THOMSON REUTERS
Westlaw®

Vendor management: Regulatory expectation and traps for the unwary

By Scott Sargent, Esq., *Baker Donelson**

NOVEMBER 13, 2017

Regulators have directed banks to effectively manage vendors for several years. The Federal Reserve,[1] Office of the Comptroller of the Currency,[2] Federal Deposit Insurance Corp.[3] and Consumer Financial Protection Bureau[4] have all issued guidance on what they expect from financial institutions that fall under their respective jurisdictions.

A rash of public data breaches, caused by third-party service providers, at several large retail companies led the regulators to strictly interpret their guidance during bank examinations. The recent disclosure of a massive data breach at Equifax will likely only reinforce the regulators' resolve to enforce effective vendor management practices.

The regulators' guidance outlined four steps for identifying and mitigating the risk from a third-party vendor: risk assessment, due diligence, contract structure and ongoing monitoring.

A bank's board of directors and senior management are responsible for managing the risk that third-party service providers pose to their institution. Therefore, it is incumbent upon every bank's management team to have an effective vendor management process that addresses the four steps outlined by the regulators as well as the termination of vendor services.

RISK ASSESSMENT

The bank should first determine whether outsourcing to a third-party vendor is consistent with its strategic direction. If it is, the bank should conduct a cost/benefit assessment that examines all risks associated with the outsourcing.

To start, the bank must consider whether there are qualified and experienced vendors to perform the service on an ongoing basis; whether it will be able to provide appropriate oversight and monitoring of the vendor; the resources that are required; and the contingencies that are in place for disruptive events.

Once these preliminary issues have been addressed, additional key risks arising from the outsourcing of functions to external vendors must be considered.

Country risk

Country risk is exposure to economic, social and political conditions and events in a foreign country that may adversely affect the vendor's ability to deliver the required level of service, and thus cause harm to the bank.

Reputational risk

To evaluate reputational risk, careful consideration must be given to the vendor, its location and the function that is outsourced to ensure that the relationship does not compromise the bank's reputation.

Operational/transactional risk

Risk analysis must include consideration of the practical ability of the vendor, including its subsidiaries and subcontractors, to perform its obligations. This analysis should entail, but not be limited to, the vendor's infrastructure, resources, training program, employee onboarding process, expertise, equipment, facilities, employees and corporate governance.

The regulators recommend that institutions manage operational risks introduced by the relationship with the vendor by adopting internal controls. Basic internal controls, including background checks, segregation of duties and dual controls,[5] are given as examples the regulatory guidance.

Compliance risk

Compliance risk analysis is performed to ensure the bank will comply with U.S. laws and regulations. Specifically, the bank should consider laws governing privacy, consumer protection, information security, record retention, the Bank Secrecy Act and the Office of Foreign Assets Control when evaluating the outsourcing and.

If the vendor is outside the United States, the bank should further consider federal restrictions on the exportation of certain types of encryption and software.

Concentration risk

Concentration risk analysis is performed to ensure continued operations are not jeopardized or potentially impaired by a limited number of service providers or those concentrated in the same geographic location.

Strategic risk

Strategic risk analysis looks at the bank's strategic plan for future development and growth to make sure it is not impaired by the outsourcing relationship.

Legal risk

An evaluation of legal risk determines whether the vendor will pose a risk of legal exposure, expense and/or litigation.

Financial risk

An assessment of financial risk involves examining the financial condition of the third party and whether it will financially be able to perform as agreed.

Credit risk

Credit risk must be considered when the bank is contracting with a third party to originate loans on the bank's behalf or when the third party solicits or refers customers, conducts underwriting analysis or implements product programs for the bank.

DUE DILIGENCE

The level of due diligence required is directly related to the degree of risk and complexity associated with the vendor's service. Critical vendors, as well as those with access to confidential data, particularly customer data, will require the most extensive due diligence.

Some regulators have observed that banks too often rely on their prior experience with the vendor or on positive recommendations from third parties as a proxy for due diligence and do not conduct their own thorough vetting of the vendor.

