



Vendor Management and Service Provider Oversight

An effective Vendor Management Program provides appropriate oversight and risk management of significant third-party relationships. We recommend that a thorough evaluation is performed on all vendors that have access to customer information and vendors who are deemed to be mission critical. Typically, vendor evaluations are performed annually by the Information Technology Steering Committee, and the results are forwarded to the Board of Directors.

An effective Vendor Management Program addresses the following areas:

- Risk Assessment
- Due diligence
- Financial condition
- Contract provisions
- Third-party reviews
- Third-party oversight
- Source code agreements
- Ongoing monitoring requirements

Risk Assessment

A successful vendor management program begins with the completion of a risk assessment to determine the risks vendors may present to the bank. The risk assessment should consider:

- How critical each vendor is to your company
- Whether the vendor has access to your financial institution's customer data
- What activities are performed by the vendor and the relative risk of each activity

You should also consider any items analyzed during the initial and ongoing due diligence efforts during the risk assessment process.

Due Diligence

Due diligence should, of course, be performed before selecting a vendor. However, you should also perform due diligence periodically throughout the vendor relationship. This is to make sure nothing has changed that would affect your decision to keep the vendor. The results of the due diligence process should be taken into account when the vendor management risk assessment is performed. Due diligence could include (but is not limited to) evaluating:



Due Diligence (continued)

- Vendor financial statements
- Vendor SAS 70 report
- Vendor management and employee turnover
- Vendor business continuity planning efforts (if applicable)
- Vendor geographic location
- Vendor company history and reputation
- Vendor legal and regulatory issues

Financial Condition

An annual appraisal of the vendor's financial condition is an important part of the Vendor Management Program. This assessment should be performed by an employee who is familiar with reviewing financial statements. The employee could prepare a short overview of the financial condition of each major vendor, and present it to the IT Steering Committee or the Board of Directors.

Contract Provisions

It is important for bank management to examine the contract provisions to ensure the specific expectations and obligations of both the bank and the vendor are documented and are being adhered to. Contract provisions to review typically include:

- Contract terms
- Automatic renewal and notification requirements
- Required service levels
- Disaster recovery capabilities
- Compliance with regulatory requirements
- Fees

Third Party Reviews

All third party vendors that store sensitive customer information should have a SAS 70 Type II (or Level II) audit covering control procedures performed on a regular basis. Management at your financial institution should review the SAS 70 report, paying particular attention to the "User/Client Control Considerations" section. This section states the controls that your financial institution should have in order to complement the controls at the vendor. Management at your financial institution should also assess any exceptions noted in the SAS 70 audit report and assess the vendor's response to the exceptions.



Third Party Oversight

The [FDIC FIL 44-2008 "Guidance for Managing Third Party Risk"](#) states:

An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution.

The term "third party" is broadly defined to include all entities that have entered into a business relationship with the financial institution, whether the third party is a bank or a nonbank, affiliated or not affiliated, regulated or non-regulated, or domestic or foreign.

The [guidance noted above](#) contains a list of recommended items to include in performance monitoring of third parties. Documentation of these activities should also be retained at the bank.

Source Code Agreements

A source code agreement allows the financial institution to obtain a copy of the source code if a vendor becomes unwilling or unable to provide continued support. The source code is often held in third-party escrow until such time that it is necessary to distribute the copies. We recommend that you review the software used by your financial institution to determine if you need to have a source code agreement with your vendor.

Ongoing Monitoring Requirements

The level of vendor supervision required is, of course, dependent on your financial institution's assessment of risk for service being provided by the vendor. The staff assigned to oversee each vendor should have the necessary expertise related to the service provided.

Please contact us if you have questions or concerns regarding your Vendor Management Program. We are available to help you with all aspects of developing a Vendor Management Program and monitoring vendor relationships. Call us at (901) 682-2431.

© 2009 Reynolds, Bone & Griesbeck PLC