Virtual Innovation
Availability | Recovery | Security

WHITE PAPER

VENDOR MANAGEMENT

Tips for Vendor Oversight

Vendor Management:

Tips for Vendor Oversight.

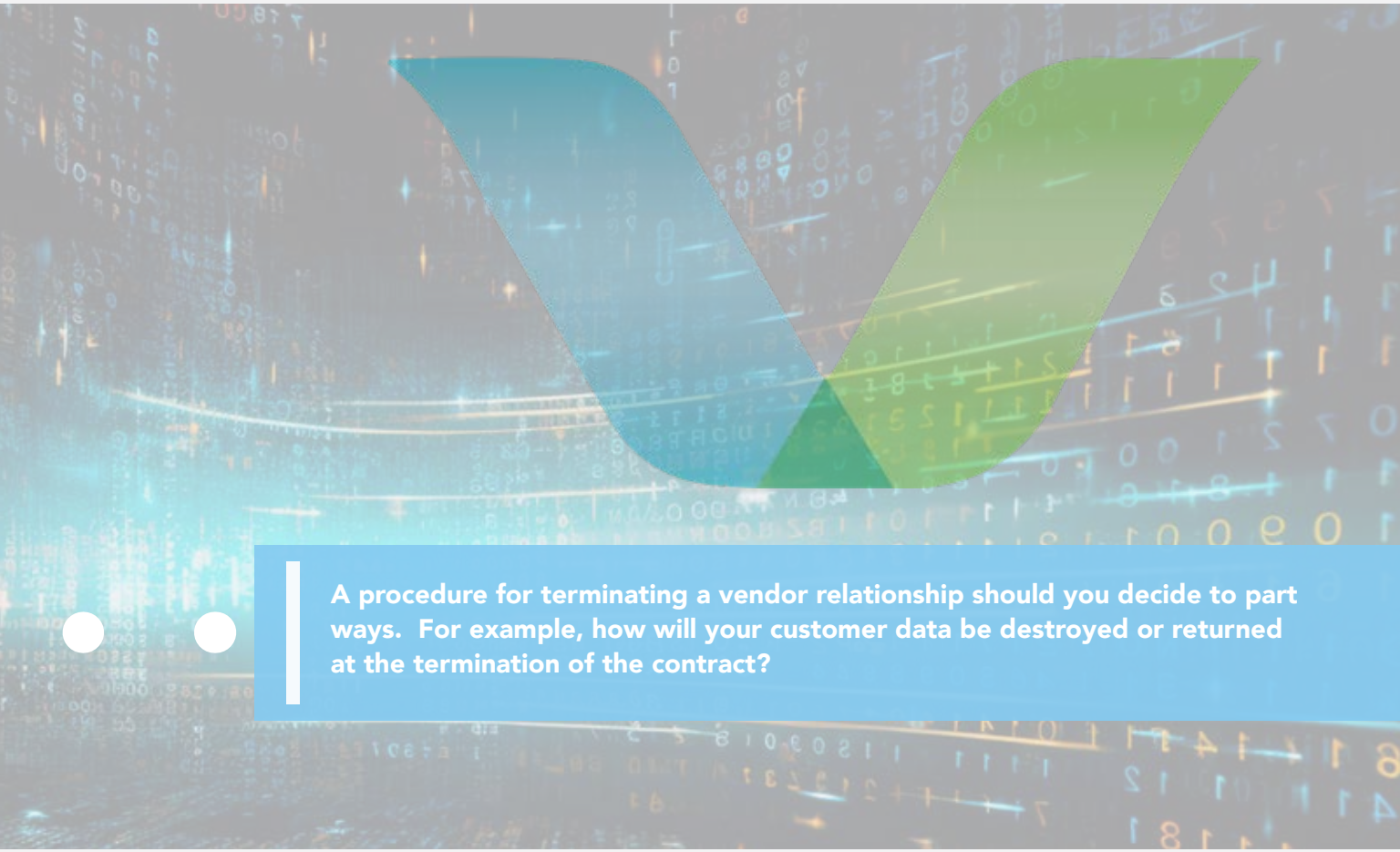
It's no secret that third-party vendors represent risk for financial institutions. Regulators hold financial institutions responsible for vendor activities and third-party offerings which hold or have access to customer data OR who hold a key role in your financial institution's operations. How can you be sure that your financial institution is doing everything possible to ensure that your vendors are good partners in your business? Read on for tips and best practices for third-party management.

TONE AT THE TOP

Your Board plays a pivotal role in vendor management. The first, and most essential, step in vendor management is setting a policy that mirrors regulatory guidance as well as reflecting the depth of your financial institution's reliance on third-party vendors.

