COMPASS ROSE
BY 360ADVANCED

STEP-BY-STEP GUIDE TO ACHIEVING CMMC COMPLIANCE

CMMC@360ADVANCED.COM | 360ADVANCED.COM | (866) 418-1708

Table of Contents

Introduction

Overview of CMMC

On October 11, 2024, the final program rule for the Cybersecurity Maturity Model Certification (CMMC) Program was released for public inspection on federalregister.gov and is expected to be officially published in the Federal Register on October 15, 2024. This marks a critical step in the Department of Defense's (DoD) efforts to improve the cybersecurity posture of the Defense Industrial Base (DIB).

The **CMMC program ensures that defense contractors comply with existing safeguards** for Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). These protections are tailored to the risks posed by cybersecurity threats, including advanced persistent threats (APTs)–sophisticated attacks aimed at compromising sensitive data.

Streamlined and Simplified Process

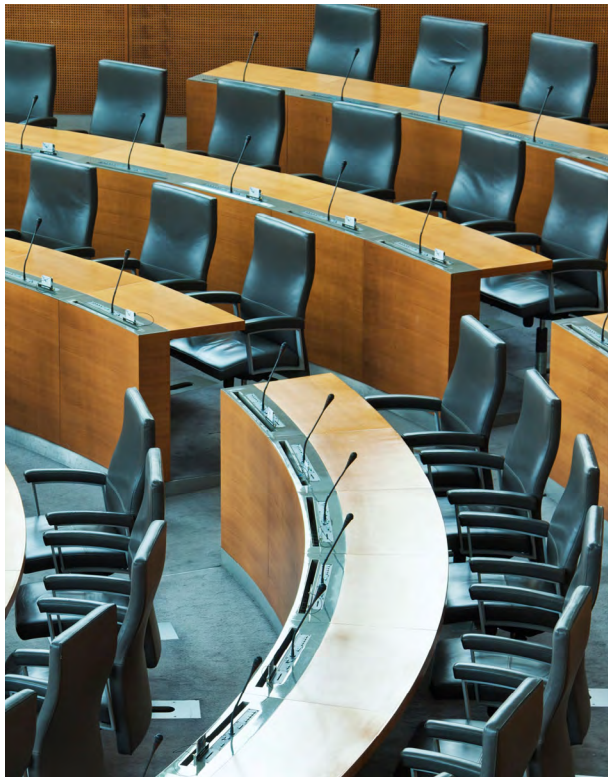
The updated CMMC rule **streamlines the certification process for small- and medium-sized businesses** by reducing the number of assessment levels from the original five to the current three. This makes the process easier and more efficient, while still ensuring that appropriate cybersecurity measures are in place based on the level of risk.

The final rule aligns with key cybersecurity standards, such as:

- Federal Acquisition Regulation (FAR) 52.204-21.
- NIST SP 800-171 Rev 2 for protecting CUI.
- NIST SP 800-172, which introduces additional security requirements for CMMC Level 3.

New Assessment Structure

With this updated 32 CFR rule, the **DoD is offering a more flexible approach for businesses to assess their compliance.** Depending on the type of information being handled and the level of cybersecurity protection required:



- **Level 1** requires a self-assessment for basic protection of FCI.
- **Level 2** allows for either a self-assessment or a third-party audit for general CUI protection.
- **Level 3** mandates a Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)-led audit for high-risk CUI and protection against APTs.

The CMMC framework is designed not only to safeguard critical information but also to **hold contractors accountable for their cybersecurity practices.** The self-assessment options and flexible assessments in the new rule are intended to **reduce the burden on companies while still maintaining high security standards.**

By simplifying compliance processes and offering different pathways for assessment, the **updated CMMC rule helps DIB companies of all sizes meet their obligations to protect sensitive data**–enabling them to continue participating in critical defense contracts without unnecessary barriers.

