New Supplementary TPRM Guide from Regulators Aims to Vendor Management Guidance Easier to Understand

By Rafael DeLeon

The release of the Interagency Guidance on Third-Party Relationships: Risk Management in June 2023 has left some community banks grappling with implementation challenges. Recognizing this, regulatory agencies published "Third-Party Risk Management: A Guide for Community Banks" in May, to help these institutions develop and implement effective third-party risk management practices.

The 24-page booklet, while not introducing new regulations, serves as a translator of sorts. It breaks down the dense June 2023 guidance into digestible chunks, offering community bankers (and even fintech companies and third-party vendors) a roadmap through the intricate landscape of vendor risk management with sample questions they should be asking.

Here are some of the key insights and critical reminders included.

Risk-Based Approach to Vendor Oversight

One of the guide's central themes is the necessity of a risk-based approach to vendor management. Not all third-party relationships pose equal risk, and therefore, they don't all require the same level of scrutiny. The guide emphasizes the importance of identifying and categorizing vendors based on their risk profile.

For high-risk or critical vendors, banks should implement enhanced due diligence and monitoring processes. This might include more frequent performance reviews, stricter contract terms, or more detailed reporting requirements. Conversely, low-risk vendors might require only basic oversight.

This risk-based approach not only helps banks allocate resources more effectively but also aligns with regulatory expectations. It's a crucial point for vendors as well, especially those providing critical or high-risk services. Understanding this perspective can help them prepare for the rigorous vetting process they're likely to face.

Comprehensive Vendor Management Lifecycle

The guide provides a detailed breakdown of the vendor management lifecycle, offering specific questions and considerations for each stage:

- **Planning:** What business need does this third-party relationship address? How does it align with the bank's strategic goals?
- **Due Diligence and Selection:** What is the vendor's financial condition? What are their information security practices? Do they have necessary licenses and certifications?
- **Contract Negotiation:** Are performance metrics clearly defined? Are there provisions for audits and regulatory examinations?
- **Ongoing Monitoring:** How frequently should performance be reviewed? What key risk indicators should be tracked?
- **Termination:** What are the exit strategies? How will data and services be transitioned?

For each stage, the guide not only poses questions but also suggests where answers might be found and provides examples of how a hypothetical community bank might approach these issues. This level of detail serves as an invaluable starting point for banks developing or refining their vendor management programs.

Governance as the Cornerstone of Risk Management

The guide places significant emphasis on governance, illustrating it as a triangle surrounding the vendor management lifecycle. This governance triangle consists of three key elements:

- **Board Oversight:** The guide stresses the board's role in setting the tone for third-party risk management. It suggests specific areas where board involvement is crucial, such as approving the overall third-party risk management program and reviewing critical vendor relationships.
- **Independent Reviews:** Regular independent assessments of the third-party risk management program are emphasized. These reviews could be conducted by internal audit, external auditors, or other qualified independent parties.
- **Documentation and Reporting:** The guide underscores the importance of maintaining comprehensive documentation and establishing clear reporting lines. It suggests highlights reports and documents, such as risk assessments, due diligence findings, and performance metrics.

The guide encourages banks to align their vendor management decisions with their strategic plans, ensuring that third-party relationships support overall business objectives.

Practical Implementation Strategies

While the guide provides valuable insights, some community banks may find implementation challenging. Here are several strategies for building a robust and compliant vendor management program:

1. **Leverage technology:** Many financial institutions are turning to vendor management software solutions to streamline their processes. These tools can help banks navigate vendor on boarding, risk assessments, contract management, due diligence, reporting, and other areas.

2. **Invest in training:** Vendor management is rarely a planned career path, with most professionals falling into the role without prior specialized education. This knowledge gap underscores the importance of vendor management training programs for staff.
3. **Seek expert assistance:** For banks that lack internal resources or expertise, engaging with consultants or specialized firms can provide valuable vendor management program support, including help building out programs, conducting due diligence and vendor risk assessments, and reviewing contracts, among other activities.

Conclusion

The new guide represents a significant effort by regulatory agencies to make third-party risk management more accessible to community banks. By providing practical examples, specific questions to consider, and a framework for risk-based oversight, it offers a valuable resource for banks navigating this complex landscape.

However, the guide is just that – a guide. Each bank must tailor its approach based on its unique size, complexity, and risk profile. By leveraging the insights provided in the guide, along with appropriate tools and expertise, community banks can develop third-party risk management programs that not only satisfy regulatory requirements but also effectively protect their institutions from third-party risks.

Remember, effective vendor management is not just about compliance – it's about safeguarding your bank's operations, reputation, and ultimately, its success in serving its community.

About the Author

Rafael E. DeLeon is a vibrant spokesperson with a wealth of knowledge on risk management, governance, and regulatory compliance for financial institutions. In addition to handling educational initiatives, thought leadership, and outreach to regulators, industry leaders, and association partners for Ncontracts, Mr. DeLeon is on the Board of Directors of MainStreet Bancshares, Inc., parent company of MainStreet Bank in Fairfax, Virginia.

Before joining Ncontracts, Mr. DeLeon completed a successful career spanning three decades with the Office of the Comptroller of the Currency (OCC), having most recently served as the Director for Banking Relations in the Office of the Comptroller of the Currency (OCC), as well as an OCC National Bank Examiner, trainer, and industry analyst who was sought after to speak at industry events nationwide.

Mr. DeLeon earned a Bachelor of Arts degree in business education from St. Mary's University in San Antonio, Texas.