GET TO KNOW BDO

BDO CONSULTING Q&A:

April 2016

A Q&A session with Mike Mager, BDO Consulting Director, on Third-Party Vendor Oversight

A big area for regulatory scrutiny in recent years has been banks' relationships with their vendors. What's changing?

Regulators are making it increasingly clear that banks are ultimately responsible for any harm that comes to their customers, including issues that arise indirectly via vendor relationships. The Consumer Financial Protection Bureau, the Office of the Comptroller of Currency (OCC) and other regulators have shared explicit examination guidance on third-party risk management, asserting that banks are accountable for their vendors' actions. Pursuant to the OCC's 2013 bulletin on third-party relationships, "A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws." In other words, banks should view their third-party relationships as extensions of their business and hold them to the same risk management and compliance standards.

Banks are now expected to proactively manage third-party risk and conduct ongoing monitoring throughout the relationship lifecycle, from the initial due diligence stage to contract negotiations to execution of the work to termination. As banks continue to rely on and expand their third-party relationships, an ad hoc approach to oversight and accountability is no longer feasible. To keep pace with the rapidly changing regulatory environment and efficiently evaluate hundreds or even thousands of third-party providers, banks need to formalize their third-party risk management framework, define the "critical activities" involving third-party subcontractors and create clear standards that can be subject to periodic evaluation.

What is a “critical activity”?

Critical activities are the aspects of the business where disruption would cause the highest business impact. The definition of “critical” has grown beyond core business functions and information technology systems to include any activity that could draw regulatory scrutiny or damage reputation. However, it’s important to note that what constitutes “critical activities” can vary significantly from entity to entity, depending on the business and its value proposition.

For example, a vendor should be considered critical if:

- Operations would be impacted by disruption or inadequate service.
- Customers would be significantly impacted by inadequate service or misconduct.
- Privy to competitive information or sensitive customer data.
- Significant investment in implementation is required.

What are the biggest risks posed by vendor relationships?

An area of third-party risk management quickly gaining traction is information security and data loss prevention as data breaches become increasingly commonplace. Notably, more than 60 percent of data breaches originate via third-party vulnerabilities. However, according to BDO's recent board survey, only one-third of public company board members have cyber risk requirements for third-party vendors, suggesting a significant gap in oversight and internal controls.

CONTACT:

Michael E. Mager
BDO Consulting Director
212-885-8401
mmager@bdo.com

How are regulators addressing the increase in cyber risks?

The nature of cyber breaches is constantly evolving, and regulators around the globe are growing more concerned that financial institutions and their partners aren't doing enough to keep pace. Regulators have been warning banks that more needs to be done. In February of 2015, the Financial Industry Regulatory Authority released cybersecurity guidance including effective practices for risk-based due diligence of third-party vendor relationships and contractual provisions to protect firm and customer information, noting that a one-size-fits-all approach is not practicable. In addition, the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations announced its Cybersecurity Examination Initiative in a September 2015 alert, warning financial institutions that examiners will more closely scrutinize firm practices and controls related to third-party vendor management. Then, in November, the Federal Financial Institutions Examination Counsel (FFIEC) alerted financial institutions to the growing threat of cyber extortion, urging companies to conduct due diligence assessments of third-party services and to test the effectiveness of incident response plans with their providers.

Federal regulators aren't the only entities cracking down on third-party vendor cyber risk. In November 2015, the New York State Department of Financial Services (NYSDFS) issued a letter highlighting its concerns about the industry's cyber vulnerabilities, including its reliance on third-party providers. NYSDFS plans to issue cybersecurity guidelines for financial institutions that are expected to be adopted by other state and federal regulators. The guidelines will include minimum requirements for third-parties to ensure sensitive data is protected.

How can banks better mitigate risks with third parties?

As a starting point, banks need to identify their critical infrastructure, identify all existing and future third-party vendor relationships and map those relationships against those critical assets. More or less oversight may be required depending on the level of risk associated with the service provider and the extent to which they participate in critical activities. Vendors' risk management policies and procedures should be closely examined, as should their compliance practices from the onset of the relationship. Vendors must have a thorough understanding of federal and state consumer protection laws as well as the bank's risk management standards--and the consequences of running afoul of those rules. Contracts must clearly communicate the risks and responsibilities of both parties. However, the key to successful risk mitigation is that it is a continuous process—not something that is simply conducted upfront and then forgotten. Banks must diligently monitor risk and review internal controls with service providers to ensure they remain compliant in the changing environment.

How can BDO help?

BDO has multidisciplinary teams that protect organizations from third-party vendor risk on multiple fronts. Having provided services to some of the most complex and high-profile monitorship engagements, our professionals have established credibility with top regulators and have extensive experience performing independent examinations and oversight services. With the majority of data breaches coming through third-party relationships, vendor risk and compliance management is also a significant area of focus for BDO in evaluating our clients' cybersecurity preparedness. As part of our cybersecurity service offerings, we perform vendor risk assessments and testing with respect to information security and data governance, and work with clients to create cyber-risk requirements for their vendors and shore up their third-party information security compliance programs and capabilities. Through our forensic service offerings, BDO can also help banks conduct investigations of suspected inappropriate behavior or security issues, respond to any inappropriate conduct or breach of contract and then implement necessary remediation. We have professionals who are experienced in due diligence and work with clients to proactively address changing regulatory rules and guidelines. Our global network and deep technological resources provide tailored solutions to meet clients' individual needs.