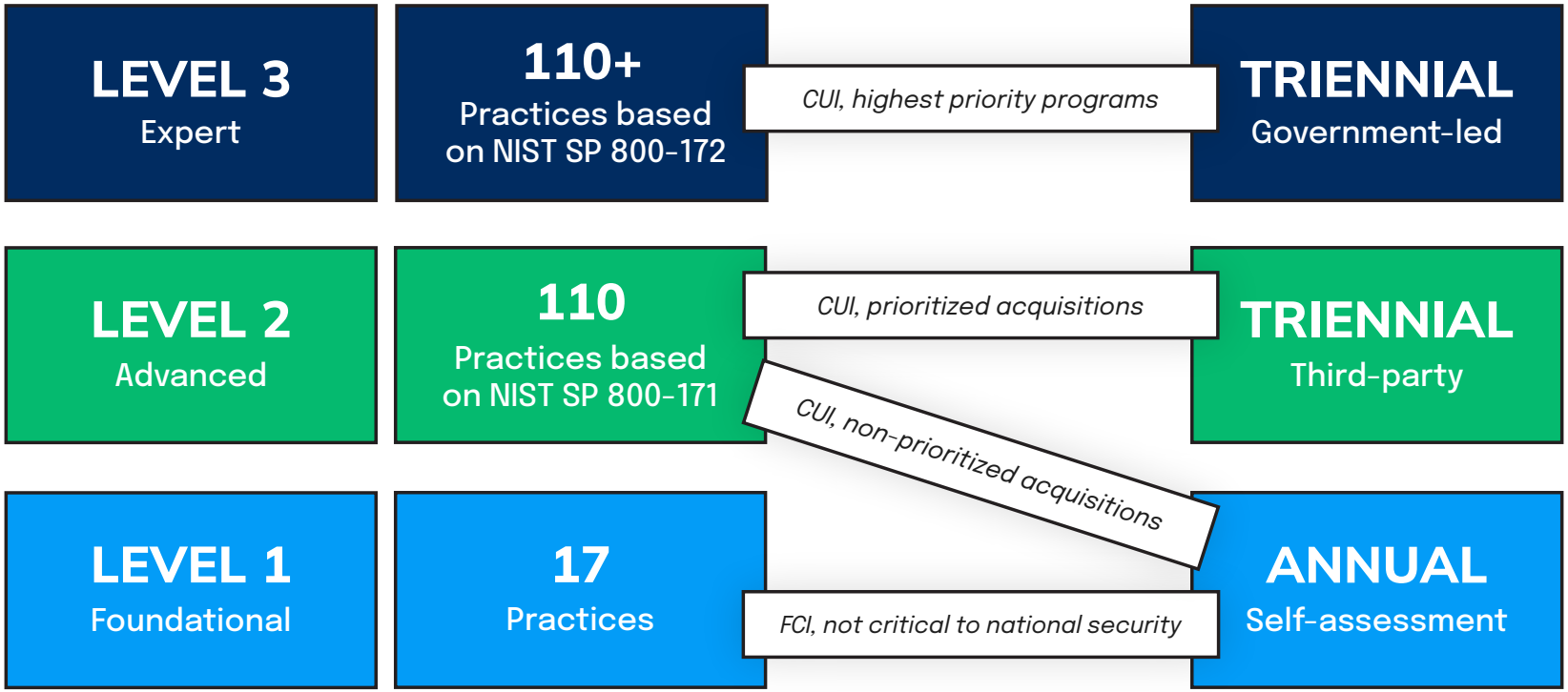
This new CMMC framework provides the tools necessary to safeguard national security while balancing the needs of businesses.

CMMC is the DoD initiative to ensure that companies handling Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) are practicing adequate cybersecurity. CMMC is mandatory for defense contractors and helps protect the sensitive information of the United States from cyber threats.

Why CMMC Compliance Matters

Achieving CMMC certification is crucial for maintaining contracts with the DoD. Non-compliance means losing the ability to bid on contracts, regardless of size. In simple terms, think of CMMC like a fitness requirement for participating in defense programs–if your organization isn't "cyber-fit," you're ineligible.

