KPMG LLP

Firm drives compliance with RSA® Archer™ eGRC Suite

AT-A-GLANCE

Key Requirements

- Common platform for all eGRC activities to enhance accuracy and efficiency of compliance efforts
- Easily deployable solution for fast time to value and rapid response to own and client demands
- Clear, flexible management and reporting capabilities to satisfy business unit and other stakeholders

Solution

- RSA Archer eGRC Suite modules provide single platform for ITS (Information Technology Services) policy development, management, and monitoring
- Automated tracking of remediation activities streamlines and solidifies compliance stature
- Flexible dashboard and reports deliver information to management in digestible format

Results

- Quick, comprehensive response to requirement to comply with NIST 800-53 directive won new business
- Business and clients are reassured by ability to provide fast and comprehensive responses to their requests using online policy center
- Risk of inadvertent regulation breaches is minimized with tighter, automated compliance controls

"To enable our IT governance program, we decided that investment in the GRC platform was needed in addition to defining necessary processes. The GRC technology helps us to achieve alignment of controls with policies. It accelerates the definition, management, measurement, and reporting of IT-related controls through the mapping to regulatory mandates, managing remediation tracking and policy exceptions, and reporting on them to our ITS executive management."

IRINA GILLER, DIRECTOR, ITS POLICY AND GOVERNANCE, KPMG

Formed in 1987, KPMG LLP provides audit, tax, and advisory services and industry insight to help organizations negotiate risks and perform in dynamic and challenging business environments. KPMG LLP is the U.S. member firm of KPMG International whose firms have a total of 140,000 professionals, including more than 7,900 partners, in 146 countries.

KEY REQUIREMENTS

The services that KPMG offers vary hugely, with each project tailored to the specific needs of the client in question to deliver impactful results. Despite this variety of activity, the organization's focus on quality remains constant. Part of providing high-quality service means anticipating and meeting its legal, regulatory, and client requirements.

With many clients in highly regulated industries such as finance and healthcare, a key priority for any business initiative or IT project is ensuring compliance with relevant industry regulations – from Sarbanes-Oxley (SOX) to the Health Insurance Portability and Accountability Act (HIPAA). KPMG must therefore demonstrate its ability to easily and rapidly meet these and other enterprise Governance, Risk, and Compliance (eGRC) demands when undertaking client projects.

This challenge is not a new one, and the company has long had policies in place to meet its own and clients' requirements. However, these policies were stored in various repositories across the ITS organization, meaning it was difficult to map policies to new standards. Irina Giller, Director, ITS Policy and Governance, KPMG, heads up the team responsible for ITS policies and compliance. She explains: "We were unable to easily confirm whether or not we could comply with a new client request using an existing policy, so there was a lot of manual work involved every time – even after we created a more centralized repository using available tools."

CUSTOMER PROFILE

KPMG needed a common eGRC platform with a fully centralized policy repository to both publish policies and map them to authoritative sources while maintaining a comprehensive overview of its eGRC capabilities. Flexibility was also important to ensure that KPMG could set, operate, and report on its own policies and processes where required to satisfy a variety of legal, regulatory, and client requirements.

SOLUTION

KPMG considered leading GRC platforms against its IT governance requirements and selected the eGRC solutions from RSA Archer. It also received feedback from KPMG's Client Delivery team on RSA Archer capabilities as they worked with RSA Archer on various client projects.

"We needed a solution that would enable us to publish and search all policies from a central point," says Giller. "It was also important to have granular access controls to make sure that policies and control standards could be accessed by all KPMG partners, employees, and other authorized parties while baseline technical controls and specifications could only be accessed by the central ITS organization. Lastly, we needed the ability to map policies based on authoritative sources."

> "Clients are reassured by our commitment to meeting their needs, especially when they come in to conduct on-site reviews and we navigate them through our online policy center."
>
> IRINA GILLER, DIRECTOR, ITS POLICY AND GOVERNANCE, KPMG

Giller and her team addressed these requirements by deploying the Policy Management and Compliance Management modules of the RSA Archer eGRC Suite. These solutions enable KPMG to ensure comprehensive management of its policies, and any exceptions, as well as remediation tracking for compliance.

"With this solution, which includes a number of internal processes and the eGRC tool, we can carry out self-assessments to identify any gaps in our compliance stance, then easily work in amends to our policies to ensure we're covered," comments Giller. "Likewise, if a client has a new compliance requirement or wants to review our capabilities, it's easy for us to show them online how our processes measure up against their expectations and make any necessary enhancements in an efficient manner."

Implementation was carried out by KPMG's ITS Policy and Governance team, following brainstorming sessions with KPMG's Advisory team to develop a roadmap for rollout of RSA Archer modules. A consultant from RSA Archer was on site to help manage the implementation of both modules, and RSA also provided training to KPMG's development and support groups. This equipped them with the knowledge necessary to manage the new eGRC platform themselves.

RSA provided Professional Services support by assisting KPMG in deploying the solutions out of the box and then customizing the Policy Management module to build in the required notification processes. It also helped customize and map the compliance and remediation-tracking aspects of the Compliance Management module to fit with KPMG's planned usage model.

RESULTS

The first test for the new platform came shortly after deployment, when a new client project required KPMG to affirm and where necessary enhance its policies and procedures in alignment with the National Institute of Standards (NIST) 800-53 directive, which impacts data hosting for government organizations. KPMG won this new client's business by building a hosting environment in compliance with the directive. Enabled by RSA Archer, KPMG mapped the requirements to its internal policies and procedures, performed gap analysis, and, where necessary, developed and published additional policies, procedures, and technical baselines, all in a reasonable timeframe.

Having a centralized and automated online eGRC solution has simplified many tasks for Giller's small team. "Previously, client audits necessitated the printing out and processing of reams of paper documentation," says Giller, "which was time-consuming and unscalable. Now all the information we need is there on the system, so it's much

easier and quicker for us to find the policy or control standard we're looking for. Not only has this accelerated our own ability to meet requests for information, but clients are reassured by our commitment to meeting their needs, especially when they come in to conduct on-site reviews and we navigate them through our online policy center."

Managing IT policy exceptions is another area where the team has seen a marked improvement. The RSA Archer solution issues automatic alerts to KPMG's ITS Policy Review Board whenever an exception is submitted for review and approval, or is due to expire. The board can then notify the individual of its decision to allow a time-limited exception where business justification warrants it and adequate compensating controls are in place, or direct individuals to either take the necessary steps to become compliant or remove the incompliant situation from the network. "This model means we have tighter control over our compliance capabilities and are able to reduce the risk of any inadvertent breaches of regulations," says Giller.

CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.RSA.com