

CASE STUDY: DEVELOPING A REPEATABLE METHODOLOGY TOWARD CMMC COMPLIANCE

SITUATION

Edwards Performance Solutions (Edwards) was a true early adopter and thought leader in the Cybersecurity Maturity Model Certification (CMMC) ecosystem. However, Edwards needed a formal Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessment to be able to handle Controlled Unclassified Information (CUI) and conduct assessments as a CMMC Third-Party Assessment Organization (C3PAO) – maintaining its ethos as an industry educator (as an active LTP and LPP) and consulting/assessment powerhouse.

When Sam Bell, Edwards' Chief Information Security Officer (CISO), began preparing for Edwards' formal assessment, he worked with the team to design an internal assessment tool that tracks the alignment of Edwards security posture to meet CMMC compliance requirements. This was prior to the formal CMMC assessment guides being released, providing the team an advantage in preparing for CMMC.

The pivot from CMMC 1.0 to CMMC 2.0 demanded Edwards show its agility by swiftly adapting to the updated CMMC scoping guidelines, including changes to the CUI Data Flow Diagramming templates to reflect additional scoping requirements. This diagramming process enabled Edwards to successfully defend its system scope with the DIBCAC assessors, as all flows of CUI and Federal Contract Information (FCI) were clearly identified. Overall, the team's structured approach to CMMC readiness allowed for a quick realignment to CMMC 2.0 requirements.



SOLUTION

Edwards leveraged its years of project management expertise to architect its Government Community Cloud (GCC) High Enclave for use as a C3PAO environment. Edwards' project management skills ensured this project remained focused to meet all CMMC Level 2 compliance requirements.

Edwards internal Subject Matter Experts (SMEs) have numerous years of experience conducting security control assessments and making recommendations to improve organizational security. They employed this knowledge by documenting the CMMC controls and recommending security solutions to maintain compliance. Edwards developed a System Security Plan (SSP), policies, procedures, data flow and network diagrams, as well as other forms of documentation, which together govern their cybersecurity program and prove CMMC compliance.

“

I couldn't be more proud of the team. They followed a structured approach, to evaluating, documenting, and demonstrating our CMMC compliance to the DCMA DIBCAC assessors.

As a result of their keen focus, CMMC understanding, and strong process background founded in ISO 9001 and CMMI, they were able to pass both the DIBCAC scoping and assessment on the first try!

This also makes Edwards the only organization who supports the entire CMMC ecosystem.

”



Sam Bell

Chief Information Security Officer (CISO)
Edwards Performance Solutions

SOLUTION | CONTINUED

Based on this firsthand experience, Edwards determined the key to preparing for a smooth DIBCAC (or C3PAO) assessment is to ensure all assessment objectives are met in the documentation, with the proper evidence to support the objectives, and a team ready to demonstrate how the practices are in place, ensuring the assessor have no trouble marking each practice and practice objective as met.

Edwards utilizes this experience and expertise to support Defense Industrial Base (DIB) clients prepare for CMMC certification and conduct formal CMMC assessments.

RESULTS



Built a Data Flow Diagram to successfully map the flow of FCI, CUI, and other confidential data to ensure the scope is accurate and concise.



Built a SSP to address the 110 CMMC practices, linking to supporting documentation to further satisfy other requirements. This established environment expertise to effectively navigate and demonstrate implementation of the practices.



Completed the DIBCAC assessment ahead of schedule and recommended for C3PAO status to The Cyber AB. Edwards now leverages this experience to enhance the assessment experience and preparation for other organizations.