Step 1: Understand the Three Levels of CMMC



Level 1: Foundational

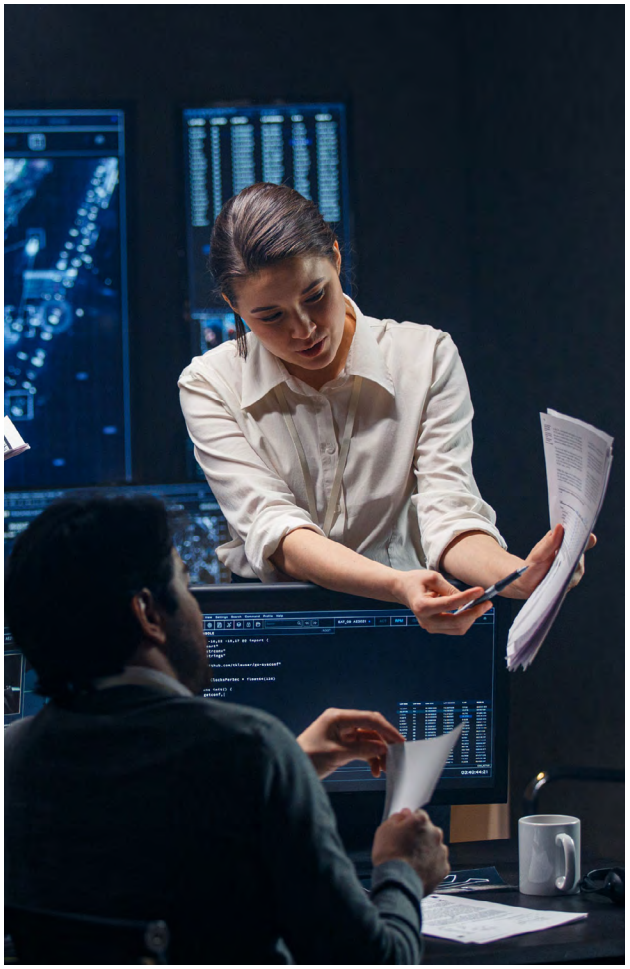
- **Purpose: Designed for companies handling FCI only**, which doesn't include sensitive national security information.
- **Requirements:** Companies must **implement 17 basic cybersecurity practices,** such as regularly updating antivirus software, managing user access, and ensuring password hygiene.
- **Assessment Type:** Self-assessment conducted annually.

Level 2: Advanced

- **Purpose: Aimed at companies handling CUI,** requiring increased cybersecurity measures.
- **Requirements: Implement 110 practices based on NIST SP 800-171.** These include encryption, access control, and incident response measures.
- **Assessment Type:** Third-party audit by a C3PAO, required every three years.

Level 3: Expert

- **Purpose:** Required for companies working on high-priority defense projects with **higher risks from advanced persistent threats (APTs).**
- **Requirements:** This level includes the **110 practices from Level 2, plus 24 additional practices from NIST SP 800-172 for advanced threat protection.**
- **Assessment Type:** Government-led assessment every three years.



Once the organization understands whether they handle FCI or CUI, they need to perform a data mapping exercise to see where that information lives (I.e. where it is stored, processed, and transmitted. This is done to define the boundary or scope of the system(s).

Step 2: Conduct a Gap Analysis

What is a Gap Analysis?

A gap analysis helps your company understand where it currently stands in relation to the CMMC requirements that apply to the scope of the system(s) based on the findings from Step 1. It's like getting a baseline fitness test before starting a training program. This analysis identifies cybersecurity gaps that must be addressed before you pursue certification.

Identify Areas for Improvement

- Review your current cybersecurity practices and policies.
- Compare these against the requirements for the CMMC level your organization needs to achieve.
- Identify specific areas where controls, technologies, or processes are lacking.
- Collaborate with 360 Advanced to create a customized roadmap for closing these gaps.

Step 3: Develop a Plan of Action and Milestones (POA&M)

Create a POA&M

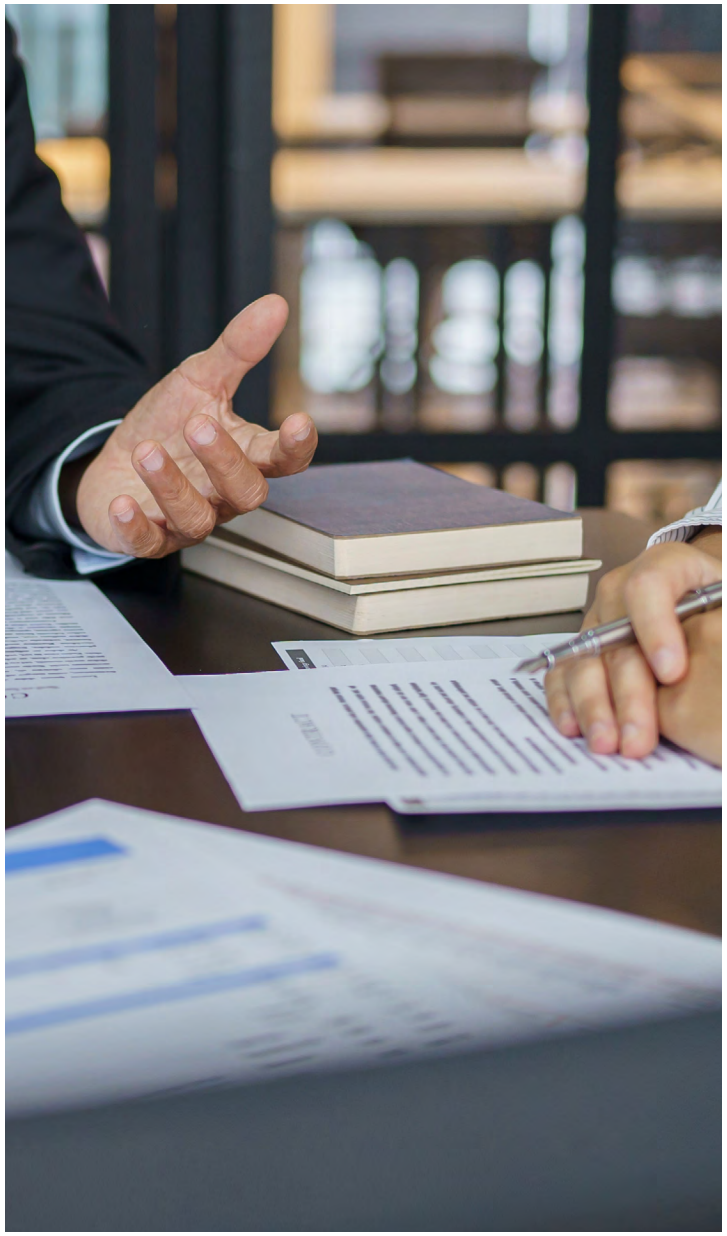
POA&M serves as a cybersecurity workout plan for achieving CMMC compliance. It outlines the **specific steps needed to address the deficiencies found during the gap analysis.**

