Trustwave®

CMMC Readiness Accelerator

PREPARE FOR CMMC CERTIFICATION AND INCREASE SECURITY MATURITY

Benefits

- Access a team of Trustwave consultants with deep subject matter expertise in governance, risk, and compliance.
- Achieve greater visibility into the data assets you are responsible for securing.
- Identify security weaknesses and corrective actions for the CMMC requirements.
- Proactively protect your security investments from potential vulnerabilities.
- Ensure preparedness for upcoming visits from the assessors.
- Be ready to win government contracts requiring CMMC certification.

The U.S. Department of Defense (DoD) requires contractors and subcontractors to meet certain cybersecurity standards and announced the release of Cybersecurity Maturity Model Certification (CMMC) 2.0 as the new standardized program in November 2021. With the expected inclusion of CMMC 2.0 in contracts starting in 2025 it means that organizations must not only comply with these standards but also demonstrate their compliance effectively by getting certified at the appropriate level before a contract is awarded.

To meet the CMMC requirements, organizations need to address two fundamental questions:

1. Is your cybersecurity maturity at the level required to receive an award for the DoD contracts you are bidding on?
2. How can you implement and maintain compliance with these new best practices for managing cybersecurity?

The Trustwave CMMC Readiness Accelerator provides you with a roadmap to prepare your security programs for CMMC certification. Depending on the certification goal, Trustwave will provide guidance and remediation planning to help you align with the CMMC requirements.

Understanding the CMMC 2.0 Certification

CMMC is a DoD program to safeguard sensitive information that is shared by the DoD with its contractors and subcontractors. CMMC is designed to enforce protection of federal contract information (FCI) and controlled unclassified information (CUI) in alignment with DoD's information security requirements, while keeping the supply chain running safely. The National Institute of Standards and Technology (NIST) Special Publications (SP) 800-171 and 800-172 serve as the basis for these protection measures.

CMMC is codified as part of the Defense Federal Acquisition Regulation Supplement (DFARS) within the Code of Federal Regulations. The CMMC program is overseen by the Office of the Under Secretary of Defense for Acquisitions and Sustainment. The DoD has designated an independent non-profit organization, the Cyber AB, to manage the certification and accreditation process, which is at the core of CMMC. The DoD and the Cyber AB work together to implement the CMMC program from end to end.

The new CMMC 2.0 program has three levels of compliance:

- **Level 1 (Foundational):** Applies to organizations that focus on the protection of FCI. It includes 17 practices based on FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.
- **Level 2 (Advanced):** Builds upon Level 1 requirements to include 110 practices based on NIST SP 800-171, introducing additional practices to increase security maturity. This level has additional requirements to ensure the protection of the two types of CUI data – prioritized and non-prioritized.
- **Level 3 (Expert):** Builds upon Level 2 requirements to introduce an additional subset of practices based on NIST SP 800-172, intended to protect CUI from advanced persistent threats (APTs).

The Approach

Trustwave will produce a roadmap for you to prepare for CMMC certification and increase security maturity, and can adopt a modular approach to address your specific requirements for CMMC certification:

1. **Requirements Gathering:** Trustwave works with you to outline the CMMC requirements and identify the in-scope systems based on the compliance level (i.e., 1, 2, or 3). This includes reviewing CMMC documentation, guidelines, and practices, and identifying in-scope systems and processes.
2. **Gap Analysis:** Trustwave conducts a gap analysis to identify weaknesses or deficiencies in your current security programs. This includes reviewing existing system security plan (SSP), policies, procedures, and technical controls, and identifying areas that need improvement.
3. **Roadmap Development:** Trustwave works with you to develop a prioritized roadmap tailored to your needs, based on the findings from the gap analysis. This includes developing recommendations for addressing identified gaps and identifying controls and processes to meet the CMMC requirements.

Implementation Support: Trustwave can also help you implement changes to your security in alignment with the CMMC requirements. Implementation services may include implementing the corrective actions from the roadmap or any other activities that you are looking to implement to increase your security maturity. We can also work with you and relevant third parties to conduct a 'mock' CMMC assessment (i.e., pass or fail) in preparation for your certification.

Access to the CMMC Readiness Tool

Trustwave is a Registered Practitioner Organization (RPO) with the Cyber AB. As an RPO, we have access to the CMMC Readiness Tool (CRT) from the Cyber AB.

Key benefits of the CRT for the CMMC Readiness Accelerator:

- Ensures that the evaluation is conducted using the tool provided directly by the CMMC accreditation body.
- Provides an effective way to manage CMMC compliance gaps and remediation activities, including ownership and responsibilities.
- Enables effective information sharing with relevant auditors, C3PAOs, governing bodies, and other appropriate stakeholders.
- Saves time and resources by streamlining the review and analysis process.
- Provides advanced dashboarding capabilities, demonstrating trends and progress over time.

Microsoft & CMMC

Trustwave is endorsed and validated by Microsoft as a leading cybersecurity partner.

Microsoft provides a Microsoft Sentinel CMMC solution, which empowers governance and compliance teams to design, build, monitor, and respond to CMMC requirements across cloud, on-premises, hybrid, and multi-cloud workloads. The solution contains: 1) workbook, 2) analytics rules, and 3) playbooks.

Trustwave can help you enable CMMC reporting in Microsoft Sentinel via the Trustwave Accelerator for Microsoft Sentinel service. This service provides you with a roadmap to accelerate value and security outcomes from Microsoft Sentinel.

Build, Test, & Run a Secure Organization

Trustwave's range of capabilities help you get the right service to suit your specific needs, including:

Cyber Advisory Services:

- Digital Forensics & Incident Response
- Threat Detection & Response
- Data Protection
- Governance, Risk, & Compliance
- Security Colony
- Technology Partnerships
- Executive Training
- Tactical Training

Security Testing Services:

- Penetration Testing (Network, Application – Internal, External, Wireless)
- Vulnerability Scanning (Discovery, Network, Application, Database)
- Red/Purple Teaming
- Intrusion Detection & Prevention
- Database Security (DbProtect, AppDetectivePRO)
- Secure Email & Web Gateways
- Physical Assessments

Managed Security Services:

- Managed Threat Detection & Response
- Co-Managed SIEM/SOC
- Security Technology Management
- Managed Web Application Firewall
- Proactive Threat Hunting
- Security & Compliance Bundles
- Managed Application Control

Trustwave®

www.trustwave.com