KTL Solutions is proud that we were chosen to help guide Redspin on their trailblazing journey to become the first authorized C3PAO on the CMMC-AB's Market Place. This case study examines the challenges, processes and outcome of the Redspin project.

Challenges

Redspin's goal was to become a CMMC Third Party Assessor Organization (C3PAO). A C3PAO is an assessor that performs the Cybersecurity Maturity Model Certification (CMMC) assessment. The Department of Defense (DoD) introduced this measure to ensure that the Defense Industrial Base (DIB) strictly controls cybersecurity, with an extra layer of accountability.

Redspin, a division of CynergisTek, is a cybersecurity company focused on helping their clients build an approach to cybersecurity and privacy that responds every day through IT security assessments and consulting services. They provide cybersecurity consulting using various frameworks including NIST CSF, ISO 27001, and PCI DSS and wanted to expand their service offerings by becoming a CMMC assessor. The challenges to becoming a CMMC C3PAO included:

- CMMC is a new framework established for government contractors concerning cybersecurity.
- Serving both government contractors and business customers, Redspin would have to create a secure enclave to protect Controlled Unclassified Information (CUI).
- Redspin associates primarily work remotely, creating another layer of security needed to protect their network and devices.

Processes

Redspin had internal security policies and procedures in place before coming to KTL for assistance. However, these policies and procedures did not meet CMMC requirements. Redspin began a self-assessment in mid 2020 to define which areas needed to be addressed. This allowed Redspin to document revisions and updates to organizational policies and procedures over time, which illustrated the maturity aspect of CMMC that Redspin continues today.

KTL Solutions began working with Redspin in late 2020 to help create a secure enclave to support their remote workforce. The first step was to determine the scope of the engagement and the assessment environment.

- As a CMMC Registered Provider Organization (RPO), KTL is authorized to guide our clients through the CMMC Preparedness process.

Creating a secure enclave for Redspin was necessary to support the remote workforce. A secure enclave has advantages and disadvantages. An advantage is the ability to limit data access to only those who have a verified reason for accessing Controlled Unclassified Information) CUI. A disadvantage is that a secure enclave requires internet access 100% of the time in order to function.

- As a Microsoft Gold Partner, KTL implements Azure Cloud solutions for clients requiring cloud security. The Microsoft Shared Responsibility Model transfers responsibilities to Microsoft for items like physical security domains and maintenance domains in datacenters.

Outcome

The KTL project with Redspin including all preparation for the CMMC-AB assessment took over six months. The CMMC-AB announced that Redspin became the first C3PAO on June 9, 2021.

Lessons learned:

- Organizations preparing for a CMMC assessment must ready their *entire team* for interviews. The first person interviewed at Redspin was not the CISO, but rather the VP of Marketing. She was ready to answer questions about the handling of information because she had been included in the CMMC preparedness process.
- Redspin brought in a third-party provisional assessor to evaluate their CMMC preparedness. However, even with this extra layer of attention, organizations may face challenges during the CMMC assessment and will need to adjust quickly. Ensuring that an RPO, in this case, KTL, was in the background helping the team make the adjustments quickly or risk losing their place in line for the assessment led to their success in becoming the first C3PAO.

"KTL was instrumental in helping us navigate the requirements of GCC High. Their support and expertise played a part in our success of becoming the first Authorized C3PAO." *–Thomas Graham, PhD, Vice President & CISO of Redspin*