- **Actionable Steps:** Define actions to address each cybersecurity weakness.
- **Milestones:** Set clear deadlines for achieving each goal.

Set Milestones

- Assign accountability to team members for completing tasks.
- Break down large goals into manageable steps, such as improving incident response systems or upgrading encryption technologies.
- Track progress regularly to ensure your organization stays on schedule.

Step 4: Implement Security Controls



Key Cybersecurity Practices

Implementing security controls is where you build the cyber muscles needed to meet CMMC requirements.

These controls include:

- **User Access Control:** Ensure that only authorized personnel can access sensitive information.
- **Data Encryption:** Protect CUI both when it's stored and transmitted by encrypting the data.
- **Incident Response Plans:** Develop a strategy for quickly detecting, responding to, and recovering from cyber-attacks.

Align with NIST Standards

At CMMC Level 2 and above, your company will need to align with NIST SP 800-171 (and for Level 3, additional practices from NIST SP 800-172). This includes monitoring for security incidents, protecting against unauthorized access, and managing risks from third-party service providers.

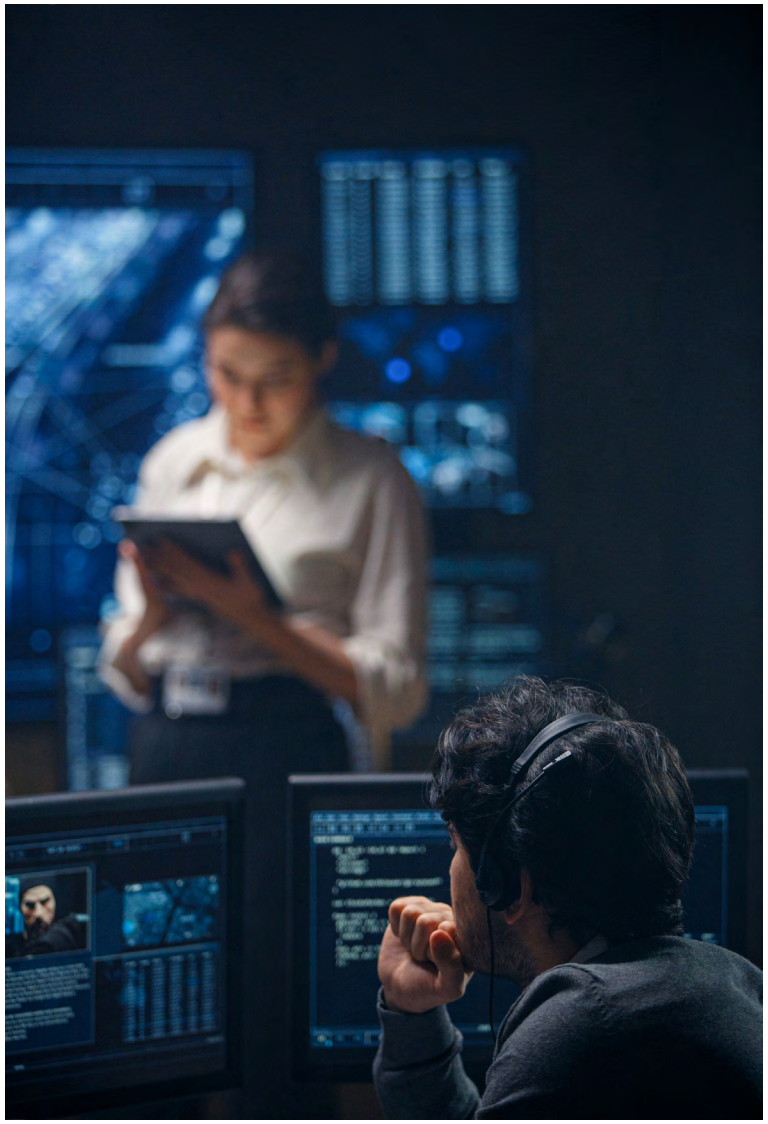
Step 5: Conduct a Self-Assessment (For Level 1 & Some Level 2)

