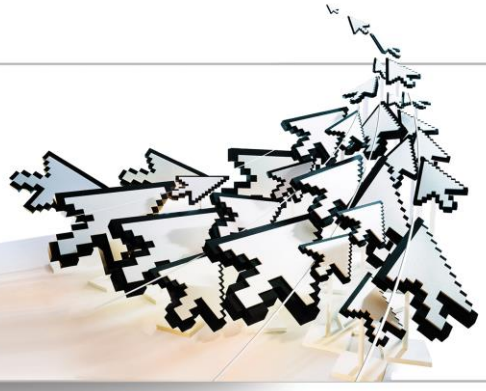
Financial Institution Compliance Update



November 4, 2014

This communication is designed to provide you with quick snapshots and timely perspective on recent regulatory developments.

Vendor Risk Management: Guidance for managing third-party relationships

Background

The landscape of managing third-party vendor relationships has changed with updated guidance issued by the prudential regulators and the CFPB. The CFPB issued an updated bulletin on April 12, 2012 followed by an OCC update on October 30, 2013 regarding managing third-party relationships. Core principles are the same in both regulatory releases along with leading practices in the industry. While the effective dates of these regulations are more than two years old, many companies are still struggling to stay in compliance. During September 2014, several banks were fined for vendor related failures. Effective vendor management must include planning, due diligence in third-party selection, contract negotiation, ongoing monitoring, termination, oversight and accountability, documentation and reporting, and independent reviews.

Consequences of an ineffective vendor management program

There are significant consequences for third-party management weaknesses and recent articles about banks, for example the large regional bank that was fined by the CFPB, highlight that the penalties or findings can occur even after a vendor is terminated. The CFPB, OCC and other regulators have been extremely active in bringing enforcement actions resulting in Consent Orders or settlements related to failures to properly manage third-party risk. In these cases, the penalties have been severe and do not begin to account for the ancillary expenses involved in responding to the action itself. Nor do they account for the costs associated with compliance or vendor programs that could have been avoided had there been effective processes throughout the vendor relationship.

Another example involves a health care credit card lender that utilized a third-party for implementation of its services. The CFPB found that the lender failed to oversee, train and monitor the third-party and incurred an Unfair, Deceptive or Abusive Acts or Practices violation (UDAAP). The CFPB ordered a restitution fund in excess of $30 million. What was the lesson learned? The service provider was found to have deficient contract management, monitoring and oversight. Failures were also found in training, documentation and reporting with areas specific to document retention and Service Level Agreement failures.

In another action, a credit card provider was utilizing internal and third parties for the sale of add-on products for its credit card customers. A $20 million fine was issued by the CFPB as the result of inadequate vendor management oversight. The CFPB found that management had failed to identify the risk factors associated with the add-on products that it was marketing and selling. As a result, the company was found to have violated UDAAP. Not only did the company owe a fine, the CFPB also required the implementation of vendor training on consumer laws, mandated third-party site visits, enhancement and maintenance of internal controls, and the establishment of an independent auditing group and requirements for termination of a vendor that fails to perform. The CFPB also ordered the lender to maintain call records for 25 months.

In a more recent matter, a bank was ordered to pay $37.5 million in damages to mortgage consumers for allegedly providing misinformation to borrowers, miscalculating income and mishandling mortgage modifications. The findings included failed vendor oversight of a third-party used by the bank to assist it with a backlog. In a public statement, the CFPB reinforced its commitment to protect consumers against bank actions.

This steady stream of findings by the CFPB illustrates the long-term commitment of the agency on these issues. Companies need to be aware of the long compliance tail after findings. It is no secret that many institutions and large vendors, subject to Consent Orders in April 2011, are still implementing program enhancements and changes and undergoing heightened regulatory scrutiny. The April 2011 Consent Orders illustrates one of the most publicized vendor management failures that spread through the financial services industry. Regulators at many banks found that bank employees, outside law firms and vendors executed documents without requisite knowledge, took short cuts in notarization processes and failed to adequately review documentation for errors. Among other requirements, including civil money penalties, the regulators mandated enhanced board oversight, internal audit, and compliance and enhanced risk management programs. The lesson learned? Policies and procedures defining tasks and responsibilities in compliance with all applicable legal requirements must be implemented by the bank. The banks are primarily responsible for ensuring compliance with those policies and procedures including establishing due diligence that ensures the vendor has adequate qualifications, expertise, capacity, reputation, information security and training.

