Managing Third Party Risks as a Financial Institution

By Danny F. Dukes, CPA, MBA, CFE

Last week I attended a one-day financial institution conference. A prominent financial institution attorney, Mark Kanaly with Alston and Bird, LLP, brought something to the forefront that got many blank stares throughout the room. The topic was Enterprise Risk Management (ERM) or more specifically the management of third party risk. The rhetorical question is where does financial institution risk stop and third party risk intervene?

The FDIC has remarked on several occasions that it was nor is their intent to force all financial institutions, regardless of size, to implement a comprehensive Enterprise Risk Management system. However, in the Guidance for Managing Third-Party Risk (FIL-44-2008), they clearly state, "Financial institutions often rely upon third parties to perform a wide variety of services and other activities. An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution." This guidance placed specific responsibility on management to develop processes relative to the following four elements:

1. Risk Assessment
2. Due Diligence in Selecting a Third Party
3. Contract Structuring and Review
4. Third Party (Vendor) Oversight

While books could be written, as they do exist, on how to address the first three elements when establishing a third party assignment of business risks, it is the fourth element that can be the redeeming factor of a bad third party choice or a third party that doesn't continue to appropriately address changes in technology or regulations. The initial decision could have been a great choice, but time and change has wilted the vendor's ability to continue providing an appropriate service.

I am currently involved in a court case where a prominent data processor client sights them in a deposition as “having an extremely deficient kiting suspect report, almost unusable.” Do you think a judge and/or a jury wants to hear finger pointing as to why this financial institution failed to identify a customer with uncollected funds casing a plaintiff damages? I don’t think so. In fact, because the financial institution knew of the deficiency and did nothing to mitigate the risks, will likely haunt this financial institution. Would it matter if the financial institution was unaware of the deficit kiting suspect report? I don’t believe so because it is the reasonable and customary practices of a financial institution to be able to mitigate, within reason, the risk of loss due to uncollected funds, which could expose their customers.

The spirit of FIL-44-2008 dictates that at least on an annual basis, management should monitor the performance of each critical third-party vendor. First, a financial institution should identify and document each critical third-party vendor. The documentation should minimally contain vendor name, what service(s) are provided, and when the contractual period ends with the provider. Annually, the institution should obtain the most recent Service Organization Controls Report (SOC) and have a trained person review the report for the following:

1. Scope of the work reviewed by the third party,
2. Time period reviewed, and
3. Findings reported.

SOC reports replaced what was previously known as the SSAE 16 Report. The new format targets more critical operational functions of the third party and gives the readers a much clearer picture as to whether or not the third party has all their critical controls in place to protect the institution concerning compliance, regulatory and other critical applications. I have found deficiencies in these reports that warrant follow-up with the vendor to determine that corrective actions were taken. I’ve even seen cases where a follow-up SOC was needed to determine major breakdowns in controls and procedures were effectively corrected. An example I had recently was a vendor that did not use a password token for employees that had remote system access through a Virtual Private Network (VPN). For my client, this vendor transferred funds and the lack of this remote access control, which was an industry standard, was unacceptable. So, we had to work through this with the vendor.

Additional items that should be obtained annually from third parties are licenses, financial statements, and insurance policies. We should make sure that the vendor is properly licensed, if appropriate, in sound financial health and has the appropriate insurance coverage.

The regulators have made it clear that while many institutions may not need a comprehensive and elaborate ERM system, there is clearly a mandate for the

accurate identification of critical third party vendors and subsequent annual review of their functionality. This review should include SOC Report reviews, financial statement review, current license determination, and insurance policy review. Conclusions should also be documented as to how the vendor adequately or inadequately mitigates the financial institution's third party assigned risks. Any concerns the institution may have with the vendors should be vetted and documented. In some cases, a vendor could be asked to adjust the way they do things. In other cases, they could be replaced for violating contract provisions or non-renewal of their contract at expiration. One thing is clear the financial institution should control the relationship because regulators are holding them accountable should the vendor miss-step. Finger pointing will not be tolerated.

Danny F. Dukes is the managing member of Danny F. Dukes and Associates, LLC, a forensic and financial institution consulting firm founded in 2010 and located in Canton, GA. For additional information please refer to their website at http://www.dannyfdukes.com.