Prepare for the Self-Assessment

For CMMC Level 1 and portions of Level 2, companies are allowed to conduct self-assessments.
This process involves evaluating your current cybersecurity posture using an internal review.

Tools for Self-Assessment

- Use the **CMMC self-assessment guides provided by 360 Advanced** to document compliance with the required practices.
- **Review** your access control policies, check that data encryption is properly applied, and verify incident response capabilities.
- **Submit the self-assessment results annually to the DoD** as required for maintaining Level 1 compliance.



Step 6: Schedule a C3PAO Audit (For Level 2 & Level 3)

Choose a C3PAO

For CMMC Level 2 and Level 3 certifications, an audit must be performed by an accredited C3PAO. A Third-Party Assessment Organization (C3PAO) is like the “personal trainer” who certifies your company’s cybersecurity readiness.

Prepare for the Audit

- Gather all required documentation to demonstrate compliance.
- Ensure that all policies, procedures, and technical controls are in place.
- Coordinate with the C3PAO to schedule an audit, either onsite or virtually, and prepare your team for interviews and system evaluations.

Step 7: Address Findings and Achieve Certification

Handle Audit Results

After the audit, the **C3PAO may provide you with findings** where improvements are needed. These are areas to fix before certification is granted. It's like receiving feedback from a coach on how to improve your form.

Achieve Certification

Once all gaps are addressed, submit evidence of your corrections.
The C3PAO will then issue a CMMC certification for the appropriate level, which is valid for three years (for Level 2 and Level 3).

Step 8: Maintain Your Certification

Ongoing Compliance

Cybersecurity is not a one-time effort; it requires ongoing maintenance. **Maintain your certification** by ensuring that cybersecurity practices are regularly reviewed and updated.

Monitor and Re-Assess

- Conduct internal reviews and self-assessments annually (for Level 1) or as needed to maintain compliance with changing standards.
- Re-certify with your C3PAO every three years (for Level 2 and Level 3).

CMMC Audit Pricing and Budgeting

Estimated Pricing for CMMC Level 2 Audit

- **Small Businesses** (up to 100 employees): $20,000 to $50,000
- **Medium Businesses** (100 to 500 employees): $50,000 to $100,000
- **Large Businesses** (500+ employees): $100,000 and upwards (CMMC Audit Pricing).

Factors Affecting Audit Costs

- **Company Size:** Larger companies with more complex environments face higher audit costs.
- **Scope of Audit:** The number of systems, facilities, and locations being assessed can increase costs.
- **Pre-Audit Preparation:** Companies that have done significant preparation (e.g., through gap analysis) may reduce their audit costs.

Additional Costs

- **Remediation Costs:** If security gaps are identified during the audit, fixing them could add significant expenses.
- **Monitoring & Re-Assessments:** Companies may also need to budget for continuous monitoring and potential re-certification in future years.

Conclusion

Stay Cyber-Ready

Achieving and maintaining CMMC compliance is essential to protect your company's contracts with the DoD. Cybersecurity is an ongoing process, and **360 Advanced is here to help your organization every step of the way**–from preparation to certification and beyond.

Partner with 360 Advanced for CMMC Success

360 Advanced provides the guidance, expertise, and tools to help your company navigate the complexities of CMMC certification.

Contact 360 Advanced today to start your journey toward CMMC compliance!

CMMC@360ADVANCED.COM

Candidate

COMPASS ROSE
BY 360ADVANCED