Deloitte.

Blind spot

Banks are increasingly outsourcing more activities to third parties. But they can't outsource the risks.

For anyone familiar with the banking industry, it comes as no surprise that banks are relying more heavily on vendors and other third parties now more than ever before. Plus, as banks look to focus their efforts, vendors are performing a wider range of functions, developing new products and services to meet rising demand from banks. From back office functions like payroll processing and mortgage servicing to evolving customer service channels such as electronic banking, mobile payments, and social media, third parties are showing up in some interesting places today.

As a result of these expanded arrangements, banks may benefit from much more than cost savings: relying on vendors to help them reach more strategic business goals such as enhanced performance and new product innovation. Cost is only the beginning.

You can outsource the work, but not the risk

As banks increase their dependence on vendors, they may also be taking on something far less desirable: mounting risk exposure. While third-party vendors may be developing the products or providing outsourced operations, the banks that hire them may be stamping these products and services with the bank's name. If a data breach occurs, a disruption to online banking services strikes, or a product or service misfires, customers are likely to point to the bank, not the vendor.

No matter how effective banks are at managing vendors, there is no way to outsource the risk that comes with such an approach. In the end, the banks are ultimately responsible — and the impact on their reputations, financial viability, and customers may be significant. As the complexity and volume of these arrangements grow, many banking leaders may fear that when it comes to risk, their blind spot is growing, exacerbated by their loosening grip on many business processes and activities.

Unless you've experienced the repercussions from a vendor arrangement gone wrong, it can be tempting to think your organization is immune. But scratch below the surface and what you find may be alarming. Here are a few questions that may reveal gaps in your approach to managing vendor risks:

- How does your bank identify its risk exposure to vendors? Does it solely rely on spending levels?
- What contingency plans do you have in place if a supplier for a critical process goes out of business?
- Does your bank have a central repository for all its vendor contracts?
- How does your board of directors deal with the issue of vendor risk exposure? Is the board involved in providing oversight at all? Are they being apprised of key relationships and status?
- How familiar are your vendors with consumer financial protection laws, e.g., Unfair, Deceptive, or Abusive Acts or Practices (UDAAP)?

- Are you having a risk and control discussion early enough in the process when sourcing and onboarding vendors?
- Which risk management and internal audit activities are in place to mitigate risks? How strong are they?

Renewed interest from regulators

The idea that banks are responsible for the risks undertaken on their behalf by vendors isn't exactly new. In fact, these responsibilities were clearly outlined in the Office of the Comptroller of the Currency's OCC 2001-47 Bulletin, which was issued November 2001.[1]

What *may be* new is the level of interest that regulators have recently shown when it comes to this issue. As banks have expanded their arrangements with vendors, regulators such as the new Consumer Financial Protection Board (CFPB) have ramped up their scrutiny of risk management, especially focusing on bank interactions with their customers. Deceptive, high-profile marketing practices in areas such as credit card offerings have only bolstered their interest. As a result, regulators expect banks to proactively identify potential risks, verify compliance, and monitor changes. If banks don't comply with consumer laws and other regulations, they could take a hit to their reputation and incur significant fines and other penalties.

Banks already have mature controls and approaches that help lock down IT and security risks. Today, they should consider the need to apply the same rigor and discipline to managing the risks that come with their relationships with vendors.

Different vendor risk categories require different approaches

Some banks have thousands of relationships with third-party vendors based on the type of operation or service they are providing. While a single vendor may provide several different services, the risks associated with each arrangement can be quite different. Plus, not all suppliers are created equal — some services and relationships may be more critical than others and some vendors may have more robust risk management than others.

Given this complexity, it can help to divide vendor risks into categories. There are a number of risk categories banks may want to consider when dealing with third-party vendors — including strategic, reputation, compliance, operational (including information security) and business continuity.

For example, a vendor with most of its resources and operations in one location may pose a concentration risk

[1] Office of the Comptroller of the Currency OCC 2001-47 Bulletin on Third-Party Relationships http://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-47.html

to a bank. If a natural disaster strikes, it could prevent the vendor from providing services. If neither the vendor nor the bank has contingency plans in place, the bank could be exposed to significant risks. The same goes for banks that depend heavily on a single supplier for a critical process. What happens if that supplier goes out of business, or if its operations are even temporarily disrupted?