To address that problem, the regulators have determined that every outsourcing project should include a due diligence phase that incorporates the following elements:

- Strategies: The bank must ensure that the vendor's business strategy, such as plans for mergers and divestitures, aligns with its own.
- Legal and regulatory compliance: The bank should evaluate the vendor's legal and regulatory compliance programs to ensure the vendor has the appropriate licenses and the necessary internal controls and programs to provide the services in compliance with applicable laws and regulations.
- Financial condition: The bank should review the vendor's audited financial statements and otherwise conduct due diligence of its financial condition.
- Experience: Evaluation of the vendor's experience and reputation is a critical part of any due diligence practice. The bank should thoroughly examine the vendor's market share, resources, business model and prior results on other projects with other vendors, other partners or other banks.
- Fee structure: The proposed fee structure must be analyzed to determine if it creates inappropriate risks, such as a vendor charging high up-front fees or fees that could incentivize inappropriate behavior.
- Background checks: The bank must ensure that the vendor conducts thorough background checks on its management and other employees, as well as on subcontractors who have access to critical systems or confidential information.
- Security: The bank must assess the vendor's information security and physical security programs, and may require site visits to the vendor's facilities and/or a review of the company's internal and/or external audit reports.[6]
- Risk management: The bank should consider the effectiveness of the vendor's risk management program and internal controls. This generally will include a review of the vendor's internal audit department and its effectiveness, as well as a review of Service Organizational Control reports[7] and any external certifications.[8]
- Management of information systems: The bank should have a clear under-standing of the vendor's technology systems, processes, maintenance and compatibility with its own systems. It should also understand how the metrics expected from the service will apply to the vendor systems and schedules for upgrades and/or enhancements.
- Disaster recovery: The bank must evaluate the vendor's ability to deal with service disruptions from external and internal events and determine how those disruptions and recovery plans will impact its operations.
- Incident reporting: The bank should determine if the vendor has a satisfactory and sufficient process to identify, report, escalate and resolve incidents, including but not limited to those involving data security, employees, operational disruptions, compliance violations and legal claims.
- Human resource management: The bank should review the vendor's programs to train employees on policies and procedures and its process for dealing with violations and any failure of employees to pass internal screening procedures. Depending on the nature of the services provided, the bank may need to consider the vendor's succession plan for key personnel and its ability to continue to retain or attract employees with the skills needed to perform the services.
- Subcontracting: It is imperative that the bank assess any potential vendor's use of, and reliance on, subcontractors, and its ability to monitor and manage them. If the services provided by the subcontractor have the potential to impact the bank or if they involve customer information, additional due diligence may be required.

- Insurance: The bank must assess the vendor's insurance coverage to insure that appropriate types and levels of coverage exist.

CONTRACT STRUCTURE

Once the due diligence is completed and a vendor is selected, attention must be turned to documenting the relationship. The key provisions that should be considered in each service agreement are:

- Nature and scope of arrangement: A thorough and complete description of the services to be provided is at the core of any services agreement. The regulators also recommend that the description include ancillary services such as software or other technology support and maintenance, employee training and customer service.

- Performance measures: Service levels, metrics, deliverables or benchmarks are a second essential element of an outsourcing agreement. However, the regulators caution that performance measures should not incentivize undesirable performance, such as sacrificing accuracy for speed or to meet compliance requirements, or have an adverse effect on customers.

- Responsibilities for providing, receiving and retaining information: The regulators recommend that the contract require the vendor to provide and retain timely, accurate and comprehensive information that allows the bank to monitor performance, service levels and risks. Also, the regulators have recommended other reporting requirements that many vendors are not eager to accept:

  1. The prompt notification of financial difficulty, catastrophic events and significant incidents such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions or other regulatory actions.

  2. Personnel changes, or implementing new or revised policies, processes and information technology.

  3. Notification to the bank of significant strategic business changes, such as mergers, acquisitions, joint ventures, divestitures or other business activities that could affect the activities involved in the outsourcing arrangement.

To draft contractual provisions that meet regulatory expectations, careful consideration must be given to the nature of the services, the risk posed by the outsourcing and the nature of the parties' relationship — particularly when dealing with publicly traded companies.

Additional factors to consider include:

- Responsibility for compliance with applicable laws and regulations: The services agreement should address compliance with laws, regulations, guidance and best practices standards. Third-party service providers for banks should be made aware that they may be obligated to follow and implement rules, regulations and laws that apply to banks.

