Third Party Vendor Due Diligence Quick Reference Guide

Provided by the Independent Bankers Association of Texas

Purpose

As regulators and examiners place increased scrutiny on the management and oversight of financial institutions’ third-party relationships, the Office of the Comptroller of the Currency subsequently issued guidance (OCC 2001-47; RE: Risk Management Principles for Third-Party Relationships) to banks on managing the risks that may arise from their business relationships with third-parties. While the responsibility of oversight, management and appropriate and sufficient due diligence remains with the board of directors and management of Texas Community Banks, The Independent Bankers Association of Texas has summarized the OCC’s guidance to provide a quick reference guide as a resource to its members for evaluating and performing due diligence on third-parties.

Risks Associated with Third-Parties

**Reputation risk** arises when a third party’s service or products don’t meet the expectations of the bank’s customers, or when the third party or line of business is subjected to public scrutiny or experiences negative publicity.

**Strategic risk** arises when a bank doesn’t perform an adequate risk assessment or possess sufficient knowledge about a new product, business line, or activity—or when the activity is inconsistent with the bank’s goals or doesn’t provide the expected return on investment.

**Compliance risk** arises when the third party’s operations are not in compliance with law or the bank’s internal policies and procedures, and when audit and control features are weak or nonexistent. Banks must take special care to avoid violating fair lending and consumer protection laws.

**Transaction risk** arises when the third party is unable to deliver its product or provide its service due to error, fraud, or technology failure. Ineffective business continuity planning increases transaction risk. Credit risk arises from the third party’s failure to meet the terms of the contract or otherwise to perform as agreed, and when the quality of loans marketed or originated by the third party is inferior.

Depending on the circumstances, third-party relationships may also subject the bank to liquidity, interest rate, price and foreign currency **translation risk**. In addition, a bank may be exposed to **country risk** when dealing with a foreign-based service provider, which arises when the economic, social and political conditions and events in a foreign country will adversely affect the bank’s financial interests.

Risk Management Process

Banks should adopt a dynamic risk management process over third-party arrangements that includes:

1. An assessment of the risks involved in the activity and whether it coincides with the bank’s strategic goals
2. Due diligence to identify and select a third party provider
3. Written contracts that outline duties, obligations, and responsibilities of both parties
4. Ongoing oversight of the third party and third party activities

Because third-party relationships are important in assessing a bank’s overall risk profile, the OCC’s primary supervisory concern in reviewing a bank’s relationships with third-parties is whether the bank is assuming more risk than it can identify, monitor, manage and control. **Management and the board remain responsible for managing the relationship with third-parties.**
Third-party Vendor Due Diligence Check List

Evaluate third party’s experience in implementing and supporting the proposed activity

- Determine that the third party's culture, vision, and business style fit with the bank
- Check references, including peer institutions and industry groups
- Contact Better Business Bureau, state attorneys general office, state consumers affairs offices
- Consider checking backgrounds and reputations of company principals

Determine adequacy of third party’s risk-management infrastructure

- MIS, internal controls, systems security, use of confidential customer information, and contingency planning
- Determine reliance on subcontractors
- Analyze third party’s financial information
- Would the bank extend credit to the third party?
- Audited statements should be required for material activities and relationships
- Adequacy of insurance coverage

Banks should consider the following issues in contracts with third parties:

- Scope of arrangement (content, format, frequency, etc.)
- Fees and costs, including purchasing and maintaining hardware and software
- Performance measures or benchmarks
- Management reports (frequency and type)
- Audit requirements and reports (financial, security, internal control)
- Security and confidentiality (including GLBA 501b requirements)
- Business continuity planning
- Default and termination
- Ownership and license
- Indemnification
- Insurance coverage
- Dispute resolution
- Customer complaints

Oversight of third-party relationships should include:

- Monitoring financial condition of third-party
- Monitoring controls (internal/external audit reports, privacy and security reviews, business continuity plans)
- Assessment of quality of service and support

You regulator / examiners will want to review:

- Business plans for significant new products using third-parties or newly outsourced functions
- Results of due diligence reviews
- Contracts
- MIS from third party
- Information provided to board reflecting results of ongoing monitoring activities

For questions about this reference guide or any other compliance issues, please contact IBAT’s Regulatory Compliance Manager, Kelly Goulart, at kgoulart@ibat.org or 512-275-2231.