party risk assessment can help verify FedRAMP compliance and assert relevant third-party risk management (TPRM) practices.

STEP FOUR: PRE-ASSESSMENT WITH AN RPO

Although you need to employ a designated third party to conduct the official audit, pre-auditing your systems and processes will help you address any overlooked gaps (like a lack of regular data backups or missing system patching procedures, which are issues that may fall through the cracks).

Registered Practitioner Organizations (RPOs) like Richey May offer a simulated audit experience to ensure readiness, reduce the risk of a failed audit, and avoid the additional costs and burdens of a second attempt. Unlike general security firms that address a wide range of security and compliance areas, RPOs are specifically trained and experienced in the CMMC framework. They leverage their expertise to provide tailored guidance and develop a focused, structured approach to meeting CMMC requirements to streamline your formal assessment for certification as outlined below.

You can also rely on an RPO like Richey May, which is CMMC-compliant and offers other Managed Security Services, to handle your compliance needs. Outsourcing compliance efforts lightens the load on your team and ensures your organization remains fully protected.

STEP FIVE: FORMAL ASSESSMENT WITH A CERTIFIED THIRD-PARTY ASSESSOR ORGANIZATION

The final stage involves a comprehensive audit conducted by a Certified Third-Party Assessor Organization (C3PAO). Achieving certification through this evaluation confirms compliance with CMMC standards and demonstrates a commitment to cybersecurity excellence. These certifications are valid for three years, so enhancing the ongoing protection of sensitive information will be important and will also make re-certification smoother in the future.

While Richey May is not a C3PAO, we have exclusive access to a strong network of trusted C3PAO partners. Our established relationships with these partners enable us to collaborate closely throughout your audit, ensuring a smooth and efficient process from start to finish.

Organizations that complete these steps achieve compliance while strengthening defenses against cybersecurity threats. This preparation builds resilience, mitigates risks, and reinforces their role as reliable federal partners in a regulated environment.

Remember that cybersecurity isn't a one-and-done task but rather an ongoing commitment. Once you have achieved CMMC 2.0 compliance, consider employing dedicated Managed Security Services to ensure continuous monitoring and visibility over your security systems.

At Level 2 and above, your Managed Service Provider (MSP) or MSSP must also be certified to Level 2, so you must verify that they have the appropriate certification. If you're working with an MSP that doesn't meet these requirements, consider exploring other partners who are Level 2 certified and can support your ongoing compliance efforts.

RICHEY MAY | Cyber

Addressing Challenges in CMMC Compliance

Despite being a simplified version of the original framework, CMMC 2.0 compliance still requires significant investment in time, expertise, and resources. This process can be particularly challenging for smaller businesses or those with limited technical expertise. Yet, overcoming these barriers is essential for securing sensitive information and fulfilling federal contract obligations. Common obstacles include:

- **Extensive Documentation:** Crafting detailed policies and compliance evidence can be time-intensive.
- **System Overhauls:** Upgrading outdated infrastructure to meet technical requirements may incur costs and resource strain. You may also need to create a separate enclave for Level 2 items, isolating them from your network to meet CMMC requirements.
- **Regulatory Interpretation:** Misunderstanding NIST SP 800-171 requirements can result in compliance gaps.
- **Resource Constraints:** Smaller organizations often lack the personnel or expertise for compliance.
- **Ongoing Adaptation:** CMMC is constantly evolving and requires continuous updates. These ongoing adjustments mean you need access to CMMC expertise at all times, not just periodically. Having a trusted partner dedicated to keeping up with these changes can ease the stress of compliance and the pressure of falling behind.

How Richey May Supports CMMC 2.0 Certification

As an RPO, Richey May is a trusted and experienced partner supporting organizations in navigating regulatory compliance complexities. With expertise tailored to the unique challenges faced by federal contractors, Richey May offers end-to-end support to simplify and optimize the compliance process. Services include:

- **Thorough Gap Analysis:** Assessing deficiencies in systems and practices.
- **Policy Development:** Creating customized, enforceable policies aligned with CMMC requirements.
- **Technical Implementation:** Deploying critical measures such as MFA and endpoint protection.
- **Pre-Assessments:** Preparing organizations for formal certification audits with actionable feedback.
- **CMMC-Compliant Managed Services:** Providing CMMC-certified managed services so your systems remain secure and compliant with all relevant frameworks, including CMMC.

With expertise tailored to the unique challenges faced by federal contractors, Richey May offers end-to-end support to simplify and optimize the compliance process.

Partnering with Richey May reduces the uncertainty, time, and cost associated with achieving compliance while significantly strengthening defenses. With a deep understanding of federal contractors' challenges, Richey May delivers tailored solutions that address current and emerging vulnerabilities, ensuring that businesses are compliant and resilient against evolving threats.

Achieving CMMC 2.0 certification is investing in long-term cybersecurity resilience. It ensures eligibility for lucrative DoD contracts for federal contractors and underscores a commitment to protecting sensitive data—fostering customer trust and driving sustained business success.

With the support of a trusted partner like Richey May, organizations can navigate the CMMC 2.0 compliance process confidently and efficiently. Contact us today.

GET IN TOUCH **RICHEY MAY CYBER**

P: (303) 721-6131 **W:** Richeymay.com/cybersecurity-services/