Elements of a sound policy should include:

- An internal process for identifying the current and future strategic needs of the financial institutions against the current and future abilities of the vendor.
- A robust due diligence process, to ensure that the considered vendors can fulfill the duties of their contracted responsibilities, that the contracted vendors have the security systems in place to protect your customers data, and that there are acceptable insurance policies and limits of liability in place to protect your financial institution should there be a data breach or failure to provide services within their service level agreement.
- A vendor review procedure that reflects the risk associated with that vendor. For example, your core provider is critical to your success, so a more frequent review is essential to ensure that they are keeping their commitment to you. A vendor or third-party partner that does not hold or have access to customer data, or is not critical to your financial institution's operations, will not require the same frequency in its review.



A procedure for terminating a vendor relationship should you decide to part ways. For example, how will your customer data be destroyed or returned at the termination of the contract?

PRESCREENING

Prescreening begins internally by identifying the needs and wants of your financial institution and assessing these against the demonstratable abilities of the considered vendor partners. This thoughtful and reflective evaluation should determine if the vendor's strategic plan, including future objectives, align with your financial institution's strategic plan and future goals. Also, consider if you have the necessary resources to oversee the relationship. Once you've gathered this information, you can evaluate the potential risks and rewards of outsourcing an activity.

Due Diligence

Once you have narrowed your focus on prospective vendor-partners, a review of the contract and/or terms and condition considerations should include of the vendor's:

- Legal and regulatory compliance practices
- Proven operational controls (do they have a current SOC report?)
- Information security programs and practices
- Insurance coverage and limits of liability
- Financial condition
- Business experience and reputation (get references!)
- Fee structure and increase parameters
- Human resource management
- Subcontractors/"fourth party" vendor management process
- Incident reporting and risk management programs
- Business continuity plans – service level agreements
- Contract termination procedure

The goal of this step it to outline rights and responsibilities. Cost shouldn't be your only concern, though clearly it is an important concern. When drafting the contract, you should understand performance measures and benchmarks and ensure that there is recourse should the vendor perform at a level below their contracted obligations.

ONGOING MONITORING

Ongoing monitoring is essential as it helps a financial institution ensure that a vendor meets its contractual obligations. This includes the quality and sustainability of the vendor's controls and its ability to meet service-level agreements (SLAs), performance metrics, and other contractual terms. You should regularly review audited reports that assess the vendor's ability to meet their identified controls and other items as described in the above due diligence process.

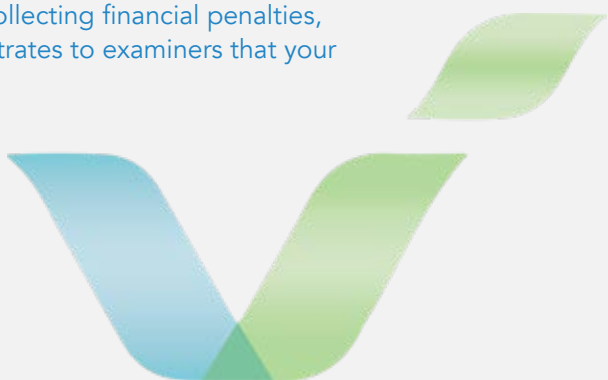
VENDOR COMPLIANCE PROBLEMS

Vendors make mistakes—we all do. Be sure you have plans in place to address when vendor mistakes are uncovered to ensure they are dealt with promptly and properly. This includes ensuring that your institution has policies and procedures for handling customer complaints related to a vendor. This is not just a potential vendor management issue. It's a regulatory expectation.

Ensure you have procedures for passing along information about vendor issues and train staff on what to do when an issue has been raised. Make it clear to whom information should be reported and how it should be reported. Include follow-up procedures to ensure nothing gets lost.

If you encounter a security flaw or other issue, ensure your staff knows exactly who to contact within your financial institution. Don't just send an email to a generic mailbox. When the issue has been raised to the vendor, ask for estimates for how long it will take to fix the problem, what will be done to solve it in the short term, and how you will be updated with developments.

Use your management tool for logging and track vendor issues so that they are remediated promptly and appropriately—or remain outstanding. With good incident management logs and findings tracking, you'll have the evidence to demonstrate non-compliance and show the vendor exactly where it's falling short of contract expectations. That can give you leverage in negotiating a new contract, collecting financial penalties, or even exiting the relationship, if necessary. It also demonstrates to examiners that your financial institution is proactively correcting the problem.



VENDOR DATA BREACH

Cyberattacks and data breaches are a growing problem requiring additional attention during vendor due diligence and ongoing monitoring. From identifying increased risk to mitigating it, here are things you should do.