These are only two of the most obvious scenarios banks should be on guard against when it comes to managing vendor risk. A deliberate, comprehensive approach to mapping risk exposures like these is essential for leaders looking to allocate their resources more effectively. With such a map in place, they may be able to prioritize each risk and apply the right mix of policies, procedures and controls to keep them in check. For example, what terms could be added to a contract to ensure the supplier has the right business continuity plan in place? How will the plan be evaluated? What exit strategy should the bank have in place in case it needs a new supplier? One of the more effective ways to answer specific, important questions like these is to have a full view of the vendor-related risks facing your organization.

Three lines of defense

While many banks have risk management practices and policies in place, they may not always periodically check to see whether the practices are effective, adequate and adhered to. To address this problem, banks may want to consider adopting a governance model — one that applies three lines of defense to enhance risk management. To address this problem, many banks are applying a three lines of defense approach for risk management of their vendor relationships. Although three lines of defense models have been implemented for managing other types of risk throughout the banks, increased risk management responsibilities and expertise are being applied to the vendor risk area."

What to do

- Identify critical third-party arrangements
- Maintain accountability of vendor risk management practices
- Determine risks and mitigation strategy
- Implement key controls

First line: Layered risk management among vendors and banks

The first line of defense may require taking a shared approach for managing controls and risks among banks and vendors across all their business relationships. The banks own the responsibility and accountability to manage risk, including oversight of the controls that lie with the vendor, which means that controls lie within both entities. For example, consider an agreement between a bank and a marketing company that provides the bank with add-on products or services. The bank could add language to the agreement that clearly spells out the approved risk monitoring practices for both parties, as well as specific procedures for assessing the effectiveness of controls and notifying the parties of breaches.

Adopting a shared approach may not mean the responsibility is shared equally. Banks and their business units have the responsibility to conduct vendor due diligence before any agreement is signed with a third party. Along the way, Banks may realize there are certain functions and processes in which the risks would be so high that they wouldn't want to outsource them or have third-party relationships in those areas. For instance, some banks may decide the risk to offshore its customer service unit — despite the cost savings and practicality of 24-hour coverage — may not be ideal for their organization. Similarly, some activities may simply be too sensitive to outsource. For example, engaging a vendor to perform end-to-end activities relating to anti-money laundering or information security management.

What to do

- Provide consistent vendor engagement processes across all lines of business
- Establish vendor risk management procedures and standards
- Develop guidelines, tools, and templates
- Interact with regulators on vendor risk and information security topics

Second line: Enterprise-wide approach

The second line of defense involves defining and implementing enterprise-wide strategy, policies, and standards — and monitoring those activities across the banks enterprise-wide vendor relationships. Following this approach, banks coordinate risk management activities across multiple risk and control functions for an integrated view of a third party's risks, compliance, and controls. While many banks may have taken steps to create a true enterprise-wide approach to risk, vendor risks may not have been a top-tier priority. With so many activities being outsourced today, vendor risk management is a prime candidate for an enterprise-wide approach.

What to do

- **Provide regulatory interpretation and guidance**
- **Perform periodic audits and testing to monitor compliance**

Third line: Internal audit

Once the first two lines of defense are in place, how do you know they are working? Without an examination, it may be impossible to tell. Internal Audit or an equivalent function could monitor and assess the effectiveness of the first two lines of defense on an ongoing basis. They could conduct regular and targeted reviews that vendor risk management practices are adequately designed and operate effectively according to bank policies and regulatory requirements.

Other emerging capabilities

In addition to new governance models and other emerging capabilities, banks today may have access to a host of evolving tools and capabilities to support their efforts. Because the tried-and-true practices — control assessments, information security risk tools, third-party financial stability analyses — may only take you so far. If you're planning to upgrade your approach to vendor risk management, you may want to be aware of evolving capabilities in the following areas:

Risk analysis and management. Today, banks may choose from a growing selection of evolving tools that offer specific capabilities for gauging and managing the risks that vendors may introduce to the organization. These tools are able to link supplier inventories, statements of work, contracting authorities, portals, and systems, giving leaders a detailed look at the risks and risk characteristics of third-party relationships and contracts. They may also be able to report on the effectiveness of controls and risk management practices used to mitigate the risks of each relationship.

