The three pillars of a proactive, risk-based vendor management program

Prepared by:

Joe Benfatti, Partner, RSM US LLP
joe.benfatti@rsmus.com, +1 415 848 5344

Anthony Baca, Manager, RSM US LLP
anthony.baca@rsmus.com, +1 949 255 6567

Marie Patterson, Vice President of Marketing, Hiperos LLC
mpatterson@hiperos.com

April 2014

Now that the economy is showing signs of recovery, institutions are growing, diversifying and searching for ways to enhance the efficiency of their operations. The use of third-party service providers has expanded to afford institutions opportunities to focus internal resources on what they do best, and partner with specialist service organizations to deliver routine functions. However, today’s outsourced functions are frequently the most critical and sensitive areas, which have significantly caused risk to increase, resulting in more vigorous regulatory oversight. Cost and experience are major factors in the increased use of vendors; it often makes economic sense to outsource functions to a third party with the right knowledge and infrastructure, rather than paying for and maintaining it in-house. The increase in oversight and a growing amount of vendor options underscores the need to ensure your service providers are qualified and can adhere to your risk appetite and regulatory demands.
In most cases, there is an agent and principal relationship between an institution and a strategic vendor. This means institutions that engage vendors as agents to perform certain functions on their behalf are not relieved of the responsibility, potential consequences and liability that may result if the outsourced functions are not performed properly and effectively. Therefore, a reliable and comprehensive vendor management program is needed to mitigate strategic, reputational, operational, transactional financial and credit and regulatory compliance risks that an institution is liable for when vendor services are employed.

Common sense dictates that the use of a risk-based method is the best and most efficient approach to managing vendors. Regulators expect that significant vendors be identified and distinguished between routine vendors, and those that should be referred to as critical vendors. In fact, the latest guidance from the Office of the Comptroller of the Currency (OCC)—Bulletin 2013–29—specifically calls out the need for more significant and documented management of third parties providing “critical activities.”

Critical vendors can vary by institution, so it is important to decide which vendors are performing strategic functions for your institution. These should include those related to your high-risk products, or products that have a high impact on your revenue. For example, a shredding company performs an important task, but it is typically not significant to the services that you are providing to customers. However, a company that provides core system processing services is key and integral to delivering services to customers, and requires a higher level of oversight. On the other hand, if the shredding company has access to your customers’ nonpublic personal information (NPI), consider the level of risk associated with a breach of data that could impact your customers and the institution’s reputation. Based on your reliance on a third party, apply all criteria it uses.

Other important criteria that can be used to identify critical vendors include:

- Significance of transaction volume
- Cost of vendor services
- Relevance to the entity's core business process or service offering
- Nature of the activity and its criticality to the line of business
- Length of time to transition to a replacement vendor (or bring goods and services in–house), should the relationship fail

The regulatory landscape

Regulators have become increasingly concerned about a developing trend related to third–party service providers, and have focused more attention on these agreements. Some institutions are outsourcing functions where the vendor has direct contact with the customer and little, if any, transparency exists as to the timeliness and diligence of the methods of direct oversight.

The continued trend toward the digitization of transaction-oriented data, including personally identifiable financial and demographic data, has pushed the processing, transmission and storage (cloud or otherwise) outward to trusted third parties at an unprecedented rate. Processes such as mobile banking, loan underwriting, origination and servicing are increasingly supported, often transparently to the customer, by strategic service organizations.

Banks have been under scrutiny to have an adequate vendor management program for a number of years. However, the establishment of the Consumer Financial Protection Bureau brought other financial institutions not previously regulated, such as mortgage and finance companies, under the regulatory umbrella. This has caused management of these institutions to sit up and take notice of prudent vendor management practices.

The pillars of vendor management

The pillars of vendor management include three specific areas: contract management, setting performance expectations and monitoring and contingency planning and vendor replacement.

1. **Contract management:** Written service–level agreements are a critical element of effective vendor management. They must be clear and concise; detailing the organization’s needs and establishing the minimum acceptable standards pertaining to the success factors of the work your vendors are performing, such as uptime, security, usage, throughput and response time. Establishing the true scope of the engagement and developing processes to manage your relationships are important to setting expectations and ensuring compliance.