Identify high-risk activities

A greater cyber risk that requires increased management oversight when it meets any of these conditions:

- Housing confidential data in a cloud-based system
- Housing or outsourcing confidential data offshore
- Outsourcing sensitive activities and key operations
- Conducting business transactions with customers using web-based services
- Giving access to confidential data to third-party providers

Cyber risk due diligence

Vendor cyber risk due diligence is not just important, it's crucial. This process ensures that the vendor has the necessary policies, procedures, and controls to guard against cyber risk.

What to look for:

- Controls: Vendor's committee should oversee cybersecurity controls, monitoring, protocols, and risk assessment.
- Protection: Both physical access and systems controls should be logged and monitored.

Email and customer data should be secure.

- Incident Response: Third-party vendors must have a response policy for incidents.
- Internal Controls: Controls that prevent or mitigate the severity of a cybersecurity attack.
- Business Continuity: Vendors must implement/test their business continuity.
- Human Resources: Access should be role-based/granted based on job function. Staff should be screened before hiring and undergo data safety training.
- Secure Data: There should be protocols, multi-factor authentication, during transmissions and storage, and protocols for safely destroying data.
- Cloud Risk: Cloud-based systems require additional scrutiny.

VENDOR DATA BREACH

As noted earlier, to mitigate risk, it is crucial to negotiate controls in the vendor contract. A well-designed contract should include notice of breach clauses and the right to audit the vendor's internal processes. The contract should also have policies to protect customer data and evolve with regulatory and technological changes. Maximize the value of controls by monitoring and mitigating risks regularly. Review audits and reports to ensure the vendor meets expectations. Use a monitoring system that provides assessments of the vendor's ability to resolve incidents, comprehensive documentation, and assurances that a vendor's cyber risk aligns with your institution's appetite for risk. The FFIEC Cybersecurity Assessment Tool (CAT) is one tool that can assess overall cyber risk and preparedness, including vendor relationships. The CAT will ensure preparedness aligns with risk appetite and identify controls or enhancements needed.

VENDOR MANAGEMENT PRACTICES

Working with your third-party "partners" is an essential part of managing your business. Regulators also recognize the critical role played by third-party vendors in delivering products and services, and the associated risks that come with outsourcing, which is why they take vendor management regulations very seriously.

Regulators are looking for the following practices:

- Documented processes: Vendor management should not be treated as an ad hoc activity. Examiners expect to see a documented plan for managing vendors and ensuring they remain compliant.
- Identification of compliance risks: Examiners want to see the identification of the risks of working with third parties. It's hard to guard against a risk if it's not known.
- Ongoing vendor management and risk management: Examiners expect ongoing monitoring of vendors to determine if anything has changed that would impact their ability to remain compliant.
- Justification for decisions: Examiners want to see the logic behind the decisions. Policies and procedures are not enough. If there's no good business case for the decisions, the whole program may be questioned.
- Resources to analyze reports and carefully negotiate and track contracts: Resources are necessary to oversee the vendor and analyze reports as well as track and negotiate contracts. These resources are essential to a compliant vendor relationship.
- Evidence of board and management oversight: Vendor management is such an important issue that board and management need to be involved, especially when it comes to critical vendors. Board meetings, minutes, and reports dealing with vendor management should be documented.
- Understanding of how vendor selection ties into ERM: Selecting a vendor is about aligning the benefits of the vendor relationship with your risk tolerance. Risk management plays an important role in ensuring that an institution's mission, vision, and values influence its strategy, strategic plan, and ultimately its strategic success.

VENDOR WARNING SIGNS

What are some of the signs you should look for when your third-party vendor is not meeting their contractual obligations?

- Third-party operations are inconsistent with laws, regulations, ethical standards, or bank policies and procedures.
- Third-party implements or manages a product or service in an unfair, deceptive, or abusive manner.
- Third-party doesn't comply with BSA or OFAC.
- Bank oversight lacks appropriate audit and control features (especially for new or expanded activities).
- Activities are further subcontracted without appropriate disclosure.
- Activities are conducted in foreign countries.
- Customer and employee data is transmitted to foreign countries.
- Conflicts of interest aren't appropriately disclosed or managed.
- Transactions aren't adequately monitored for compliance.
- Missing appropriate controls to protect consumer privacy and customer and bank records.

If it's not already there, you may wish to add specific language in your periodic review to ensure that you have current insight into your, or your vendors', practices.

Chicago Area
132 Venturi Drive
Chesterton, IN 46304
Phone: 219-405-6533

Phoenix Area
15550 S. 5th Avenue, #130
Phoenix, AZ 85045
Phone: 602-284-1505