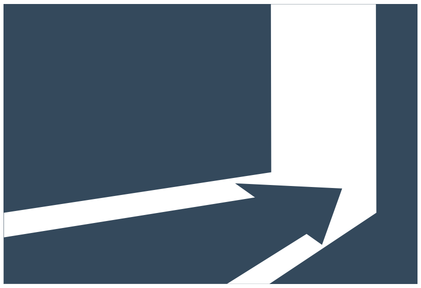
MANAGE YOUR RISK BEFORE AUDITORS COME KNOCKING

If an effective third party risk management system is not in place, auditors will be waiting.

BY MARC RICCIO

Research has shown that the financial industry outsources over 85% of their information technology. Outsourced technology can include your basic products such as the phone system, alarm system, network, servers, or computers. Your more critical outsourced technology might include lending technology, online banking system, secondary marketing system, payment solutions, core solution or ATM processing. From basic to critical technologies, all types of third parties play a key role in business operations proving that outsourcing technology directly effects your institution every day. Outsourcing technology has major benefits if managed correctly. If an effective third party risk management system is not in place, auditors will be waiting to knock down your door. Institutions rely heavily on outsourced technology to perform business functions resulting in an increased overall operational risk. If an outsourced vendor unsuccessfully delivers services then the institution relying on that vendor runs the possibility of failure. The risk associated with your outsourced technology providers directly effects the overall internal operational risk of your institution. If you are effectively managing your entire operational risk management program, you are ensuring you will always be able to perform everyday business functions, which are critical to survival.



Your risk management solution should incorporate vendor management, BCP, and incident response under one solution.

One of the biggest struggles of managing third parties is the amount of time and effort it takes to complete the tasks required by the FFIEC and FDIC. The regulations stress the importance of maintaining a strong selection and monitoring process. This process includes qualifying and assessing the risk of each vendor, communicating with the vendor to obtain the necessary due diligence criteria, receiving the authorized review of the due diligence documentation, and continual monitoring of each vendor to update their documentation. Since each vendor provides something different to your institution, the process is extremely complicated. Each vendor must be assessed based on the risk they could bring to your institution, and all due diligence must be properly performed based on the level of risk. As a result of this, there are large amounts of resources, people, and time invested in properly managing your third parties.

Typically, institutions require their Vendor Manager, Vendor Owner, Legal department, Financial advisor, and CFO to be involved in the entire process. There are many hands involved in vendor management, and this is not accounting for external vendor cooperation. The Vendor Manager has the role of overseeing the entire vendor management program and ensures that all tasks and procedures are completed correctly and timely. The Vendor Owner has the role of obtaining all due diligence documentation and screening the vendor. The Vendor Manager begins this process by requesting for the vendor to be reviewed by the Vendor Owner. The Vendor Owner is then required to communicate with their vendor to obtain the proper due diligence information. Often times this point in the process gets delayed by the vendor because the due diligence documentation is viewed as a low priority and burden. This consequently makes an already lengthy process even longer. The difficulty of involving internal company-wide efforts and external vendor participation likely leads to miscommunication and lack of collaboration. Your institution needs to have a uniform process, ensuring interdependencies across your institution are effectively controlled.

If this process is completed manually, the implementation becomes increasingly complicated. Financial institutions often rely on multiple documents and lists which are all managed by different people and could contain duplicate information. One of our current clients previously managed three different vendor lists; contact information, accounts receivable and critical vendors. The departmental contact list was utilized by department personnel and contained contact information needed to communicate with each vendor. The accounts receivable list was utilized by the accounting personnel and contained billing information related to products and services as well as contract renewals. The critical vendors list was created by the IT department to track which vendors provide the most critical services and what due diligence needed to be performed based on the assigned criticality. The three lists each contained important information needed by multiple personnel. It would be impractical to eliminate any of the lists and would also cause chaos to simply combine. The vast amount of documentation and acknowledgements needed on an individual vendor basis essentially takes up more time and effort to maintain separately than it would with a centralized repository. This particular institution and many others have experienced the agony of maintaining a manual vendor management process and have therefore invested in an automated solution.

Simply automating might not be the answer to all prayers. The key is to invest in an automated solution that can easily maintain all vendor information as well as the management process from acquiring a new vendor and vetting an existing vendor to monitoring their relationship. Current systems are often difficult to use and lack the ability to delegate tasks to specific personnel. Since the vendor

One of the **biggest struggles of managing** third parties is the amount of time and effort it takes to complete the tasks required by **the FFIEC and FDIC.**

management process is so lengthy, it requires many hands to get involved to perform due diligence activities. This leaves room for miscommunication, error, and missed deadlines. The ideal automated solution would include user access roles, built in alerts, and a complete document repository. User access roles would allow all involved internal personnel the ability to manage their specific functions and keep track of their individual vendors. Built in alerts would ensure that all review dates and contracts are being reviewed and managed on time and monitored correctly. A complete repository would centralize all vendor due diligence documentation in one area to ensure that each vendor is being properly evaluated and controlled. The overall goal is to mitigate all outsourced technology risk by centralizing all tasks into one system. To achieve this goal, you must anticipate the risks before the auditors.

Unfortunately, institutions tend to maintain a defensive "band aid" approach to auditors and regulations. They panic after a visit from the auditors and find a quick fix to the problem. Usually the quick fix is to purchase a system to cover the area that the auditor scrutinized. Sometimes that system is only covering just a small part of the bigger problem and the institution falls in to a vicious cycle to constantly require more band aids. They might devote the time and money into a vendor management system but then still manage the other areas of risk manually. Instead, the approach should be proactive to eliminate the "band aid" cycle because eventually those band aids will run out and your institution will suffer. The newest FFIEC IT Examination update guides the way to a proactive strategy.

Appendix J in the FFIEC IT Examination handbook explains the importance of strengthening the resilience of outsourced technology by stressing the need to identify, measure, monitor, and mitigate all areas of risk associated with outsourcing. It is no longer practical to invest in several solutions to separately maintain all areas of risk management because of this regulation. In order to stay ahead of the game, it is better to have a solution that ties all areas of risk management under one umbrella. A complete risk management system is the solution to the worries that Appendix J has brought upon the industry. An all-encompassing risk management solution will identify which vendors are correlated to your critical business functions. The vendor must allow you to complete your critical functions or you will be in jeopardy of financial loss or loss of business. You should maintain your institution's business continuity plan and incident response policy and also monitor the BCP and incident response policies of your third parties. This will ensure that if a disaster affects your vendor, they will be able to continue to provide their product or service to your institution.

Your risk management solution should incorporate vendor management, BCP, and incident response under one solution to ensure that all involved personnel can work together, eliminate further short term solutions, and anticipate future regulatory requirements. An all-encompassing operational risk management solution will ultimately make your institution prosperous. ❖

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.