Vital Relationships

Related Attorneys

Kimberly J. Schaefer

Related Industries

Financial Institutions

AUTHORED ARTICLE | Summer 2012

The Bankers' Statement – Summer 2012

Appeared in the Summer 2013 issue of *The Bankers' Statement*

Financial institutions increasingly look to vendor relationships, including all types of third-party relationships with service providers, as a way to gain a competitive advantage. Vendors can offer institutions a variety of safe and secure opportunities to improve overall success by, for example, reducing costs, performing functions on the institution's behalf and providing products and services that the institution does not offer.[2]

Reliance on vendor relationships, however, can significantly increase a financial institution's risk profile. Each institution's risk profile is unique and commands a tailored risk mitigation approach appropriate for the scale of its particular vendor relationships, the materiality of the risks present and the ability of the institution to manage those risks.[3] A financial institution's responsibilities to properly manage vendor relationships and identify and control the risks arising from such relationships lie with its board of directors and senior management.[4] Failure to adequately manage vendor risks leaves a financial institution exposed to regulatory action, financial loss, litigation and damage to its reputation.[5]

The Federal Deposition Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC) require, and the Board of Governors of the Federal Reserve urges, financial institutions to control risk and oversee vendor relationships.[6] Each agency has issued guidelines pertaining to such requirements.[7] Given the uniformity among all three sets of guidelines, the Federal Financial Institutions Examination Council (FFIEC) has compiled them and created a comprehensive handbook to aid financial institutions in vendor management and oversight.

Many vendor relationships should be subject to the same risk management, security, privacy, oversight and other consumer protection policies that would be expected if a financial institution were conducting the activities directly.[8] An effective vendor management

program should provide the board of directors and senior management with the framework to identify, measure, monitor and control the risks associated with outsourcing to a third-party vendor.[9]

The key to vendor oversight is effective risk management, which involves several key factors, as noted in the FFIEC Handbook:

- Establishing senior management and board awareness of the risks associated with vendor agreements in order to ensure effective risk management practices;
- Ensuring that a vendor arrangement is prudent from a risk perspective and consistent with the business objectives of the financial institution;
- Systematically assessing needs while establishing risk-based requirements;
- Implementing effective controls to address identified risks;
- Performing ongoing monitoring to identify and evaluate changes in risk from the initial assessment; and
- Documenting procedures, roles or responsibilities and reporting mechanisms.

The Importance of Documentation

Before delving into the specifics of vendor management, financial institutions must always keep one necessity in mind: documentation. As a financial institution proceeds through each step of vendor management, it must always document *everything* that relates to the vendor relationship, including valid contracts, business plans, risk analyses, due diligence and oversight activities (including reports to the board, management or other delegated committees). Documentation of the risk assessment is especially important to help ensure coordination, consistency and standardization between the financial institution and the vendor.[10]

This risk management process, as noted in each agency's guidelines and the FFIEC Handbook (collectively, the "Interagency Guidelines"), encompasses **four steps:**

1. Risk Assessment
2. Due Diligence
3. Contract Negotiation and Structuring
4. Ongoing Monitoring

The first three steps involve risk management procedures before a financial institution begins a contractual relationship with the vendor, while the fourth, and often overlooked step, involves continual oversight responsibilities throughout the vendor relationship.

Step One: Risk Assessment[11]

The Interagency Guidelines urge financial institutions to complete risk assessments on vendors that store or have access to confidential customer information or whose services have a major impact on the institution's operations.

The first step in the risk assessment process is to ensure that the proposed vendor relationship is consistent with the institution's strategic planning and overall business strategy. Because a risk analysis is so integral to an institution's overall strategic planning, it should be performed by senior management and reviewed by the board or an appropriate committee.

Next, management should analyze the benefits, costs, legal aspects and the potential risks associated with the vendor under consideration. Generally, the riskier a vendor's activity, the more important the need is for diligence in selection, contracting and monitoring. Risk is assessed by identifying threats and vulnerabilities, and then determining the impact the threats can have on a financial institution. A vendor may pose various risks, including strategic, reputational, legal, operational, transactional, credit and compliance risks.

