CMMC Mock Assessment Services

augustschell

Validate & Prove Your Readiness for CMMC Certification Before it Counts

Preparing for a Cybersecurity Maturity Model Certification (CMMC) assessment requires organizations to demonstrate that required cybersecurity practices are not only documented but fully implemented and operational. August Schell delivers structured non-certification "mock CMMC assessments" aligned to formal certification methodologies enabling Defense Industrial Base (DIB) organizations to identify gaps, reduce assessment risk, and avoid costly delays or certification failure prior to SPRS scoring and CMMC eMASS submission.

Our Assessment Methodology

Our mock assessments follow a structured five-step process aligned with CMMC program guidance & assessment standards.

1. **Assessment Planning**
   Define scope, schedule, and required documentation.
2. **Documentation Review**
   Evaluate the System Security Plan and supporting artifacts.
3. **Technical Evaluation**
   Examine implementation of required security practices.
4. **Personnel Interviews**
   Validate operational processes and control effectiveness.
5. **Assessment Reporting**
   Document findings and certification determination.

CMMC Level 2 Mock Assessments

Our mock assessments align with the 110 security requirements in NIST SP 800-171 Rev. 2 (32 CFR Part 170). We evaluate your scoped environment to determine whether implemented controls demonstrate the objective evidence and operational effectiveness expected during a formal certification assessment.

- ✓ Review of System Security Plan (SSP) & supporting documentation
- ✓ Examination of implemented security controls & configurations
- ✓ Review of policies, procedures, & technical artifacts
- ✓ Interviews with personnel responsible for security operations
- ✓ Evaluation of objective evidence demonstrating security practices

OUTCOME: Control-by-control determination of gaps that may result in findings during a formal CMMC assessment.

Level 3 Enhanced Mock Assessment – NIST SP 800-172

Organizations pursuing Level 3 must first hold Final Level 2 (C3PAO) status (32 CFR § 170.18). Level 3 adds 24 enhanced requirements from NIST SP 800-172, targeting Advanced Persistent Threats (APTs) — bringing the total to 134 requirements. Formal certification is conducted exclusively by DCMA DIBCAC, making mock preparation especially valuable.

- ✓ Prerequisite check: confirmation of Final Level 2 (C3PAO) CMMC Status for the applicable scope
- ✓ Level 3 scope boundary review per 32 CFR § 170.19(d), including CRMA and Specialized Asset treatment
- ✓ Review of Organization-Defined Parameters (ODPs) as required by NIST SP 800-172
- ✓ Evaluation of 24 enhanced controls targeting Advanced Persistent Threats (APTs)
- ✓ Level 3 SSP documentation review and eMASS readiness for DCMA DIBCAC submission

OUTCOME: Structured evaluation of readiness for DCMA DIBCAC assessment, identifying gaps across all 134 combined Level 3 security requirements.

CMMC Mock Assessment Services

Evidence & Documentation Review

CMMC assessments require organizations to demonstrate objective evidence showing controls are implemented and functioning as intended.

- ✓ Review of control implementation evidence
- ✓ Examination of policies, procedures and supply chain flow down practices
- ✓ Identification of missing or incomplete artifacts
- ✓ Validation of documentation alignment with assessment objectives

OUTCOME: Improved visibility into the documentation and evidence that will be evaluated during certification assessments.

Assessment Interviews & Operational Walkthroughs

Personnel interviews are a key component of CMMC certification assessments. Mock interactions help organizations understand how operational cybersecurity practices will be evaluated.

- ✓ Structured interviews with key personnel
- ✓ Walkthrough of operational security procedures
- ✓ Review of incident response, access control, and monitoring processes
- ✓ Validation of how security controls operate in practice

OUTCOME: Organizations gain clarity on how operational processes will be evaluated during certification assessments.

Mock Assessment Report

At the conclusion of the engagement, organizations receive a structured report aligned with assessment expectations.

- ✓ Summary of evaluated security practices
- ✓ Identification of findings that may qualify as allowable POA&M items vs. those requiring remediation prior to formal assessment
- ✓ Documentation of reviewed evidence
- ✓ Assessment observations aligned with NIST SP 800-171 & 800-172 security requirements

OUTCOME: Consolidated view of the organization's current alignment with CMMC assessment expectation.

Standards Alignment

- ✓ NIST SP 800-171 Rev. 2
- ✓ DFARS 252.204-7012 safeguarding requirements
- ✓ 32 CFR Part 170 (CMMC Program Rule)
- ✓ DFARS 252.204-7021 (CMMC Requirements Clause)
- ✓ NIST SP 800-172 —24 enhanced Level 3 requirements
- ✓ NIST SP 800-172 —24 enhanced Level 3 requirements

Important Notice

Mock assessments are non-certification assessments and do not result in the issuance of a CMMC certification or status determination. Certification assessments must be conducted by an authorized and independent CMMC Third-Party Assessment Organization (C3PAO) in accordance with CMMC program requirements.

Conflict of Interest Notice

August Schell operates as both a CMMC RPO (advisory/consulting) and an authorized C3PAO (certification assessments). In accordance with Cyber AB accreditation requirements, August Schell is prohibited from conducting a CMMC Level 2 certification assessment for any organization it has provided consulting or remediation services to within the preceding three years. Affected organizations must obtain certification from an independent C3PAO.

Schedule a Mock Assessment

Contact August Schell to learn how a mock assessment can help your organization better understand its readiness for CMMC certification.

cmmc@augustschell.com | www.augustschell.com | 301838.9470