- Cost and compensation: Banks should ensure the contracts do not include burdensome up-front fees charged by the vendor or incentives offered by the vendor that could cause either party to take an inappropriate risk. The contract should specify the conditions under which the cost structure may be changed, including limits on any cost increases and penalties for failures to meet service levels or audit requirements.

- Ownership and license: The contract should include warranties by the vendor that any third-party intellectual property is licensed for the services provided, that such use will not infringe upon someone else's intellectual property and, in the case of software and/or hardware, the property will not transmit any unwanted or harmful programs to the bank's systems.

- Confidentiality and integrity: The contract must require the confidentiality of any information shared or provided to the vendor. It should also specify when and how the vendor will disclose information security breaches, regardless of whether the breach resulted in unauthorized intrusions or access that may materially affect the bank or its customers. In addition, the contract should address each party's power to change security and risk management procedures and requirements, and to resolve any confidentiality and integrity issues arising out of the shared use of the third party's facilities.

- Business resumption and contingency plans: The services agreement should require the vendor to provide the bank with disaster recovery plans, to conduct periodic testing of the plans and to share the results of those tests.

- Indemnification: The bank must be sure that any indemnities they provide to the vendor make sense from a risk management perspective and that any indemnities they get from the vendor appropriately assess the risks inherent in the relationship.

- Insurance: The services agreement should stipulate that the third party is required to maintain adequate and appropriate insurance coverage, notify the bank of material changes to coverage and provide evidence of coverage either periodically or on demand.

- Liability caps and dispute resolution: The bank also should determine whether any liability caps are in proportion to the amount of loss it might experience and

consider whether the services agreement should include a dispute resolution process. The bank should reject the all-too-common "annual fees paid" formulation, which service providers often utilize to limit their liability under any given contract with a bank to the amount of fees paid annually or some multiple of that amount, unless that amount is an accurate reflection of the bank's risk.

- Default and termination: In addition to provisions specific to deliverables, warranties, obligations and/or payments, the regulators identify three other points to be addressed in the default/termination clause of the vendor contract:

  1. The bank should determine whether the agreement includes a provision that enables it to terminate the contract, upon reasonable notice and without penalty, in the event that, among other circumstances, a regulator formally directs the bank to terminate the relationship.

  2. The services agreement should permit the bank to terminate the relationship in a timely manner without prohibitive expense.

  3. The services agreement should include termination and notification requirements with time frames that allow for the orderly conversion to another vendor.

- Customer complaints: If a vendor might receive complaints from customers, the services agreement should specify whether the bank or the vendor is responsible for responding. The contract should set forth specific standards for when a response is to be made or if the complaint is to be forwarded to a specific area of the bank. In those situations, the contract must also address retention guidelines for records of complaints and escalation procedures for customer complaints.

- Subcontracting: The services agreement should specify: (1) any specific activities that cannot be subcontracted; (2) whether the bank prohibits the vendor from subcontracting activities to certain locations or to specific subcontractors; and (3) that notification to the bank must be made before a subcontractor is engaged (giving the bank an opportunity to perform due diligence on the proposed subcontractor) or when an existing subcontractor is terminated. The bank should also have the right to terminate the services agreement without penalty if the vendor's subcontracting arrangements do not comply with the contract or if the bank does not approve a proposed subcontractor.

- Foreign-based third parties: Contracts with foreign-based third parties should include choice-of-law and jurisdictional provisions that provide for adjudication of all disputes under the laws of a specified jurisdiction. The regulators do not require that the jurisdiction or applicable law be the United States or a political subdivision thereof. Nonetheless, when a U.S. bank submits to the laws and jurisdiction of a foreign country, there should be a plan in place to protect its rights in that jurisdiction and an articulable reason for accepting the foreign jurisdiction.

- Regulatory supervision: While almost any function that a bank outsources may lead to the vendor being subject to examination by the regulators under the Bank Service Company Act, the regulators expect banks' contracts to stipulate that the vendor's performance is subject to regulatory oversight. This oversight includes, but is not limited to, access by regulators to all work papers, drafts and other materials.

ONGOING MONITORING

Once a contract is signed, banks need to establish procedures to monitor the vendor's activities on an ongoing basis, particularly when critical functions are involved. Banks also should ensure that their ongoing monitoring is prepared to adapt because both the levels and types of risks may change over the lifetime of third-party relationships.