The Interagency Guidelines recommend that management consider the following factors in evaluating the quantity of risk of the proposed vendor relationship:

- For risks pertaining to the vendor's function:
  - Sensitivity of data accessed, protected or controlled by the service provider;
  - Volume of transactions; and
  - Criticality to the financial institution's business.
- For risks pertaining to the vendor itself:
  - Strength of vendor's financial condition and its ability to maintain a long-term financial relationship;
  - Turnover of management and employees;
  - Ability to maintain business continuity;
  - Ability to provide accurate, relevant and timely management information systems;
  - Experience with the function outsourced;
  - Reliance on subcontractors;
  - Location, particularly if cross-border; and
  - Redundancy and reliability of communication lines.
- For risks pertaining to the technology used:
  - Reliability;
  - Security; and
  - Scalability to accommodate growth.
- For a risk/reward analysis:
  - Performance criteria and harm to the institution if a function failed;
  - Dependence on the vendor to perform an essential function;
  - In-house availability of the function; and
  - Availability of other vendors to provide same service if current one fails.

A financial institution should never assume more risk than it can identify, monitor, manage and control. After completing the foregoing assessment of risks, management should review its ability to provide adequate oversight of the proposed vendor relationship on an ongoing basis (see Step Four for more details). Appointing a senior manager to serve this function is recommended.

Step Two: Due Diligence[12]

The due diligence process provides management with the information needed to address qualitative and quantitative aspects of potential vendors to determine if a relationship would help achieve the financial institution's strategic and financial goals and mitigate identified risks. Similar to risk assessment, due diligence occurs not only when selecting a vendor, but it should also be an ongoing annual assessment of the vendor's performance and ongoing suitability. Due diligence should include consideration of strategic plans, vendor reputation, financial condition and ability to provide monitoring reports.

The scope and depth of due diligence is directly related to the importance and magnitude of the institution's relationship with the vendor. Obviously, vendors that are contracted to perform large-scale functions with sensitive data integral to the institution's success, a financial institution should perform an in-depth due diligence assessment.

Although many due diligence considerations overlap with risk assessment considerations, they are worthy of repetition. When evaluating a vendor on the front-end, management should consider the vendor's:

- *Operations.* To ensure that a vendor's operations are adequate, management should appraise the vendor's security procedures in handling customer's confidential information; internal controls, including change-control process; record maintenance; scope of management information systems, data security and privacy protections; and employee background checks. If the vendor is reviewed under the FFIEC's Technology Service Provider examination program, review recent Report of Examination's Open Section, which is available to serviced financial institutions. Further, management should consider the institution's ability to review the vendor's internal audits, the cost for additional system and data conversions or interfaces presented by the vendor, and the vendor's level of technological expenditures to ensure on-going support.
- *Financial condition.* This includes a thorough evaluation of the status of any financial audits, most recent balance sheet, income statement, SAS-70 report, SEC filings and any other relevant financial documentation. Further, management should consider the potential impact of economic, political or environmental risk on the vendor's financial stability. The ability of the vendor to take on additional investments that the institution may require should also be assessed. Finally, management should review the vendor's insurance coverage, particularly fidelity bond coverage, liability coverage, fire, data loss, document protection and other coverage in amounts deemed adequate for the services the vendor is to perform.
- *Staffing.* Management should evaluate the vendor's employees and management, including the quality, experience, training, competency and familiarity with the industry, particularly in dealing with situations similar to the institution's environment and operations. Similar considerations include the vendor's turnover rate and any shortcomings in the vendor's expertise that an institution would need to supplement in order to fully mitigate risks.

- *Reputation.* The vendor's reputation should be measured by assessing its length of operation; market share; references, ideally from other financial institutions; service philosophies and quality initiatives; reliance on third parties or subcontractors to provide the service; and the vendor's awareness of regulatory and legal requirements to which financial institutions must adhere.
- *Problem-solving skills*. Vital to disaster recovery is a vendor's ability to quickly resume service in the event of an operational failure, including the vendor's ability to respond to service disruptions. The institution should review any past or present complaints, regulatory actions or litigation against the vendor; any previous breaches in the vendor's security; the adequacy of the vendor's contingency plans should an issue arise; off-site or backup storage; and the willingness of the vendor to handle security incidents in the past, if any.
- *Location.* Although physical location becomes less important as global technology increases, management should nevertheless consider the vendor's ability to serve the institution if geographically distant, whether the vendor is located off-shore, and physical security of the vendor's premises.

Although a comprehensive due diligence assessment may yield an ideal vendor, a financial institution should stipulate a vendor's responsibilities in writing to ensure that it does not divert from its current status.

