CLARK SCHAEFER
CONSULTING

CASE STUDY

CMMC Compliance Journey for Aerospace and Defense Manufacturer

Context

The customer, a renowned aerospace and defense manufacturing company, has been a trusted supplier of military equipment and aircraft products for many years. Registered under the International Traffic in Arms Regulations (ITAR), the company develops Controlled Unclassified Information (CUI) systems for the Defense Industrial Base (DIB). They have approximately 250 employees and an annual revenue of $18 million, with 70% of that coming from government contracts. They faced new challenges in meeting the Cybersecurity Maturity Model Certification (CMMC) requirements, which are set to become mandatory for defense contractors by 2025.

Challenges

The company was initially uncertain about where to start or how to approach the CMMC requirements. Leadership sought external guidance to gain a clearer understanding of CMMC, its implications, and the necessary steps for compliance. They explored several options, as the chart below outlines the pros, cons, and potential outcomes of each approach.

Alternative	Pros	Cons	Outcome
MSP	Handles most IT-related needs	Lack of CMMC knowledge, would need to learn CMMC before educating the organization	Not a fit
Online Resources (YouTube, Webinars)	Low cost, wide range of information	CMMC more complex than anticipated, time-consuming, lack of tailored guidance	Insufficient
Clark Schaefer Consulting	Prior positive experience, CMMC expertise, tailored approach	Requires investment of time and budget for tailored solutions	Selected: Leadership gained confidence in understanding CMMC, resulting in a signed project proposal due to Clark Schaefer Consulting's expertise, offerings, and approach

SOLUTION

After considering the alternatives, the leadership team chose to work with Clark Schaefer Consulting due to its expertise, positive reputation, and tailored approach to meet their CMMC needs. The solution was divided into three phases:

Phase 1: Risk Assessment (Gap Analysis)	**Phase 2:** Remediation	**Phase 3:** Ongoing Maintenance & Preparation
• Assess the organization's current level of CMMC compliance and identify gaps. • Develop essential documentation, including the System Security Plan (SSP), Plan of Action and Milestones (POA&M), and a Shared Responsibility Matrix (SRM).	• Define the scope of the CUI environment for assessment. • Address compliance gaps, such as misconfigurations and access control, and implement necessary security measures. • Acquire needed equipment (e.g., security cameras, software), conduct user awareness training, and establish policies and procedures to support CMMC compliance.	• Prepare for the official CMMC assessment while managing budget constraints through phased work. • Ensure the MSP is fully aligned and prepared to support ongoing compliance efforts.

Implementation and Timeline

The project was launched in March 2024, and by May 2024, the company had completed Phase 1 meeting 60% of the assessment objectives and increased its Supplier Performance Risk System (SPRS) score. Ongoing efforts included further enhancing the score and preparing for a mock assessment scheduled for Q3/Q4 2025.

MARCH 2024	APRIL 2024	MAY 2024	JUNE 2024	JULY 2024	AUGUST 2024	SEPTMEBER 2024	OCTOBER 2025
Project initiation focused on identifying gaps and setting initial goals for compliance.		Completion of Phase 1. The company met 60% of assessment objectives, achieving an SPRS score of -10.				The company aims to reach an SPRS score of 60 by the end of Q3, moving closer to the required 88/110 threshold for government project eligibility.	A mock assessment is set to take place as a preparation step for the official CMMC assessment. This pre-assessment will identify any final adjustments needed for full compliance.

NEXT STEPS

To achieve the target score of 60 by **Q3 2024**, the company focused on the following areas:

- **Data Classification:** Identified and contained CUI and ITAR data.
- **Access Controls:** Restricted data access using Role-Based Access Controls (RBAC).
- **Documentation and Evidence Collection:** Developed necessary documentation and gathered evidence to support compliance.
- **Configuration Updates:** Deployed security-related configuration changes, such as Network Time Protocol (NTP) and local admin access.
- **User Training:** Conducted security awareness training for employees.
- **Technology Upgrades:** Implemented new solutions, including firewall enhancements, antivirus, Security Information and Event Management (SIEM), and keycard access.

Results

Clear Roadmap: Established a detailed roadmap to full compliance with clear next steps outlined.

Scoping Approach: Defined an enclaving strategy to limit assessment scope and reduce costs effectively.

Improved Score: Achieved a higher score, bringing the company closer to the 88/110 threshold. This progress positions them to continue government projects while remediating remaining requirements within 6 months.

Mock Assessment: Scheduled a mock assessment ahead of the official CMMC Assessment in Q3/Q4 2025.

Cost Efficiency: Ensured efficient allocation of funds and resources to support compliance solutions.

Customer Satisfaction: Attained high customer satisfaction, with the client expressing appreciation for CSC's work and the foundation for a strong long-term partnership.

Benefits Gained by the Customer

Established a Compliance Roadmap: Defined clear steps toward full CMMC compliance.

Protected Revenue: Preserved critical government contracts constituting 70% of revenue.

Reduced Costs: Streamlined focus on essential areas through a defined scoping approach.

Enhanced Security: Improved DoD Assessment Score, strengthening security practices.

Boosted Confidence in Compliance: Increased assurance in achieving full compliance by the 2025 deadline.

Positioned Strategically: Enabled the company to share progress with primes and subs, driving new opportunities and revenue growth.

Prepared for Tangible ROI: Strategically set up for long-term growth as noncompliant competitors were eliminated.

Adjusted Pricing: Positioned to raise prices, as encouraged by the DoD, to offset compliance costs.