Everything You Need to Know About Vendor Risk Assessments

Partnering with third parties—or vendors—is often essential for operational efficiency in today's financial services landscape. Financial institutions of all sizes and resources are frequently using vendors, specifically financial tech (fintech) and banking-as-a-service (BaaS) providers. Sixty percent of credit unions and 49% of banks in the U.S. believe that fintech partnerships are important.

However, these external relationships come with significant potential risks, from data breaches and other cyber threats to operational disruptions. Moreover, most financial institutions aren't fully aware of their vendors' internal risk management practices and compliance standards, which adds another risk layer.

Enter vendor risk assessments, your key tool in identifying, evaluating, and mitigating risks associated with third-party vendors. With the proper vendor risk assessment, careful monitoring, and consistent communication, you can maximize vendor relationships while protecting your organization and customers.

But first, what exactly is a vendor risk assessment?

Why are vendor risk assessments so important?

The main objective of a vendor risk assessment is to ensure that a vendor can deliver services aligned with your institution's standards while minimizing potential vulnerabilities. This assessment should comprehensively review many factors, including the vendor's financial stability, operational capabilities, and ability to protect sensitive information.

Conducting a vendor risk assessment is part of the due diligence phase in the vendor risk management lifecycle. This process collects and analyzes documentation — such as System and Organizational Controls (SOC) reports and financial statements — to pinpoint any potential gaps or concerns that may pose risks to the institution.

Beyond compliance: More benefits of vendor risk assessments

Vendor risk assessments are essential in maintaining compliance, but too often, financial institutions start strong in evaluating vendors but fail to update their risk assessments over time.

Vendor risk assessments are more than a regulatory obligation; they can save your institution valuable time, money, and human resources, as well as gain a competitive edge by:

- **Identifying risks proactively**: By identifying risks ahead of time, institutions can implement controls and take necessary actions to mitigate potential threats, from data breaches and power outages to regulatory violations and reputational loss.
- **Enhancing oversight**: Regular assessments foster stronger scrutiny over vendor operations and accountability, ultimately leading to better management of third-party relationships. Remember, your vendor's risk is your organization's risk, too.
- **Informing strategy:** An effective assessment process equips financial institutions with the insights needed to make informed choices regarding vendor partnerships and align their decisions with strategic goals and risk tolerance.

Best practices for implementing vendor risk assessments

Effective vendor risk management starts with a structured approach to implementing risk assessments. Use these best practices as you revisit your institution's vendor risk assessments:

- **Take a tailored approach.** Customize the scope of the assessment based on the vendor's inherent risk level. Vendors with higher risks handling sensitive customer data, such as mobile and digital payment solution providers, should undergo more rigorous scrutiny than lower-risk vendors.
- **Evaluate inherent risks.** Inherent risk refers to risk that exists when there are no safeguards to mitigate issues. Before applying mitigating controls, assess the inherent risks associated with a vendor. Examine factors like access to sensitive information, the critical role of the vendor in operations, and potential vulnerabilities, such as cybersecurity risks and financial instability.
- **Tier vendor risk levels.** After completing the risk assessment, classify the vendor into a risk tier—low, medium, high, or other classifications that suit your institution's specific needs. This classification helps prioritize attention and resources.
- **Document and report findings.** Maintain thorough records of the assessment process, including due diligence results and recommendations. Documentation

is crucial for internal records and for demonstrating compliance to regulators. Remember, if it isn't documented, it didn't happen.

- **Continuously assess.** Vendor risk assessments should not be one-time events. Perform ongoing evaluations, especially when there are changes in the vendor's operations or shifts in the overall risk landscape.
- **Use a vendor management solution.** The right vendor management solution can make storing, tracking, and managing each aspect of the vendor management lifecycle, including risk assessments, more efficient and effective. The more aware you are of your vendors and their activities, the better your organization can confidently mitigate risk.

Vendor risk assessments are essential to the health and security of financial institutions. By recognizing their importance and adhering to best practices, your organization can manage third-party risk seamlessly and effectively and make better-informed strategic decisions—a win-win for your organization and customers.