

DEFENSE / MANUFACTURING

CERTIFIED

Achieving CMMC Compliance: A Defense Contractor's Certification Journey

CMMC CERTIFICATION | Certification required to retain existing defense contracts

01 Engagement Overview

A defense subcontractor supporting prime contractors on multiple active awards faced a certification requirement tied directly to contract eligibility, with no formal cybersecurity program in place beyond basic IT hygiene.

- Scope: Full environment covering controlled information handling, access management, and incident response practices across the contractor's network
- Approach: Gap assessment against required practices before building a remediation roadmap, rather than attempting certification directly
- Baseline: No documented security policies, ad hoc access controls, and no formal incident response process

02 Technical Discovery

The gap assessment surfaced foundational gaps that are common across small and mid-sized defense subcontractors who have relied on informal IT practices.

- Mechanism: Controlled information was stored alongside general business data with no separation or access restriction based on role
- Scope: Multi-factor authentication was inconsistently applied, active on some systems and absent on others depending on when they were provisioned
- Why it mattered: Without documented policies, the organization had no way to demonstrate that informal practices were consistently followed, which is a certification requirement in itself

03 Risk & Business Impact

The risk here was not a breach. It was losing eligibility to bid on and retain the contracts the business depended on.

- Missing certification would have disqualified the contractor from renewal on its largest existing award
- Standards exposure: Gaps spanned multiple control families, meaning a narrow fix would not have been sufficient to pass assessment
- Undocumented practices meant the organization could not prove compliance even where the underlying behavior was reasonable, turning a documentation gap into a certification blocker

04 Remediation & Outcome

Remediation focused on closing control gaps and building the documentation required to demonstrate compliance, not just achieve it technically.

- Implemented consistent multi-factor authentication and role-based access control across all systems handling controlled information
- Established formal, documented security policies covering access control, incident response, and system configuration
- Built an incident response plan and ran a tabletop exercise to validate it before assessment
- Achieved certification ahead of the contractor's renewal deadline, preserving eligibility on its existing awards