Another dimension of risk management is the evolving of risk modeling, which offers a framework for managing both the inherent and residual risks of the supplier base. While tools have been around for a while, many powerful new versions may help bank leaders zero in on and prioritize vendor risks. From there, banks may apply a mix of controls, resources, and investments commensurate with the threat level the risks represent.

Enterprise-wide performance monitoring. While many banks may monitor the performance of service-level agreements (SLAs) at an individual supplier or relationship level, they may be unable to aggregate these at an organizational level. New enterprise scorecards may provide greater transparency into these high-risk relationships. Using these tools, for example, banks may be able to assess how hundreds of important, high-risk relationships are performing across the board — without having to delve deeply into each one.

Contract review. In negotiations with third-party suppliers and contractors, individual business units may not include certain terms and conditions that could help lessen risk. In some cases, banks may have to conduct audits of hundreds or even thousands of contracts to verify that certain clauses have been included. Evolving tools can help banks scour their contracts and confirm that certain terms and conditions, which help with risk management practices and controls, are embedded in them. The same process may also be integrated into backend systems to catch and remedy gaps.

Customer management. While it's not a new concern, many banks today have further elevated their focus on monitoring customer complaints and satisfaction on the

sales, marketing, and service offerings provided by their vendors. This is also an emerging concern for regulators like the CFPB, which has already taken enforcement action in some cases. As a result, banks may be trying to strengthen current processes or implement new ones that adequately monitor, report, escalate, and resolve third-party customer issues. For example, some banks are listening to customer calls with third-party vendors to find out if policies and procedures are being followed.

Impossible to ignore

Ask bank executives whether they have a plan for managing information security risks, and they are likely to give a tight, clear response detailing an integrated, comprehensive approach. Ask the same about vendor risk management, and you might hear a more tenuous response. Some may not have caught up with the rapid rise of vendor risks and some may have even overlooked it. A formalized, structured, and disciplined approach to vendor risk may be required.

To do that, banks should consider implementing a holistic, beginning-to-end vendor risk management program that combines current processes and practices with emerging capabilities. As an example, by applying third-party risk profiling and tiering to each vendor relationship, banks may be able to determine the appropriate mix of risk management practices and tailor them to the specific risks of an arrangement. These risks could potentially be evaluated and managed across the lifecycle of the vendor relationship, from selection to termination.

As another example, at the point of evaluation and selection, banks may have clear protocols — such as risk assessment, risk profiling, and more — to understand the risks that a vendor brings to the table. At the contracting and onboarding stage, they might pay special attention to issues such as contract language and exception management. During the management and monitoring phase, activities, including information security reviews and SLA and performance monitoring, rise to the fore. And when a vendor relationship is terminated, banks may undertake tasks such as confirming that the third party meets contractual obligations and removes all bank data. These are just a few examples of what a disciplined, comprehensive approach to managing vendor risk throughout the relationship might look like.

While regulatory scrutiny and compliance pressures may offer plenty of reasons to take a closer look at vendor risk, bank leaders also understand that forging stronger and safer vendor relationships may become a business imperative. As an example, banks may be franchising their names to vendors, who in -turn are offering more banking and non-banking products and services on the bank's behalf. If not handled properly, fallout from these joint marketing arrangements could potentially damage a bank's reputation and significantly impact its customer base and bottom line.

The issue at hand may be that banks do not have a holistic vendor risk program that considers different types of services provided and risk associated with them. The good news is that there's an emerging body of processes and technologies focusing specifically on this issue. The question is: What will you do about it?

To learn more, please contact:

John Graetz
Principal
Deloitte & Touche LLP
+1 415 783 4242
jgraetz@deloitte.com

Alfred Spahitz
Senior Manager
Deloitte & Touche LLP
+1 212 436 6955
aspahitz@deloitte.com

Walter Hoogmoed
Principal
Deloitte & Touche LLP
+1 973 602 5840
whoogmoed@deloitte.com

Christopher Spoth
Director
Deloitte & Touche LLP
+1 202 378 5016
cspoth@deloitte.com