

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



## Situation Summary

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. Like many organizations, they had resorted to leveraging a manual spreadsheet process for risk assessments, which made it nearly impossible to scale coverage and 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.

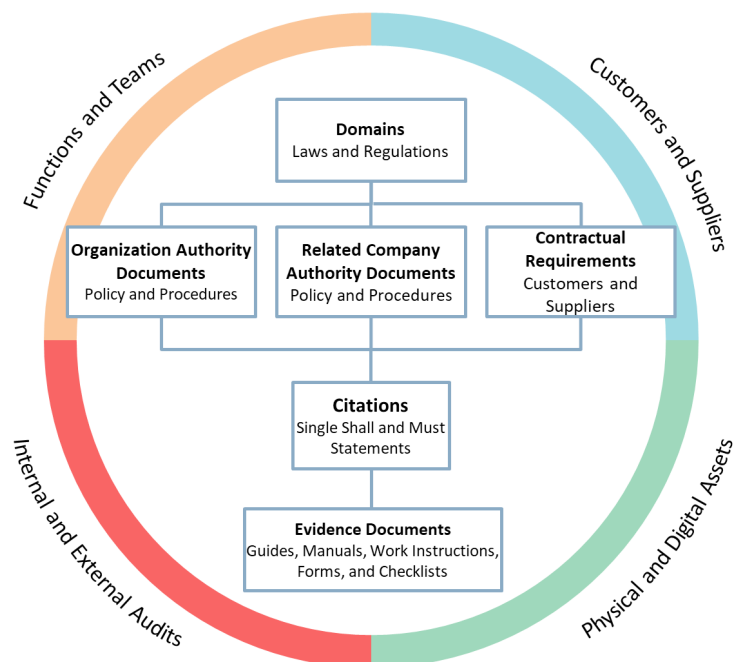
They also had difficulty demonstrating how their GRC strategy incorporated into required policies, procedures, and controls. Additionally, as a government contractor, they had a number of federal mandates and standards to meet—including NIST 800-171.

## Solution

The organization turned to Rsam 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, Rsam implemented several modules, including:

- **UCF Connector:** They leveraged their UCF subscription and Rsam’s UCF connector to provide the organization a common control framework. This allowed them to synch upstream policies and procedures with downstream risk assessment and other monitoring activities.
- **Risk and Compliance Assessments:** They also automated NIST 800-171 assessments using Rsam’s flexible records-based assessment question library.
- **Vulnerability Management:** By implementing Rsam’s integration with Tenable Security Center, the organization increased management visibility into open vulnerabilities and enabled timelier remediation by IT personnel.
- **Risk Register:** The organization now uses this Rsam module to track risks that require leadership insights.



Rsam’s flexible data model helped the organization ensure a legal basis within all of the organization’s policies, procedures, standards, controls, and assessment activities.

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



## Results

Implementing these Rsam modules 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 re-engineering.

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 now 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.



## About Rsam

Rsam is a leader in the field of Governance, Risk, and Compliance (GRC) solutions and is the fastest time-to-value GRC provider. The Rsam platform delivers unparalleled flexibility for companies to leverage out-of-the-box solutions and "Build Your Own" (BYO) applications for a wide range of GRC functional areas, including audit, business continuity management, compliance, enterprise risk, IT risk, incident management, operational risk, policy management, security risk intelligence, vendor risk management, regulatory change management and more. Learn more about Rsam at [www.rsam.com](http://www.rsam.com).