Fundamentals of a vendor management system

Organizations need to ensure that they have effective programs in place to manage and oversee third-party vendors. Programs must include a systematic oversight process to ensure its vendors comply with all applicable legal requirements. Focusing on the risk factors, the implementation and oversight of every third-party relationship must account for the following risks:

- Strategic
- Compliance
- Reputational
- Operational
- Transactional
- Credit

To address these risks, the fundamentals of any vendor management system must include the following elements:

- Due diligence and third-party selection
- Contract negotiation
- Ongoing monitoring
- Termination framework
- Oversight and accountability
- Documentation and reporting
- Independent reviews

How does an organization begin to develop an effective vendor management program? Start by taking a holistic view from the top. How does the guidance apply to the operation of the business? Am I subject to oversight as a vendor, a vendor manager myself or both? How do vendor relationships work in my operations? What are my clients going to require and what do they need to demonstrate their compliance to regulators? Understanding the requirements of a client is a roadmap to the types of information, data and controls a client is going to demand of a vendor. These requirements will often include contractual and regulatory requirements in vendor contracts, rigid onboarding processes, periodic reviews, vendor tiering based upon risk and tier re-evaluations.

Strategies for addressing regulatory audit reviews

The case studies and penalties are not the only reason to implement a robust vendor management program. Some industry players have shared that client and regulatory audits have quadrupled over the last few years. While pre-2013 areas of audit inquiry and questionnaires typically focused on a vendor profile, the nature of the vendor's business, financial stability, insurance coverage, privacy and confidential data and business continuity, the areas of inquiry in 2014 have exploded. Businesses can now expect inquiry into the following:

- Business information, including licensing, financial information, management, employee qualifications, outstanding litigation, regulatory matters or inquiry, product ownership and system development lifecycles
- Security including networks, physical security, application security, hardware, access control and identity access management
- Privacy/GLBA/PCI
- Operations oversight including policies and procedures, change management, consumer complaints
- Risk management
- Vendor management
- Compliance program oversight including compliance with both internal and contractual requirements, applicable laws, records retention/destruction and training
- Business continuity planning, disaster recovery
- Diversity
- Environment

The increased frequency of audits and inquiry, together with the rise in scope, can be daunting for both risk managers and their vendors. To be successful in addressing reviews of your business by clients, there are a few key strategies that can be employed:

- **Audit management planning** – design an effective response strategy and make as many advance decisions as possible. Use past audits and inquiries to help define the scope.
- **Pre audit preparation** – create a library of commonly asked questions and answers. Set a review period to ensure answers remain appropriate and haven't changed. Standardizing answers increases vendor response time and helps to create consistency. Creating collateral on predictable topics such as privacy policies, document retention or disaster recovery creates efficiencies.
- **Audit execution** – Dedicate a team to manage the audit or inquiry with centralized communication, standardized responses, calendar management, and timeline oversight. Set expectations by defining roles and centralizing communication to help streamline the response process and build client trust and relationships. This also enables a company to gather data on audit areas to spot trends and adjust business operations more quickly.
- **Post audit** – Save your work! Vendor audits are often repetitive. Use prior responses and audits to set baselines and frameworks. Make sure any findings, good or bad, are shared with all stakeholders. Be sure to complete any remediation efforts and test those controls going forward.

How Experis can help

The increased frequency of audits, for both client and regulatory, along with the risk in scope can be overwhelming for an organization and their vendors. Effective and well-documented programs can help manage the process. **Experis Finance** offers industry experience in all aspects of regulatory compliance, risk management and third-party vendor management including: organizational design, infrastructure, governance, program initiation, comprehensive risk assessments, controls and monitoring techniques, management information systems and board reporting.

If you have any issues or need support, contact an **Experis** representative or visit us online at **Experis.US/Finance**.

Experis™ Finance
ManpowerGroup