

CMMC COMPLIANCE & OPERATIONS FOR THE DEFENSIVE INDUSTRIAL BASE

Corporate Overview

Our firm specializing in CMMC assessment remediation for the defense industrial base. We evaluate contractor environments against all NIST SP 800-171 controls, close compliance gaps, and build the defensible evidence C3PAOs require for certification.

We do not just prepare organizations for assessment. We stay engaged as the technical liaison throughout the entire process, from first gap assessment to post-certification compliance management - ensuring your organization becomes and remain compliant.

Company Data

UEI: M18VJDQNP8V9

CAGE: 9SP27

Industry Certifications

CISSP, CISM, CISA, CAP, CCSP, CISM, CISA, CHFI, CTIA, CEH, PMP

Contact Information

cmmc.ready@ikaanconsulting.com

Clients



Core Competencies

- Readiness Assessment
- NIST SP 800-171 Gap Analysis
- SPRS Scoring and Score Improvement Planning
- Plan of Action and Milestones (POA&M)
- System Security Plan (SSP) Development
- Remediation Roadmap and Execution
- 24/7 Security Operations Center (SOC)
- Managed Detection and Response (MDR)
- Vulnerability and Patch Management
- Continuous Compliance Monitoring
- C3PAO Assessment Liaison and Technical Support
- vCISO Advisory Services

CMMC Service Lifecycle

01

Rapid CUI Scoping

Assess CUI scope and security posture to focus compliance efforts.

02

CMMC Gap Assessment

Baseline your cybersecurity readiness and map processes to CMMC controls.

03

Remediation, Artifacts & Audit Prep

Remediate gaps, draft policies, and train teams to meet CMMC standards.

04

Continuous Support & Maintenance

Sustain compliance, strengthen resilience, and adapt to shifting threats.

CMMC COMPLIANCE & OPERATIONS FOR THE DEFENSIVE INDUSTRIAL BASE

Engineering and Logistics Contractor

Federal consulting & solution provider | Founded 2017 | 2 facilities

CMMC L2

Challenge	Approach	Outcome
Active Army contract with a CMMC requirement. Outdated cybersecurity program and no dedicated IT staff. A 10-person client team running a hands-on logistics business needed an auditor-ready program that would not overwhelm daily operations.	Right-sized the path: self-assessment, minimal CUI footprint, milestone-based pricing tied to SPRS score gates. Hands-on technical enablement on Nessus, OpenSCAP, PowerShell CMMC scripts, and WatchGuard, transferring capability to the client team rather than holding it.	Lean CUI architecture stood up: 10 encrypted laptops, segregated Wi-Fi, GCC subdomain for CUI mail. Full policy suite drafted by the client with Ikaan review. SSP and POA&M. SPRS submission of 92-110 on track ahead of November 2026.

IT & Cybersecurity Contractor

Federal consulting & cybersecurity provider | Founded 2019 | 1 facility

CMMC L2

Challenge	Approach	Outcome
Active Navy contract with a CMMC requirement. A 2-person client team managing IT program management contract needed an auditor-ready program to ensure they maintain prime contractor status.	Standardized policies and procedures, full hardware re-inventory with on-site validation, and migration to CMMC-compliance MSP/MSSP technology stack.	MSP/MSSP transition complete. Clean CUI architecture: 2 dedicated workstations on an isolated VLAN, GCC for email and storage, USB blocking, no physical media. Auditable evidence in place across change, incident, and log management.