CASE STUDY: COMMUNITY BANKING

Flexible IT audit addresses bank’s emerging risks and strengthens controls

Overview

Our client is a large, independently owned community bank in the Midwestern United States. The institution has several branches in multiple states.

Background

Our client sought an experienced advisor to evaluate and improve its information technology control environment by performing its annual IT audit. Banks are required to perform annual IT audits, which primarily fall under Federal Financial Institutions Examination Council (FFIEC) requirements to determine whether controls are in place and adequate. A typical audit includes standard network controls, settings and policies, e-banking, mobile banking and credentialing, among other considerations. Management is also examined to ensure compliance with regulations and efficient performance.

Annual IT audit

The institution chose RSM over seven years ago to perform its IT audit, based on the team’s experience in reviewing controls and addressing emerging risks. The bank has continued to come back to RSM in subsequent years, due to the team’s depth of experience, knowledge of emerging risks and industry trends, and capabilities in other areas of risk, such as technology, that are beneficial to the bank.

On an annual basis, RSM reviews the institution’s controls and performs the IT audit as an extension of the internal audit program. The audit satisfies regulatory risk demands, in addition to identifying potential future threats. The RSM team brings several potential issues to the bank’s attention annually from an information security perspective, including recent discussions surrounding mobile device security, mobile banking, virtual tellers, out of pocket authentication and revamping secret account questions. As a result, the project is fluid, with additional areas of focus integrated as needed to address the appropriate level of risk.
The scope of the IT audit is discussed anew each year, and is adjusted depending on new and future potential threats as well as to address regulatory updates. The project utilizes the audit program derived from the IT risk assessment findings and the RSM team works with the bank to dive into details of areas that need to be evaluated and any changes that have occurred since the last audit.

The bank undergoes periodic testing outside of the IT audit, and RSM works with the institution’s IT and internal audit staff on scheduling to avoid putting too much strain on the department. RSM also collaborates with the bank on staffing capabilities, ensuring the appropriate skill sets and level of experience are involved in the engagement.

In many IT audits, a client has items that require immediate remediation efforts and should be subsequently validated to verify that the remediation was effective. Validation testing ideally should take place within a reasonable time period to ensure all concerns are accounted for, and bank systems are secure. In the past year, in particular, during this client’s annual audit process, RSM discovered several such items. After discussing the concerns with the client, the RSM team developed a strategy for bank management to correct these issues with a plan for validation testing so the audit could conclude and meet originally planned timeframes.

At the conclusion of each annual audit, RSM conducts an exit interview, with all substantial findings identified and documented to discuss with bank representatives. If any critical issues or observations or documentation misunderstandings occur, they are resolved to avoid surprises when the final report is distributed. With former implementers and bank employees on the RSM team, the report presents actionable management items rather than vague suggestions for improvement.

**Value-added consulting services**

Over the past seven years, RSM’s IT audit work has resulted in additional consulting services for the bank. These include strengthening disaster recovery and business continuity capabilities, as well as network assessments after discovering security issues within the bank’s network or systems.

As a by-product of the bank’s most recent IT audit, RSM is implementing a focused social engineering testing program for the bank. This is designed to replicate a potential real-life social engineering attack, using various techniques (calls, emails, in-person visits) to exploit vulnerabilities and gain access to key target areas that may contain sensitive customer information.

RSM worked with the bank to determine where criminals may attempt to access information or data in secure areas. A test was then devised to perform reconnaissance, observing an attacker’s actions to circumvent authentication, authorization or identification measures. Although social engineering is not required by the FFIEC, the bank is choosing to undergo rigorous testing to validate control strength and employee compliance with security policies.

**Outcomes**

In many cases, an IT audit is a cookie-cutter process and considered to be more of a necessity than a value-add. However, RSM’s open dialogue and proactive approach to emerging risks brings additional value to the bank. Every institution faces different types of risk and the RSM team understands that, tailoring the IT audit program to the bank’s unique risks.

This fluid engagement based on the changing nature of risk has strengthened the bank’s controls and positioned it for continued growth. Other benefits of RSM’s service to the bank include:

- A customized IT audit program, based on specific threats and bank operations
- Increased knowledge of and protection from emerging risks
- A flexible audit, accounting for new vulnerabilities and changes within the organization
- A comprehensive social engineering project to test the strength of current security measures

+1 800 274 3978
www.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. 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® and the RSM logo are registered trademarks of RSM International Association. The power of being understood® is a registered trademark of RSM US LLP.

© 2015 RSM US LLP. All Rights Reserved.