RGS GLOBAL ADVISORS
1441 Broadway, Suite 6057, New York, NY 10018
390 North Orange Avenue, Suite 2300, Orlando, FL 32801

Case Study – IT and Cybersecurity Risk Assessments

The Problem

A $400 million bank used the Cybersecurity Assessment Tool ("CAT") to evaluate its cybersecurity risks and assessed its Information Technology ("IT") and Information Security ("IS") risks documenting separate IT and IS Risk Assessments. The bank, understandably, believed that these risk assessments appropriately documented cybersecurity and technology risks and related controls and that these were aligned to their policy and procedures. The bank's regulators, as part of their annual examination, however, determined that these IT, IS and Cybersecurity risk assessments did not adequately reflect the bank's technology environment and its risk exposure. They determined that the evaluations were too subjective, and that the evaluations didn't adhere to any standardized rating system. As a result, the regulators required the bank to update its risk assessment methodology, and then reperform the risk assessments.

An inadequate evaluation of IT/IS and Cybersecurity risks can potentially result in unidentified or unwarranted threats, fraud, ransomware, or system failures. Any such failures expose the bank, its executive management, and the board to severe reputation risk and potential liability or financial loss.

Banks Attempt to Resolve

RGS was engaged to establish an updated risk assessment methodology and then perform comprehensive risk assessments of IT, IS and cybersecurity risks facing the bank.

RGS Solution

RGS deployed a team of IT and Cyber experienced professionals who quickly reviewed the bank's IT environment, including oversight, governance, internal controls, and reporting frameworks. With this information and after management's approval, RGS deployed a comprehensive risk assessment methodology that complied with the FFIEC guidelines and aligned to the bank's profile and its products and services. The approach evaluated the effectiveness of controls, and applied qualitative and quantitative factors in the determination of inherent and residual risk ratings across all processes and functions such as user access, logins (remote and onsite), helpdesk, vendor system controls, exception reporting and oversight, etc.

RGS also performed an updated Cybersecurity evaluation using the CAT model which, upon reevaluating all cyber related controls, determined that certain controls were "sub-baseline".
The updated risk assessments and methodology used which now complied with regulatory directives were approved by management and the board. However, in closing, RGS pointed out the cyber risk items where the controls were deemed "sub-baseline" needed to be addressed to mitigate the exposure to cyber risks caused by the weaknesses. RGS also pointed out that not enhancing the "sub-baseline" controls, in addition to increasing cybersecurity risk for the bank, could also lead to a negative comment from the regulators later. The bank agreed with this value-added suggestion and RGS was approved to implement a solution which was subsequently adopted and approved by management and the board.

Result

The bank enhanced its understanding of exposure to cyber and other IT/ Security risks and improved controls and reporting to mitigate these risks. As a result, this reduced the exposure to fraud, identity theft, ransomware, and other ongoing cyber threats.

In addition, during the next examination of the bank, the regulators reviewed the methodology and found it to be comprehensive and appropriate. They also found all risk assessments to have been performed appropriately and agreed with the process, including evaluation of controls and residual risks in all instances. Further, they expressed appreciation of the fact that the bank had documented an appropriate action plan and implemented it to address the areas where its controls had not reached baseline levels.

RGS Global Advisors is a cost-effective provider of Internal Audit, Risk Management, Cybersecurity, and BSA/AML/OFAC Compliance Consultancy services to Financial Institutions.

For further guidance or assistance contact us at: info@RGSGlobalAdvisors.com