Tighter information security. Improved governance. More effective risk management and compliance. These were some of the goals that drove a client organization to select KPMG to implement RSA® Archer™ eGRC Enterprise and Threat Management solutions.

Critical factors involved in this selection were the ability to:

- Improve the client’s IT-GRC program productivity while meeting functional IT needs and enterprise security governance requirements
- Align vulnerability management processes across four legacy entities
- Integrate vulnerability scan results from scan tools while managing large quantities of data
- Build a sustainable, extensible framework for future solution deployment.

KPMG’s deployment plan included a roadmap that prioritized the various steps required to develop and implement the Archer Enterprise Management and Threat Management solutions. It also took into account the necessary steps for integrating Risk Management, Policy Management, and Compliance Management solutions in the future. Finally, the roadmap included steps for building custom On-Demand applications when required.

The KPMG team worked with the client to revise and improve existing processes for vulnerability management, creating a target operating model for addressing the risks posed by system vulnerabilities. Improving these processes required balancing the risk-driven needs of enterprise security with the operational requirements of IT support organizations. From scanning the systems and collecting the identified issues to monitoring remediation plans and tracking exception requests, KPMG worked with the client to build robust, consistent, measurable processes that would fit easily in the Archer data model. To support the size of this global, distributed environment, KPMG designed and built the system to integrate large quantities of data from vulnerability scan results.

**Taking greater advantage of Archer solutions**

KPMG encourages clients to leverage the strong out-of-the-box capabilities of the Archer GRC platform, adopting the motto of “configure, don’t customize.” Using the Archer solutions features, along with two On-Demand applications, KPMG was able to implement a number of key components, including capabilities to:

- Capture infrastructure assets, specifically devices and applications, from enterprise data sources
- Integrate with McAfee Vulnerability Management tool and its scan results for more than 100,000 servers
- Manage the process of submitting, reviewing, approving, and tracking exception requests, including long-term remediation plans.

**Key reports help streamline processes**

Examples of the reports available through this implementation include the Device and Vulnerabilities Dashboards.

**Device Dashboard**
The Device Dashboard includes system counts by Supported Application Classifications, Administration Support Organizations, Lifecycle, and Environment. This valuable information helps the user understand the scope of the environment and determine the level of effort required to mitigate risks and support compliance.

**Vulnerabilities Dashboard**

The Vulnerabilities Dashboard includes Vulnerabilities by Status, Vulnerabilities by Overdue Range, Vulnerability by Responsible Support Group, Vulnerabilities by Highest Number of Open Occurrences, Expired Exceptions by Expiration Range, and Exceptions Pending Approval. The dashboard provides a snapshot of the state of the environment and helps to determine the areas where the organization needs to focus for remediation efforts.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.