CASE STUDY: RSM HELPS GLOBAL BANK ADDRESS CLOUD RISKS, OVERCOME REGULATORY ACTIONS

Overview

Our client is one of the largest financial institutions in the world, with thousands of retail branches in the United States and operations in dozens of countries.

Background

The financial institutions industry faces a number of inherent challenges when implementing new technology. As a whole, the industry is very innovative and consumer-driven, emphasizing speed-to-market, emerging technology and making life easier for customers. However, financial institutions are heavily regulated, both in the United States and globally, and regulators are often slow to embrace new technology in part because they are focused on protecting banks and customer assets.

To remain competitive, banks must be agile and find new ways to leverage innovation. The cloud has become a key tool in this initiative, providing a quicker time to market and opportunities to create greater efficiency for both customers and employees. Regulators, however, are keeping a close watch on banks that transition to cloud environments, regularly issuing matters requiring attention (MRA) notices for concerns that require remediation in cloud deployments.

Our client received an MRA from regulators, after a finding regarding how it was managing and mitigating its cloud risk. The bank had strong and well-supported IT general controls for on-premise infrastructure, but it lacked an effective cloud governance model. In fact, the bank had developed cloud standards that were well beyond regulatory expectations, but it failed to meet those internal guidelines.

Project

With a 90-day deadline to remediate the MRA, the bank needed an advisor that could quickly step in and identify and address its pressing cloud risk and compliance challenges. The bank had several options, ranging from engaging a Big Four firm to hiring contractors in a staff augmentation model. Ultimately, the institution chose RSM due to our unique matrixed team. RSM provided extensive...
experience managing, implementing and securing cloud solutions along with a mature financial institution risk assurance program.

Initially, the RSM team worked with the institution to choose a cloud standard to follow in order to evaluate the risks the bank has across the cloud. A standard was needed that addressed each of the different architectures—software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). The bank utilizes all three solutions and each carry distinct risks, but previous cloud guidelines were only geared toward one architecture.

RSM chose the Cloud Security Alliance Cloud Control Matrix v3 (CCM) framework as the baseline for the institution, providing visibility into 16 different IT domains that the cloud utilizes. This framework also enabled RSM to leverage a proprietary compliance matrix, mapping CCM guidelines to each of the different domestic, international and industry compliance standards that apply to the bank. The framework was invaluable to the institution; instead of enduring several assessments based on multiple compliance and regulatory bodies, one assessment was applied to all standards without the need to duplicate work.

Once the standard was established, RSM conducted a significant evaluation to determine its risk position and whether existing policies addressed its control demands. The team evaluated several policies that applied to the cloud, including:

- Corporate policies: How the bank is auditing and assessing business continuity and disaster recovery
- Information security policies: How the bank manages encryption, portability, access and authentication
- Information technology policies: How the bank performs infrastructure, supply chain and vendor management

At the conclusion of that mapping exercise, RSM performed a gap analysis, determining where key controls were in place and where vulnerabilities existed. This process fostered a significant amount of conversation with the client, as internal personnel generally considered a policy or procedure to be the same as an actual control. However, establishing a policy or procedure without effective monitoring and management practices does not create an effective control.

Following the gap analysis, RSM identified the bank’s 30 most significant risk areas and worked with the bank to develop a strategy to monitor those risks. Now, the institution has scripts and third-party tools in place to identify when operations go outside a predetermined baseline or a process or procedure is in danger of not being followed.

With a more effective control framework in place, RSM also helped the bank establish a strong governance model moving forward.

Cloud governance and compliance is not a one-time exercise, as the cloud evolves and the bank continues to utilize new solutions to meet customer and employee demand. The new, flexible governance foundation can help the bank evaluate the risks involved with adopting new technology and understand the controls and contract terms necessary to mitigate future cloud risks.

In the past, the bank didn’t bring key stakeholders—information technology, information security and third-party vendor management—together with internal audit to develop cloud guidelines and strategies. These departments were not aligned and many incorrect assumptions were made about who was managing important cloud processes. In addition, individual business leaders were not involved in cloud decision-making, so they never fully understood the risks they were accepting and assuming by moving workloads to the cloud. This situation led to many cloud vulnerabilities and deficiencies.

The RSM team helped the bank develop a framework that brought each of these key parties together. Our advisors showed employees how to have a unified approach and view of their enterprise risk when it comes to the cloud. Instead of information technology, information security, vendor management or a single business line only focusing on their individual risk perspective, the bank now understands the importance of enterprise risk when it leverages the cloud.

**Outcomes**

Due to RSM’s quick mobilization and effective cloud risk and compliance advice and solutions, the bank resolved its issues with regulators and the MRA was lifted. The bank now has a comprehensive framework for managing cloud technology and leveraging further innovation without exposing the institution to unnecessary risk. By providing resources with extensive IT and financial institutions experience, the RSM team had real conversations about risk with the bank, and provided key tools and leading practices to strengthen cloud strategies.

Key benefits of RSM’s relationship with the bank include:

- Evaluating the institution’s domestic and global cloud risk and compliance stance with a single assessment
- Utilizing an established cloud standard that aligns with the cloud architectures the bank actually uses to help understand the specific risks
- Bringing all key areas of the bank together to implement an enterprise view of cloud risk
- Implementing a more secure and scalable cloud governance model that can safely integrate new functionality

**+1 800 274 3978**

rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and the power of being understood are registered trademarks of RSM International Association.

© 2018 RSM US LLP. All Rights Reserved.