Deliverables, metrics or service-level agreements identified in the contract must be tracked and monitored.

In addition, the regulators have identified a number of other issues that are not directly related to contract performance but nonetheless should be tracked and periodically evaluated. These include:

- Business strategy (including acquisitions, divestitures and joint ventures) and reputational matters (including litigation) that may create conflicting interests and impact the vendor's ability to meet contractual obligations and service-level agreements.

- Compliance with legal and regulatory requirements.

- Financial condition.

- Insurance coverage.

- Key personnel and ability to retain essential knowledge in support of the activities.

- Ability to effectively manage risk by identifying and addressing issues before they are cited in audit reports.

- Process for adjusting policies, procedures and controls in response to changing threats, new vulnerabilities, material breaches or other serious incidents.

- Information technology used or the management of information systems.

- Business continuity plans.

- The location of subcontractors and the ongoing monitoring and control testing of subcontractors.

- Agreements with other entities that may pose a conflict of interest or introduce reputation, operational or other risks to the bank.
- Ability to maintain the confidentiality and integrity of the bank's information and systems.
- Volume, nature and trends of consumer complaints, and in particular those that indicate compliance or risk management problems.
- Ability to appropriately remediate customer complaints.

Not surprisingly, these requirements are fairly duplicative of the due diligence that is necessary before a relationship is established. The regulators clearly expect the bank's analysis of the vendor to continue throughout the life of the relationship.

TERMINATION

Finally, banks should establish a process up front with the vendor to ensure a smooth transition to bring services in-house or to migrate to a new vendor in the event of contract expiration or termination.

This process includes data retention, the handling of intellectual property that was jointly developed by the parties, performance transition and training, and ongoing compliance with law.

Vendor management, as with every aspect of a bank's risk management program, is essential to a safe and sound financial institution. The vendor management program should be established with appropriate reporting structures so senior management and the board of directors have the information needed to control and monitor risk.

The vendor management program should also establish clear roles and responsibilities for managing relationships and integrating the risk management process into the bank's internal controls.

Finally, when appropriate, the bank should engage independent parties to review or audit a vendor's performance, processes, procedures, facilities or whatever else is necessary to assess the ongoing and potential risk posed by the vendor relationships.

NOTES

[1] Letter from Bd. of Governors of the Fed. Reserve Sys. to Officer in Charge of Supervision at Each Fed. Reserve Bank and Institutions Supervised by the Fed. Reserve (Dec. 5, 2013), http://bit.ly/2hiBvxj.

[2] OCC Bulletin 2013-29 (Oct. 30, 2013).

[3] *Guidance for Managing Third-Party Risk,* FED. DEPOSIT INS. CORP. (June 6, 2008), http://bit.ly/2zqJ7bs.

[4] *Compliance Bulletin and Policy Guidance; 2016-02, Service Providers,* CONSUMER FIN. PROT. BUREAU (Oct. 19, 2016), http://bit.ly/2AycK8C.

[5] "Dual controls" is a term widely used in business generally (and banking specifically) to refer to a security procedure requiring two (or more) people, processes or devices to corporate to complete a task or gain access to a system, resource or data.

[6] Most banking service providers, particularly those that are providing critical services and those that handle confidential data, have internal and/or external audits of their security, controls, risk management processes, governance, etc. The depth of the audits is directly related to the complexity of the operation.

[7] The Auditing Standards Board of the American Institute of CPAs adopted the Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. It is the national standard that is applied to report on a company's internal controls and the effectiveness of those controls.

[8] External certifications will depend on the vendor. Some may be part of a governing body that offers certifications; some may have paid for external certifications; or there may be no external certifications. It varies greatly depending on the nature of the service.

This article appeared in the November 13, 2017, edition of Westlaw Journal Bank & Lender Liability.

ABOUT THE AUTHOR

Scott Sargent, of counsel in **Baker Donelson**'s office in Birmingham, Alabama, advises community, regional and international banks on regulatory compliance and risk management. As part of his banking practice and work with financial technology companies, he helps his clients implement regulations and best practices concerning data security, privacy and protecting confidential information. He can be reached at ssargent@bakerdonelson.com.