Step Three: Contract Negotiation and Structuring[13]

If a vendor passes the due diligence phase, management should negotiate a written contract that meets the financial institution's requirements. The contract should clearly set forth the rights and responsibilities of each party to the contract, including, but not limited to, the following:

- *Scope of the relationship.* The contract should specify: the timeframe covered by the contract; the frequency, format and specifications of the service or product to be provided; other services to be provided by the vendor, such as software support and maintenance, training of employees and customer service; costs and compensation; insurance coverage to be maintained by the vendor; default and termination rights; and indemnification. It should also contain guidelines for adding new or different services and for contract re-negotiation.
- *Performance measures and responsibilities.* The contract should clearly specify the expectations of each party. It should require that the vendor comply with all applicable laws, regulations and regulatory guidance. Further, there should be a provision addressing the permissibility or prohibition of the vendor to subcontract or use another party to meet its obligations with respect to the contract, and any notice or approval requirements.
- *Responsibilities for providing and receiving information.* The contract should provide authorization for the institution to monitor and periodically review the vendor for compliance with its agreement, as well as the frequency for which such information reports are to be received. Likewise, the contract should authorize the institution and the appropriate federal and state regulatory agency to have access to records of the vendor as necessary or appropriate to evaluate compliance. Institutions should consider requiring the third party to notify them in the event of financial difficulty, catastrophic events, material change in strategic goals and significant staffing changes, all of which might result in a serious impact to service.

- *Authorization to audit.* The institution should have the right to audit the vendor (or engage an independent auditor) as needed to monitor performance under the contract. Institutions should generally include in the contract the types and frequency of audit reports the bank is entitled to receive from the service provider (e.g., financial, internal control and security reviews). The contract should specify the audit frequency and any charges for obtaining the audits, as well as the rights of the institution and its regulatory agencies to obtain the results of the audits in a timely manner. The contract may also specify rights to obtain documentation of the resolution of any deficiencies and to inspect the processing facilities and operating practices of the service provider.
- *Confidentiality procedures.* Any nonpublic personal information of the institution's customers must be handled in a manner consistent with the institution's own privacy policy and in accordance with applicable privacy laws and regulations. Any breaches in the security and confidentiality of information, including a potential breach resulting from an unauthorized intrusion, should be required to be fully and promptly disclosed to the financial institution. Arrangements should address the powers of each party to change security procedures and requirements, and should resolve any confidentiality or security issues arising out of shared use of facilities owned by a third party.
- *Business resumption and contingency plans.* Most significantly, the contract should outline a contingency plan for the vendor's continuation of services in the event of an operational failure. The contract should address the service provider's responsibility for backup and record protection, including equipment, program and data files, and maintenance of disaster recovery and contingency plans. The contracts should outline the service provider's responsibility to test the plans regularly and provide the results to the institution. The institution should consider interdependencies among service providers when determining business resumption testing requirements. To ensure adequate preparation, the contract should outline notification requirements and approval rights for any material changes to services, systems, controls, key project personnel and service locations. The contract should also specify the potential liabilities of each party in the event of fraud or a processing error.

Furthermore, a financial institution may want to consider including service level agreements (SLAs) in the contract. SLAs are formal documents that outline the institution's pre-determined requirements for the service and establish incentives to meet, or penalties for failure to meet, the requirements. Financial institutions should link SLAs to provisions in the contract regarding incentives, penalties and contract cancellation in order to protect themselves against vendor performance failures. SLAs addressing business continuity should measure the vendor's contractual responsibility for backup, record retention, data protection and the maintenance of disaster recovery and contingency plans.

The foregoing list indicates that, oftentimes, a financial institution's ability to effectively monitor a vendor depends upon the provisions in the parties' contract. Likewise, the most important provisions to be included in a contract include those that pertain to the process for ongoing monitoring of the vendor, such as the authorization for the institution to monitor and periodically review the vendor for contractual and regulatory compliance. A similarly vital provision would be to require, as a condition precedent, a vendor to implement appropriate measures to prevent breaches.

Step Four: Ongoing Monitoring[14]

With an increasing use of third-party vendors comes an increased risk for incidents, including compromised data, breaches and cyber attacks. Accordingly, the responsibility to review third-party vendors does not stop once the contract is signed. Rather, financial institutions must continually — at least on an annual basis — monitor vendors. The authorization of a financial institution to monitor its vendors should be clearly stated in the contract.

