Diligent | Defense Contractor

Defense Contractor Closes GRC Gaps and Gains Executive Visibility Into Risk Exposure

Company: Defense Contractor

Industry: Government

THE ORGANIZATION STANDARDIZED THEIR BUSINESS PROCESSES AND GAINED GREATER EXECUTIVE-LEVEL VISIBILITY INTO RISK.

Despite their track record of success in delivering end-to-end solutions for collecting, processing and understanding sensor data, a leading defense contractor had significant gaps in several key areas related to governance, risk and compliance (GRC). Like many organizations, they had resorted to leveraging a manual spreadsheet process for risk assessments, which made it nearly impossible to scale coverage and to report on assessment results. The lack of automated reporting capability made it difficult for leadership to get a true picture of the status of risks being tracked, and the vulnerability management team had no mechanism to drive accountability and timely remediation of problems.

They also had difficulty demonstrating how their GRC strategy incorporated into required policies, procedures and controls. Additionally, as a government contractor, they had a number of federal mandates and standards to meet—including NIST 800-171.

SOLUTION

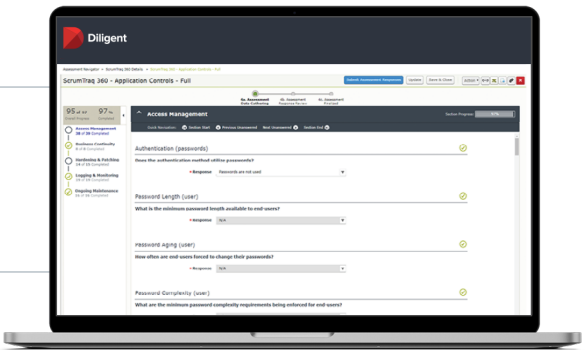


Figure 1: Harmonized common control framework.

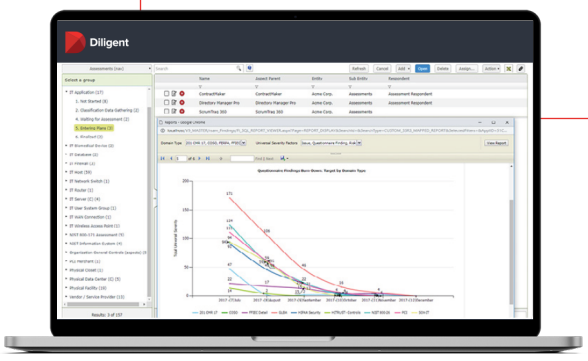
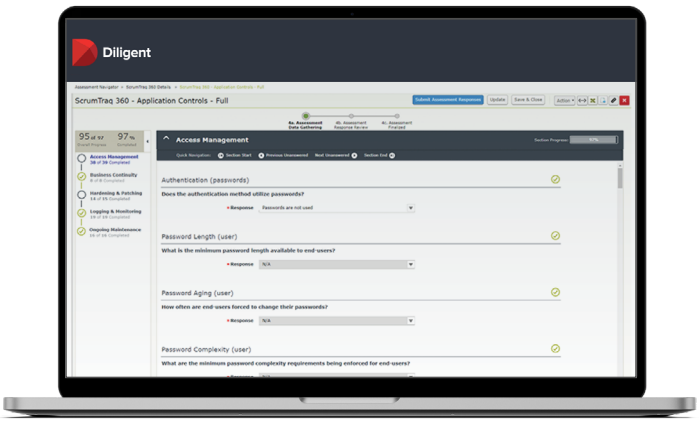


Figure 2: Organized findings by domain.

Diligent

Defense Contractor



The organization turned to Diligent for help reaching two primary goals: standardizing their business processes, and gaining greater executive-level visibility into areas of risk exposure. The solution needed to be cloud-based, meet strict GovCloud security requirements, and provide the flexibility and the diversity needed to manage various functional work processes with consolidated views of risk information.

To meet these goals, they implemented HighBond solutions, including:

IT Risk Management: The organization used the harmonized content to create a common control framework. This allowed them to sync upstream policies and procedures with downstream risk assessment and other monitoring activities. They automated NIST 800-171 assessments using IT Risk Management's flexible records-based assessment question library.

Threat and Vulnerability Management: By using the out-of-the-box integration with Tenable Security Center, the organization increased management visibility into open vulnerabilities and enabled timelier remediation by IT personnel. HighBond's flexible data model helped the organization ensure a legal basis within all of the organization's policies, procedures, standards, controls, and assessment activities.

RESULTS

Implementing these HighBond solutions created several quick wins. The organization now has a centralized framework that eliminates process redundancies, removes legal and control coverage guesswork, aligns teams to a better work quality, satisfies audit requirements, and accommodates easy onboarding of future regulatory initiatives without the need for process reengineering. They also gained an automated risk assessment methodology that satisfies audit requirements, aligns with an industry-leading common control framework, and enables risk teams to more easily analyze risk exposure and identify systemic control improvements.

The security team has a system of accountability in place that enables them to track the aging of vulnerabilities and remediation against service-level targets.

The company also has a central place to track ad hoc risks identified through various means, and create leadership awareness for proper risk treatment. The days of manually tracking and reporting with spreadsheets are thankfully behind them.

For more information or to request a demo, contact us today:
Email: info@diligent.com | Call: +1 877 434 5443 | Visit: diligent.com