McKinsey&Company

JULY 2013

Managing when vendor and supplier risk becomes your own

Hamid Samandari, John Walsh, and Emily Yueh

Financial institutions are being held accountable for the actions of their suppliers. A new approach can help to identify and manage sources of third-party risk.

The rising tide of regulatory scrutiny stemming from the global financial crisis has now reached beyond banks, to the companies that supply them. Under the broad notion that activities can be outsourced, but responsibility can't, the Consumer Financial Protection Bureau (CFPB) and other regulators are holding financial institutions responsible not only for their own actions but also for those of their vendors and suppliers. In the past year, for example, American Express, Capital One, and Discover Bank have paid a total of more than $530 million to settle complaints of deceptive selling and predatory behavior by their third-party suppliers.

This new regulatory thrust poses a big challenge for financial institutions because some of them have a limited perspective on their suppliers' interactions with customers. The largest banks and credit-card companies can have close to 50,000 suppliers. They are quite careful about some of these relationships and often have teams to manage large and midsize suppliers. Of course, many vendors provide paper, computers, and other innocuous goods and services. But a significant number of vendor relationships are not closely managed, and some carry hidden risks. A company that molds and prints credit cards, for example, is entrusted with customer data, and that poses any number of privacy and security risks.

At many institutions, vendor-management programs have focused predominantly on risks to the bank and the financial system—specifically, on business continuity, financial strength, and credit risk. With the scope of regulatory oversight broadening to include the consumer, many firms are underprepared. But since financial institutions must bear the responsibility for their suppliers' misdeeds, they must improve the way they manage these relationships.

In response to the changes, financial firms are looking for new solutions to identify and manage third-party risk. A number of leading banks and credit-card companies are developing and embracing best practices. Our research and experience have helped us develop a comprehensive approach to managing third-party risk. It consists of six essential steps, some of which can be executed in parallel.

1. A comprehensive inventory of third parties

Regulators now expect institutions to know their third parties, how each of them interacts with consumers, and what activities it performs. Many firms do not have this information readily available. Supplier databases can be incomplete, and some of the most sensitive risks can reside in relationships that are not found in them. Cobranded partnerships, joint ventures, sponsorships, and similar relationships can account for up to 80 percent of the spending that some business units assign to suppliers. But these relationships are often managed in ways that emphasize commercial goals, with only a secondary focus on risk. What's more, in some firms individual business units have different ways of tracking their suppliers, making it difficult to compare and collate them across an entire organization.

In our experience, an effective database of third parties includes all of them—that is, any noncustomer entity with which a financial institution has a business relationship. An enterprise-wide survey is a good way to get started.

2. A comprehensive catalog of third-party risks

To monitor consumer risk successfully, firms must develop a comprehensive catalog of these risks, also known as breakpoints, which form the basis for scorecards, audit routines, and other monitoring activities. Consider one breakpoint for a third-party call center: if there is a risk that agents will misrepresent product information to customers, a bank may investigate this specific problem by having calls monitored and may request regular reports on their quality and on customer-escalation metrics (exhibit). Identifying the relevant breakpoints for each category of suppliers and determining the relative weight and importance of every breakpoint can be challenging. Building a master register of breakpoints and their associated risk weights for all of these categories can help. Although broadly relevant to most firms, the master register can be adapted to the particular circumstances of an individual organization and its unique third-party relationships. This process is essential, as it helps the firm identify the true drivers of its risks and guides its mitigation program.

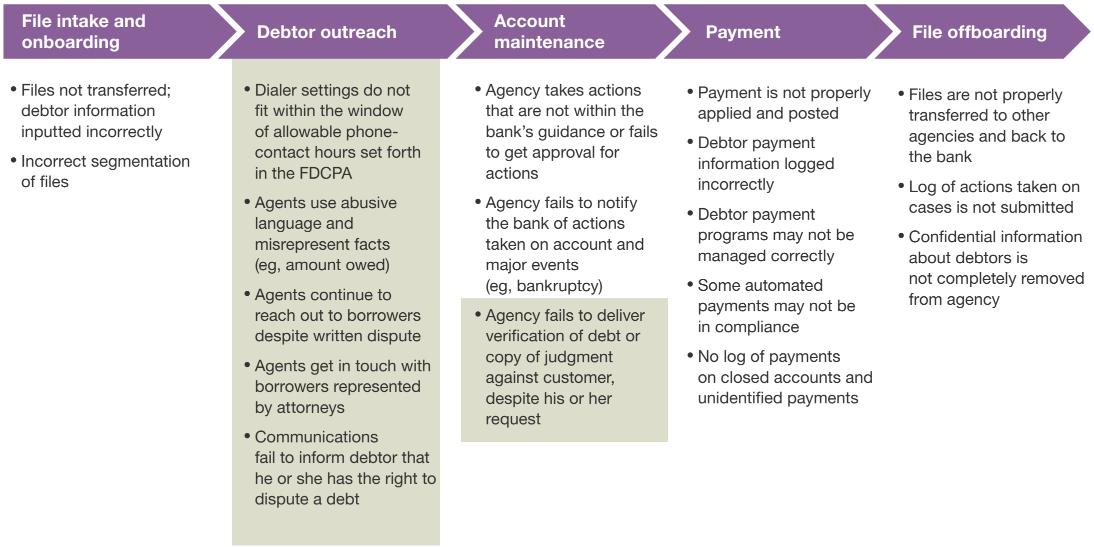
3. A risk-based segmentation

Once a firm has a complete inventory of third-party suppliers and the risks they pose to customers, it can segment its suppliers by risk level. Even a simple system of high-, medium-, and low-risk categories can be useful. We have observed that most leading institutions have 200 to 300 high-risk relationships at a time, irrespective of the total number of third parties with which they contract. An effective segmentation can help a firm determine how to utilize its resources strategically. It may, for example, conduct additional due diligence on high-risk relationships and automate regular reviews of low-risk suppliers.

