



Accelerate Compliance with AWS CMMC Enclave

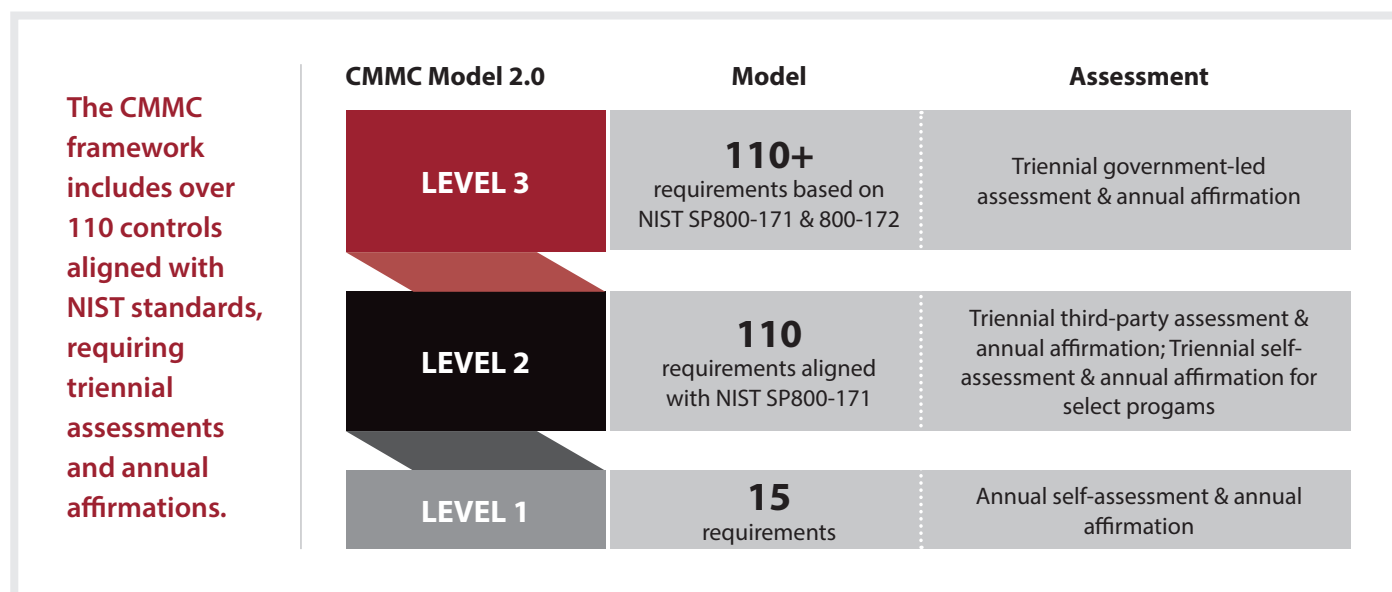
To strengthen cybersecurity across the Defense Industrial Base, the DoD introduced Cybersecurity Maturity Model Certification (CMMC) — ensuring organizations that handle CUI meet NIST 800-171 and 800-172 standards. Compliance is no longer optional—it is a critical requirement for maintaining contracts and securing sensitive data.

Minimize the Attack Surface with AWS CMMC Enclave

As a Registered Practitioner Organization (RPO), Red River offers a comprehensive approach to help organizations achieve and maintain CMMC compliance with confidence leveraging a CMMC enclave. Red River partners with AWS to deliver a CMMC enclave that is a secure, isolated cloud-based environment designed to handle CUI within a defined boundary. It builds upon existing compliance foundations to streamline implementation. Adopting this method minimizes the attack surface, making data storage and processes completely inaccessible outside of the enclave.

Key Aspects of Our Offering:

- **Strategic Assessment & Alignment:** In-depth analysis of current infrastructure to develop a migration strategy that supports organizational goals.
- **AWS Landing Zone Deployment:** Deploy customized Landing Zone based on AWS LZA (Landing Zone Accelerator).
- **Deploy CMMC 2.0 Level 2 Configurations:** Deploy CMMC 2.0 Level 2 controls on root account.
- **Review & Remediate Findings:** Automatic remediation of findings to support CMMC 2.0 Level 2 compliance.
- **Reporting:** High-level compliance reports.
- **Documentation & Knowledge Transfer:** Provide best practices including an overview of the deployed environment.



Streamlining Cybersecurity Programs with Enclaves

Enclaves offers an isolated, hardened and highly constrained environment to host security-critical applications. Along with easing the assessment efforts, these encrypted black boxes can replace outdated cybersecurity programs.

Key benefits include:

- **Built-In Governance:** Governance is built-in at the foundation, enabling organizations to adapt to constantly changing compliance programs.
- **Identification of Security Gaps:** Reporting capabilities that show compliance level and identify any gaps within the enclave.
- **Reduced Costs:** Secure enclaves typically reduce the implementation costs associated with broad data protection strategies.
- **Ability to Meet C3PAO Requirements:** A streamlined ability to use the inherent tools and reporting capabilities to satisfy a C3PAO during assessment.
- **Faster Deployment:** Repeatable and consistent build templates allow for a more efficient deployment.

Red River is a trusted partner with deep knowledge of DoD requirements and proven experience building compliant enclaves while automating deployments. To accelerate your compliance journey and get more information about the AWS CMMC Enclave, contact us info@redriver.com.



ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing more than 25 years of experience and mission-critical expertise in managed services, AI, cybersecurity, modern infrastructure, collaboration and cloud solutions.

Learn more at redriver.com.