Gray Analytics

SUCCESS STORIES

Building a Practical Roadmap to Compliance from the Ground Up

The Situation

A regional construction company needed our help to assess its corporate IT services and identify current gaps to the upcoming Cybersecurity Maturity Model Certification (CMMC) requirements for Department of Defense (DoD) contractors. The client will be pursuing DoD contracts soon and will need to be compliant with CMMC once it is required. We were asked to help the client understand how it currently measures up to the expected minimum standards for CMMC and what it should address immediately to best prepare for upcoming requirements.

The Challenge

We discovered a lack of documented IT policies and procedures as well as limited to no recorded systems architecture or IT inventories, all of which created substantial risk for the client, contributed to a lack of consensus across the company related to policies and procedures, and signaled that work needed to be done to prepare for the upcoming CMMC requirements. Specifically, we discovered:

- Lack of company cybersecurity policies and guidelines, which made effective governance almost non-existent and created confusion among staff and the client's third-party IT services provider about actual company policies and procedures;
- No dedicated, in-house IT technical representative, which made it difficult and time-consuming for our team to track down and assess IT policies and decision-making processes; and
- Lack of recorded systems architecture and IT inventories, which limited our team's ability to assess the risks and potential impact of failed control systems.

Key Successes

We helped our client add clarity and formality to its IT operations and start working toward a more secure and compliant operating environment. Our assessment illustrated the urgent need to formalize policies and procedures so that employees and third-party vendors understand guidelines and expectations. We were also able to offer implementation services of our recommendations in the future. Thanks to our team, our client is well on its way to being prepared for its eventual CMMC requirements.

Our Solution

We relied on extensive personnel interviews to piece together a complete picture of the client's corporate and third-party IT and cybersecurity environment since existing documentation was limited. This allowed us to better understand how decisions were made and ad-hoc policies were created, however informal they may have been. From there, we were able to assess where and how efforts needed to be prioritized to formalize policies and procedures to prepare for CMMC.

The Outcome

We developed a complete operational picture of the client's IT environment and used that to assess the client against the CMMC controls. Numerous non-compliant findings were highlighted that we used to educate the client on effective and practical cybersecurity measures to implement for the better protection of Controlled Unclassified Information (CUI) and corporate intellectual property. We then developed an initial road map for preparing to achieve CMMC compliance once required. We made practical cybersecurity recommendations to help streamline and improve the client's overall IT operations and security.