Exhibit To mitigate risk, companies should tailor oversight to specific breakpoints.

Example: selected breakpoints for a third-party call center in the United States

▨ Violation of US Fair Debt Collection Practices Act (FDCPA)



File intake and onboarding	Debtor outreach	Account maintenance	Payment	File offboarding
• Files not transferred; debtor information inputted incorrectly • Incorrect segmentation of files	▨ • Dialer settings do not fit within the window of allowable phone-contact hours set forth in the FDCPA ▨ • Agents use abusive language and misrepresent facts (eg, amount owed) ▨ • Agents continue to reach out to borrowers despite written dispute ▨ • Agents get in touch with borrowers represented by attorneys ▨ • Communications fail to inform debtor that he or she has the right to dispute a debt	• Agency takes actions that are not within the bank's guidance or fails to get approval for actions • Agency fails to notify the bank of actions taken on account and major events (eg, bankruptcy) ▨ • Agency fails to deliver verification of debt or copy of judgment against customer, despite his or her request	• Payment is not properly applied and posted • Debtor payment information logged incorrectly • Debtor payment programs may not be managed correctly • Some automated payments may not be in compliance • No log of payments on closed accounts and unidentified payments	• Files are not properly transferred to other agencies and back to the bank • Log of actions taken on cases is not submitted • Confidential information about debtors is not completely removed from agency

In our experience, firms typically use either of two approaches to segment third-party suppliers. Companies that follow the score-based approach conduct due diligence across all dimensions and use the results to develop a composite risk score. Although very thorough, this approach can be onerous and resource intensive for many organizations. Using the rules-based approach, a firm identifies specific rules or criteria for each segment and thereby streamlines the process of assigning suppliers to risk categories. In fact, this approach is about 40 to 60 percent faster than the score-based one. Given the importance of an approach to segmentation, leading institutions tend to invest heavily in designing it. Typically, they appoint a core team of risk experts to lead the design, the fine-tuning, and the implementation.

4. A rules-based due-diligence test

Today, firms are expected to expand their due-diligence efforts beyond the traditional assessments for supplier, operational, and IT-security risks. Regulators are increasingly sensitive to strategic and reputational risks that third parties can create for customers. Traditional approaches align specific due-diligence activities with the risk category identified by the risk-based segmentation; a supplier in the high-risk category is subject to all due-diligence investigations. Like the score-based segmentation approach, this one can be overly onerous and resource intensive. Here too the rules-based approach can be a better answer because it triggers an appropriate set of due-diligence activities for the risks identified. For example, even if a third party is deemed to pose a high risk, an information-security or data-privacy screening is unnecessary if the supplier does not hold information that personally identifies customers. We estimate that the rules-based approach can cut employee time by close to 40 percent.

5. A disciplined governance and escalation process

Organizational alignment is particularly important when decision-making rights are spread across a range of businesses and functions, such as procurement, compliance, and operational-risk management. By proactively establishing governance structures and processes to address misalignments, institutions can resolve challenges quickly.

Governance can be centralized or decentralized; both models (and some hybrids) can be successful. In the centralized model, most major risk decisions reside within a single group, such as procurement or shared services. While the centralized model identifies a clear and accountable "owner," it can sometimes lead to tension between the business unit that has a working relationship with a third party and the centralized body accountable for risk assessments.

In the decentralized model, the business unit that owns the relationship also manages the risk. This arrangement can sometimes result in a duplication of resources: several business units may, for example, assess a major third-party supplier for similar contracts. In some cases, the application and alignment of risk standards can be inconsistent in a decentralized model: the groups managing, say, procurement and operational risk could have different perspectives. A hybrid approach, carefully tailored to the organizational context, can help mitigate challenges associated with the two models as long as risk ownership is clear.

An escalation framework is critical to resolve issues—such as requests for exceptions and the resolution of third-party breaches—that exceed the decision-making limits set out in the governance structure. While most organizations have an operational-risk management group, its governance model and mandate might not be sufficient to address the additional volume of third-party issues. In our experience, leading financial institutions often choose to assign new responsibilities to standing committees rather than create new ones to support third-party escalations. Each organization must find an appropriate approach given its appetite for risk and its culture.

6. An integrated management-reporting and workflow process and tools

Clear, actionable management reports and well-designed workflow systems are essential for accountability across the business units, compliance, and audit. To work well, these tools must track and monitor the relevant data. More important, they must aid the workflow within and across business units and give managers a clear picture of real-time risk, with actionable recommendations. In our experience, most organizations currently have tools that address one or two of these functional needs, but to our knowledge none has a single tool that performs all three.

Building a new third-party risk application from scratch is a big undertaking; so too is enhancing a current risk tool to perform new functions. Some firms have turned to off-the-shelf workflow- and risk-management tools that can easily be customized to an organization's specific needs.

■ ■ ■

Risks from vendors and suppliers pose a significant challenge to financial institutions. A systematic approach to managing those risks can lower costs and help banks present a coherent approach to all key stakeholders, including regulators.

For more on this research, download the full report, *Managing third-party risk in a changing regulatory environment*, on mckinsey.com. □

The authors would like to thank Dmitry Krivin for his contribution to the development of this article.

Hamid Samandari is a director in McKinsey's New York office, where **Emily Yueh** is a consultant; **John Walsh** is a senior expert in the Washington, DC, office.