Navigating Business Continuity Red Flags: A Guide for Banks

Third-party vendors play a crucial role in the banking industry as financial institutions and technology evolve to meet consumers' ever-changing needs. However, without a shared commitment to business continuity, vendor relationships can falter, potentially impacting operations, compliance, and customer trust.

In 2023, the Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), and the Federal Reserve introduced updated vendor management requirements, emphasizing the critical nature of robust vendor risk management practices.

To sustain compliant and effective vendor relationships, banks should proactively identify potential red flags and address them early, mitigating risks before they escalate into larger challenges.

Exploring common vendor red flags

Banks' vendor relationships look different based on their needs and the services and products the vendor offers, but there are some common challenges most financial institutions face in third-party relationships.

Reluctance to disclose information

Perhaps the most common red flag banks and other financial institutions face in vendor relationships is a lack of information. Vendors should willingly share business continuity plans, which detail how the vendor will continue to deliver essential products and services amid challenges, and disaster recovery plans, which cover how a vendor will regain critical systems and resume normal operations following an unforeseen event.

If a vendor hesitates to disclose how they protect critical systems, it may indicate potential deficiencies or issues they are trying to hide. In contrast, vendors that are open about their practices generally demonstrate strong security measures and commitment to maintaining operations during disruptions. For example, if your vendor talks about investing in their failover solutions, they are not only dedicated to protecting data and fulfilling compliance responsibilities—they want you, the financial institution, to know they do.

Lack of documentation

Some vendors are also reluctant to share essential documents. Examples of documents your institution can (and should) request include:

- **System and Organizational Controls (SOC) reports**. SOC reports are independent audits that assess a vendor's internal controls and security posture.
- **Complementary User Entity Controls document.** CUECs ensure adherence to security policies and compliance standards.
- **System recovery test results.** Business Impact Analysis (BIA)and disaster recovery test results demonstrate recovery effectiveness.
- **Security policies and procedures.** These methods protect sensitive data, including encryption and access controls.
- **Business policies.** These policies include change management, record retention, and vendor management policies (if subcontractors are involved).

There are circumstances when vendors may justifiably keep information private, as it contains proprietary technology and trade secrets that could harm the vendor's competitive edge if shared.

Outdated or irregular testing

To provide system recovery test results, vendors must conduct regular system recovery testing to measure how efficiently they can recover after a failure. If the vendor doesn't readily provide this data or relies on outdated recovery reports, it may hide weaknesses or problems in its operations.

Some examples of metrics your bank should request from the vendor include:

- **Recovery Point Objectives**. RPO reflects how much data an organization can lose and when it must be recovered from backups. A shorter RPO means less data loss.
- **Recovery Time Objectives**. RTO is the target time for restoring systems and operations after an outage. It's important to compare this with the critical departments' expectations to identify any gaps.
- **Maximum Tolerable Downtime**. MTD is the longest time a system can be non-operational without causing significant harm to the organization. Compare the vendor's MTD with departmental expectations.

It's normal to encounter challenges in the testing process. If your vendor shares its test results, challenges, and resolution plans, that indicates that the vendor is taking business continuously seriously.

Lack of fourth-party vendor information

Your bank isn't only responsible for what your vendor does. It's also responsible for the activities of your vendor's third-party vendors. For example, your vendor might use Amazon Web Services or Microsoft Azure for cloud services. In that instance, the cloud service is the fourth party.

But the circle doesn't stop there. The fourth party may outsource to another vendor, creating a fifth party, etc. This ongoing trend underscores banks' importance in managing vendor relationships.

Regardless of the level, it's crucial to consider how vendor risk affects your third-party management strategies.

Communication barriers

There's a high probability that many of your bank's vendor relationships have existed for a few years or even decades. However, while a partnership can start strong, communication barriers can occur over time, often signaling more significant issues ahead.

Communication problems are also common with new or inexperienced vendors. They may fail to properly communicate their processes or policies properly, potentially creating misunderstandings and leaving your bank unprepared to handle service changes or the resulting risks.

Remember, vendor risk doesn't occur in a silo. It can easily slowball and affect your entire organization's operational, reputational, and transaction risk, to name a few key areas.

How to approach vendor challenges

Whether your bank is navigating new vendor partnerships or revisiting existing ones, there are a few ways to approach current or emerging issues:

- **Initiate communication**. Have an honest conversation and voice your concerns. Clearly outline the issues and their consequences for both parties and express your bank's commitment to resolving the stated problems.
- **Update contracts**. If there are issues, there's a strong chance your existing vendor contract will need to be updated. If there's an existing contract, consider addendums. Some potential contract addendums may require the vendor to share test results and recovery times on a set schedule or to share protocols for addressing ransomware and other threats.
- **Talk to your peers and leadership team**. Unfortunately, your efforts to repair a vendor relationship may not work out because the vendor fails to address the issues or stops communicating. In these cases, seek out peers who share the same vendor

for advice. If the vendor continues to be unresponsive, escalate your concerns to higher leadership.

While navigating vendor relationships can be tricky, addressing and mitigating risks is crucial to ensuring a mutually beneficial partnership. Remember, if you see an issue, don't ignore it. Identify it, communicate your concerns with the vendor, and take appropriate action. Remember, even minor problems can escalate and affect your bank for years.