   Also, if you are outsourcing a critical function, it would be optimal and efficient to obtain additional assurance, such as a third–party report on the service provider’s commitments. An emerging trend to support that need is the Service Organization Control (SOC) 2 framework established by the American Institute of Certified Public Accountants.

   In addition to the traditional type of report (formerly under Statement on Auditing Standards No. 70—now referred to as a SOC 1), which reports on control matters relevant to financial reporting, the SOC 2 report speaks directly to vendor performance.

   A SOC 2 report includes five distinct principles that align with any service–level agreement with an outsourced service provider. These principles are:

   - Security—All access points and processes are sound and secure.
   - Availability—Systems are available and up and running as agreed.
   - Processing integrity—Processes are detailed, and the accuracy and integrity of procedures is confirmed.
- Confidentiality—The type of data that is outsourced is detailed, including where it is stored, how it is stored and transmitted, etc.
- Privacy—Similar to confidentiality, but also details coverage for any particular type of data that is specifically governed by a regulatory or statutory privacy requirement (such as the Gramm-Leach-Bliley Act).

Obtaining and reviewing a third party’s SOC 2 report provides advantages to significantly improve vendor management efficiency. As a result, institutions are now beginning to require SOC 2 vendor standards when selecting critical vendors. The clauses of the contract should be based on the inherent risk assessed during the initial due diligence. Done correctly, this will identify whether, for instance, your heating, ventilation and air conditioning (HVAC) vendor has access to your data center, and should therefore, be deemed as higher risk than a regular or low-risk facilities vendor. In theory, the contract should address the inherent risk rating, and give you the residual risk.

2. Performance expectations and monitoring: Institutions need to understand what they want from their critical vendors, and how they are going to measure results. Performance criteria and relevant key performance indicators need to be formally established in the contract to measure vendor performance on a frequent and ongoing basis. It is often a good practice to openly communicate with vendors, and agree on the performance evaluation methods to avoid surprises when it comes to the need for performance improvements. Examples of key performance indicators include: error rate, processing time, transaction time or platform availability and uptime, response rate transaction throughput and accuracy.

One of the key problems we see is that the line of business is expected to manage the relationship and performance—yet has no visibility into the contract or the specific performance metrics by which the vendor should be managed. In our experience, very few institutions are doing performance management on more than just a handful of vendors. This in turn creates additional risk for the institution.

3. Contingencies and vendor replacement: In today’s business environment, it is important to expect the unexpected. A critical vendor’s systems can go down, due to a compromise or natural disaster. Key personnel may leave and threaten the stability of the organization, or the vendor may unexpectedly close their doors. These are growing concerns to institutions that have outsourced critical functions. To protect against these possibilities, establishing a practical and comprehensive contingency plan that addresses critical vendors is very important to mitigate service disruption risk.

What are the advantages of a robust vendor management program?

Vendor management involves awareness of critical vendors and the services they perform. It also involves evaluation of performance, and taking appropriate actions with specific vendors. Having a robust vendor management program in place allows an institution to be able to make best use of its service providers, as well as respond to inquiries from management, auditors and regulators. More importantly, you will be able to leverage your critical vendors to help your business grow and succeed.

The latest guidance from the OCC highlights the importance of understanding the risk associated with the specific goods or services that a particular third party is delivering—versus the risk associated with the vendor themselves. Therefore, you need to review the scope of work your third parties are providing. That may include routine third parties such as maintenance or HVAC that normally would not be assumed to have access to NPI.

As we have recently learned, it is important to look at each third party on a case-by-case basis through the prism of size, scale and complexity in the context of your organization, and in accordance with your risk appetite. Again, look at protecting your company by examining the factors that the third party could influence if the arrangement goes badly:

- What will the impact be on my business strategy?
- What could the impact be on my reputation?
- What could the impact be on my operational risk?

Once again, remember not every third-party relationship may rise to the level of critical activity, as defined by the OCC. However, that does not absolve you from assessing the level of risk associated with any vendor or supplier, and assuring you have the relevant controls in place, even if third parties are not at the level of needing board approval. You should be risk assessing the magnitude of your supply base or your third-party relationships, so you can fully understand the various risks they all present to you.