CYBERSECURITY MATURITY MODEL CERTIFICATION

The CMMC 2.0 Checklist

CMMC 2.0 (Cybersecurity Maturity Model Certification) is a U.S. Department of Defense compliance framework to enhance and maintain cybersecurity protection across the defense industrial base. The framework is designed to safeguard sensitive defense information, including controlled unclassified information (CUI), from sophisticated cyber threats including organized crime and nation-state attackers.

CMMC 2.0 aims to strengthen the entire defense supply chain, from large contractors to small suppliers by establishing a unified standard for cybersecurity practices and ensuring that all participants actively implement essential security measures.

Our checklist guides you through the process to achieve and maintain CMMC 2.0 compliance.

Comprehensive CMMC 2.0 Compliance Guide for DoD Contractors

1. Determine Your CMMC Level

Start by reviewing your DoD contracts to understand which CMMC level (1, 2, or 3) you must comply with. If it's unclear, reach out to your contracting officer for clarification.

The CMMC Levels are:

□ Level 1: Basic safeguarding for Federal Contract Information (FCI).

□ Level 2: Enhanced protection for Controlled Unclassified Information (CUI).

□ Level 3: Highest level of security for the most sensitive information, designed to counter advanced persistent threats (APTs).

2. Define Your Compliance Scope

□ Identify all systems, devices, and personnel handling sensitive DoD information. Segregate these from non-sensitive parts of your organization to simplify compliance and reduce costs. Smaller scopes are easier and cheaper to manage.

3. Conduct a Thorough Self-Assessment

□ Perform an internal assessment against the CMMC requirements using the NIST SP 800-171A controls. Document your findings, including strengths, weaknesses, and gaps. This honest evaluation will guide your compliance efforts.

4. Enhance Your Security Measures

□ Address identified gaps by implementing necessary security controls:

□ Use Strong Authentication and Access Controls: Implement multi-factor authentication (MFA) and compliant password policies to ensure that only authorized personnel can access sensitive information.

□ Invest in Advanced Security Tools: Acquire security software and hardware that adhere to NIST SP 800-171 standards. These should include firewalls, intrusion detection systems, anti-virus software, and secure communication tools.

□ Utilize FedRAMP Approved Cloud Services: Ensure your cloud service providers meet FedRAMP Moderate Baseline or equivalent standards. This ensures that cloud services have the necessary security controls to handle federal information securely.

□ Implement Regular Security Patches and Updates: Keep all software and systems up to date with the latest security patches to protect against vulnerabilities.

□ Ensure FIPS Compliance: If your organization handles CUI, you must use encryption that complies with Federal Information Processing Standards (FIPS) 140-2. This standard ensures that cryptographic modules used are tested and validated by approved independent laboratories. FIPS 140-2 compliance is a requirement for CMMC Level 2 and above. Your cryptographic modules must be CMVP validated to meet these standards.

Chainguard produces hundreds of FIPS Images, which have FIPS-validated cryptography automatically configured and enabled and we provide all security patching and updates. You can replace your existing containers with Chainguard FIPS Images to quickly address the FIPS and security patching requirements.

5. Develop Comprehensive Documentation

□ Create a System Security Plan (SSP) that details your security measures, IT systems, policies, and procedures. Regularly update this document to reflect any changes. You must also maintain a Plan of Action and Milestones (POA&M) to track and address security gaps. Templates from various organizations can provide a starting point for an SSP and POA&M tracking such as ComplianceForge.

6. Establish Continuous Monitoring

□ Set up systems and processes to monitor your security 24/7. Regularly check for vulnerabilities, update your software, and watch for unusual activity. Have a solid incident response plan to handle potential breaches efficiently.

7. Ensure Supply Chain Compliance

□ Review the security practices of your suppliers and subcontractors who handle DoD information. Include CMMC requirements in your supplier contracts to ensure their compliance obligations. Your security is only as strong as your weakest link.

8. Conduct Regular Training

□ Educate your employees on cybersecurity basics and specific threats to your organization. Use engaging training methods and make it an ongoing process. Regular training helps maintain a strong security culture and keeps everyone prepared for new threats.

9. Prepare for Third-Party Assessment

□ For Level 2 and 3 compliance, schedule an assessment with a Certified Third-Party Assessment Organization (C3PAO). Conduct internal audits and rehearsals to ensure your team is ready and your documentation is in order. The more prepared you are, the smoother the assessment will go. Several C3PAOs are listed in the Cyber AB Marketplace.

CMMC 2.0 should be achieved now!

The work doesn't stop here

10. Budget for Compliance

□ Allocate sufficient resources for compliance-related expenses, including new tools, training, and potential infrastructure upgrades. Treat this as an investment in securing future DoD contracts and protecting your business.

11. Plan for Incident Response

□ Develop and regularly update an incident response plan. Conduct drills to test your response capabilities and ensure everyone knows their role in case of a security incident. Being prepared helps minimize damage and recover quickly.

12. Foster a Security Culture

□ Make cybersecurity a priority across your organization. Encourage a culture of continuous improvement, where everyone understands their role in protecting sensitive information. Leadership support and employee engagement are crucial for success.

□ By following this comprehensive guide, your organization will be well-prepared to achieve and maintain CMMC 2.0 compliance. This process not only helps you secure DoD contracts, but also strengthens your overall cybersecurity posture. Stay committed, stay vigilant, and you'll build a robust defense against cyber threats.