To ensure an effective oversight program, a board may want to designate a senior manager to be responsible for the ongoing monitoring, ensuring that this senior manager possesses the requisite knowledge and skills to critically review all aspects of the vendor relationship.

Effective oversight means that, throughout the life of the contract, an institution should:

- *Monitor the vendor's financial condition.* Financial review should be as comprehensive as the credit risk analysis performed on the institution's borrowing relationships. For significant third-party relationships, institutions should review audited financial statements and follow up on any needed corrective actions. When reviewing the audit report, assess the following factors: the practicality of the vendor having an internal auditor and the auditor's level of training and experience; the vendors external auditors' training and background; and internal IT audit techniques of the vendor. Institutions should also ensure that the vendor's financial obligations to others are being met. A vendor's failure to provide adequate financial data may be a potential red flag that a vendor has serious financial stability issues. Also, management should review the adequacy of the vendor's insurance coverage.
- *Monitor controls.* Review the adequacy and adherence to the vendor's policies relating to internal controls and security issues. Verify that the vendor has a process in place to identify and assess new control exposures resulting from a change. If the vendor is reviewed under the FFIEC's Technology Service Provider examination program, review recent Report of Examination's Open Section, which is available to serviced financial institutions.[15] Review SAS-70 reports, paying particular attention to the "User/Client Control Considerations" section. This section states the controls that a financial institution should have in order to complement the controls at the vendor.

Documenting and Categorizing Vendors

As a preliminary matter, before a financial institution moves on to Step Four, it should assess its vendor relationships. Management should first create a list of vendors that have access to customer information, and, likewise, document the types of access that such vendors have, such as electronic access to customer data.

Next, a financial institution should categorize the vendors according to criticality. For instance, a vendor categorized as highly critical would mean that, if a breach were to occur, it could have a significant impact on an institution. In contrast, a vendor with low criticality may indicate that any issues involving the vendor would not gravely harm the institution. In categorizing vendors according to criticality, a financial institution generates a greater understanding of which of its vendors need more stringent, frequent oversight.

Finally, a financial institution should rank the vendors according to their level of risk, including consideration of any financial, operational or performance issues. Vendor relationships with higher risk ratings should receive more stringent and frequent monitoring for due diligence, performance and control reviews.

- *Evaluate the quality of service and support.* First, evaluate the overall effectiveness of the vendor relationship and the consistency of the relationship with the financial institution's strategic goals. Assess the effect of any changes in key vendor personnel involved in the relationship with the financial institution. Review any licensing or registrations to ensure the vendor can legally perform its services.
- *Conduct performance review.* Review reports relating to the vendor's performance in the context of contractual requirements and performance standards, with appropriate follow-up as needed. Review reports on performance, audit results, penetration tests and vulnerability assessments, including servicer actions to address any identified deficiencies. Management may want to perform a walk-through of key business processes with the vendor, ensuring compliance with business and contractual requirements — particularly those that are driven by legal or regulatory requirements. Likewise, meet as needed with representatives of the vendor to discuss performance and operational issues, such as by reviewing customer complaints and the vendor's resolution of those complaints. Further, management should closely monitor the vendor's compliance with any SLAs. Specifically, the institution should develop: a formal policy that defines the SLA program; an SLA monitoring process; a recourse process for non-performance; an escalation process; a dispute resolution process; and a termination process.
- *Assess business resumption and contingency plans.* Review test results of the vendor's business-continuity plans, contingency plans and information-security programs to ensure the plans meet current business-recovery requirements and are adequately maintained. Verify through participation or direct observation that business continuity plans are being tested at least annually. Determine if offsite backup checks are frequently performed to meet the institutions' standards. Verify the integrity of the backup either through planned or random sampling. The adequacy of any training provided to the vendor's employees should be assessed, including how they respond to issues and customer complaints. Establish a primary point of contact at the vendor in the event of a breach or service interruption. Document and follow up on any problem in service in a timely manner. Assess service provider plans to enhance service levels. Finally, acquire a copy of the source code if a vendor becomes unwilling or unable to provide continued support.

