Don’t Be Passive About Risk

September 4, 2016/in TLI 816 /by Marc Riccio

While extremely imperative to monitor and uphold, many institutions maintain a passive approach to operational risk. With increased regulatory changes, a difficult and confusing process continues to challenge us with many questions. What information do I have to monitor? How often must I review this information? Will my methods be successful in passing an audit? While most financial institutions find operational risk management to be a large burden, a centralized and intuitive platform will make the task far less daunting.

Operational risk management involves the risks resulting from breakdowns in internal procedures, people and systems. As a whole this broadly defined topic seems over bearing but when narrowed down and broken up into sections we can grasp a better perspective. The important areas to focus on are vendor management, business continuity planning, and incident response. Most often, these three areas are treated separately and managed by different departments, but with the growing audit vulnerability due to increased regulations and more intensive exams, it is beneficial to treat them as one.

Vendor management involves the process of monitoring critical vendors to ensure that your institution will not falter if there happens to be an external disruption in services. So what does happen if a vendor remains inoperable and your institution relies on that vendor to maintain critical business processes? Here is where vendor management runs head to head with business continuity planning. Information such as institutional resources, personnel, departments, critical processes, and vendors should be taken into consideration for both vendor management as well as business continuity planning. The best way to prevent complete failure is to prepare for the worst case scenarios. Disaster recovery tests should be performed internally between departments as well as externally involving vendors. Your vendor management program and business continuity planning program should unify to reflect this co-dependency.

Naturally, most financial institutions utilize around one hundred outsourced vendors. As a result, a greater dependence on third party providers can lead to a larger cybersecurity risk. Your incident response policy should prepare your institution to take the correct steps to prepare and control an incidental breach. Most often a vendor could be involved in the situation which would require further monitoring and might even increase the overall vendor risk rating. All of which is important to track and mitigate, utilizing an effective operational risk management program involving both vendor management and incident response. An integrated program will facilitate the ease of sharing imperative information across all areas of operational risk.

The best solution is to maintain one centralized platform for operational risk management. Since all areas are tied together, the systems should allow for this tight integration using shared information. If your process is easily managed and allows for well integrated information, then the implementation and ongoing monitoring will no longer be a daunting task. You should be confident in your institution’s operational risk management process and the best way to get to there is to start recognizing and managing operational risk areas in a cohesive light.

About The Author

Marc Riccio, President of Specialized Data Systems, Inc., has over thirty years of experience providing software solutions to the financial industry. Marc is known for his forward thinking and vision of introducing new and innovative technologies including “rules-based” Loan Origination software, COLD/Document Image Systems, Internet Security Services on Demand, Cloud Computing and now Operational Risk Management software. Prior to founding Specialized Data Systems in 1989, Marc worked for several technology companies as a Systems Analyst, Account Manager and Sales Manager. Among his significant previous positions, Marc served as Senior Marketing Representative for FiServ-Connecticut and worked in the Retail Banking and Systems group for Bank of America.