Reliance on vendors to perform banking functions, to provide products or services to customers, or to provide services under an institution's name decreases management's direct control, and thus requires an increased oversight effort. The key to adequate oversight is to first establish, by contract, clear performance standards to which a vendor must adhere. The contract should set forth authorization for a financial institution to monitor and evaluate the vendor. The type and frequency of monitoring needs vary, depending on the complexity of the services provided and the division of responsibilities between the institution and its vendor. Thus, the number of personnel, functional responsibilities and the amount of time devoted to oversight activities will depend, in part, on the scope and complexity of the services outsourced. Nonetheless, a financial institution must bear in mind that its duty to conduct due diligence does not end once a contract is signed. Rather, due diligence responsibilities, including continual oversight, persist for the duration of the contract.

Conclusions[16]

Given the increased dependence on third-party vendors and the increased risks they pose, the importance of proper management and oversight is critical to a financial institution's success. The more access to customer information that a vendor has, and the more integral a vendor is to a financial institution's daily operations, the more thorough the evaluation and oversight must be. Likewise, financial institutions should bear in mind that these recommended procedures are not all-inclusive. Vendor management and oversight activities continue to evolve to keep pace with new technologies and business applications. To maximize benefits from vendor relationships, financial institutions should have an effective process for managing the associated risks. In the very least, senior management should be conducting the oversight procedures listed in Step Four at least annually. While even the most comprehensive set of oversight guidelines cannot fully prepare a financial institution for an operational failure on the part of its vendor, the implementation of adequate oversight procedures will certainly alleviate many detriments in the event of such a failure. The value a financial institution will derive from its use of vendor business relationships is directly proportional to the quality of management's strategic planning, due diligence and ongoing oversight activities.

Accordingly, a financial institution should immediately assess its relationships with vendors, analyze risks, evaluate existing contracts and implement internal procedures to move toward compliance with agencies' guidelines.

For more detailed information on vendor management and oversight, please see the applicable agency guidelines:

- FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, Information Technology Examination Handbook: "Outsourcing Technology Booklet," (June 2004), http://bit.ly/QbovSC
- FEDERAL DEPOSIT INSURANCE CORPORATION, Financial Institution Letter 44-2008, "Guidance for Managing Third-Party Risk," (2008), http://1.usa.gov/167maC
- BOARD OF GOVENORS OF THE FEDERAL RESERVE SYSTEM, SR-0017, "Guidance on the Risk Management of Outsourced Technology Services," (2000), http://1.usa.gov/MKGCiA
- OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC 2001-47, "Risk Management Principles," (2001), http://bit.ly/OjrlWr

---

[1] Ms. Schaefer would like to thank Megan M. Westenberg and Evan T. Nolan for their assistance in writing this article.

[2] OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC 2001-47, "Risk Management Principles," (2001), http://bit.ly/OjrlWr (hereinafter "the OCC Guidance").

[3] *Id.*

[4] FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, Information Technology Examination Handbook: "Outsourcing Technology Booklet," (June 2004), http://bit.ly/QbovSC (hereinafter "the FFIEC Handbook").

[5] FEDERAL DEPOSIT INSURANCE CORPORATION, Financial Institution Letter 44-2008, "Guidance for Managing Third-Party Risk," http://1.usa.gov/167maC (hereinafter "the FDIC Guidance").

[6] *See* Interagency Guidelines Establishing Information Standards, 12 C.F.R. § 364 app. B (2012); 12 C.F.R. § 30 app. B (2012); 12 C.F.R. § 170 app. B (2012) (discussing the FDIC's and OCC's requirements for banks to manage and control risk and oversee service provider arrangements); BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, SR-0017, "Guidance on the Risk Management of Outsourced Technology Services," (2000), http://1.usa.gov/MKGCiA, (hereinafter "the Federal Reserve Guidance")

[7] *See* the Federal Reserve Guidance, the FDIC Guidance, the OCC Guidance, and the FFIEC Handbook (collectively, "the Interagency Guidelines").

[8] The OCC Guidance.

[9] The FFIEC Handbook.

[10] The OCC Guidance.

[11] The material detailed in Step One is adapted from the Interagency Guidelines.

[12] The material detailed in Step Two is adapted from FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, eBanking IT Examination Handbook (August 2003), p. A-8; and the Interagency Guidelines.

[13] The material detailed in Step Three is adapted from the Interagency Guidelines.

[14] The material detailed in Step Four is adapted from the Interagency Guidelines.

[15] FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, Information Technology Examination Handbook: "Supervision of Technology Service Providers," Appendix C, http://bit.ly/QbpbaB.

[16] Portions of the material in the Conclusions section are adapted from the OCC Guidelines.

This article is for general information purposes and should not be regarded as legal advice.