SPOTLIGHT ON VENDOR MANAGEMENT

Managing Third-Party Risks in Banking Relationships

A Spotlight on Third-Party Risk Management – Principles, Elements and Best Practices

StratisAdvisory

RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT

Interagency Guidance on Third-Party Risk Management

On June 2023, the Federal Reserve Board (FRB), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC), collectively the “Agencies,” issued final guidance on managing risks associated with third-party relationships (the “Guidance”).

The Agencies issued the Guidance to promote consistency in supervisory approaches and rescinded previously issued statements. Moreover, the Guidance also established the responsibilities of banking organizations to analyze the risks associated with each third-party relationship. The Agencies emphasized the importance of sound risk management regardless of the bank size and varying degree of risk and complexity of the third-party relationships. The Guidance identified four (4) key principles:

Supervisory Reviews

Risk Management

Governance

Third-party Relationship Life Cycle

SUPERVISORY REVIEWS

- The scope of reviews shall depend on the degree of risk and the complexity associated with the bank's activities and third-party relationships and will be part of the usual supervisory processes. But in general, the following areas should be looked at when reviewing third party risk management processes:
  - *The ability of the banking organization's management to oversee and manage third party relationships;*
  - *The impact of third-party relationships on the banking organization's risk profile, as well as its financial and operational performance, inclusive of compliance with applicable regulations and laws;*
  - *Transaction testing and results of testing to evaluate activities performed by the third party and to validate compliance;*
  - *Any material risks and deficiencies in the banking organization's risk management processes and discuss with senior management and the board of directors where needed; and*
  - *Plans for appropriate and sustainable remediation of identified deficiencies especially those involving the oversight of third parties with critical activities.*

RISK MANAGEMENT

- Banks should periodically analyze the risks associated with each third-party relationship, and tailor risk management practices appropriate to the size, complexity, risk profile, and the nature of individual and third-party relationship.
- Maintain "complete" inventories of third-party relationships and periodically conduct risk assessments for each third-party relationship.
- Engage in rigorous oversight and management of third-party relationships that support "higher-risk" activities including "critical activities."
- Implement proper governance whether through committees or board reporting of critical matters to ensure visibility, corrective action, and resourcing.

GOVERNANCE

- Oversight and Accountability – Management shall integrate third-party risk management with overall risk management processes, including ongoing monitoring and due diligence; periodic board reporting of risk management activities; third party contract reviews, approval and execution; internal controls; assessment of compliance management systems; data and information access; escalation; and termination of business arrangements due to non-performance.
- Independent Reviews – Conduct reviews periodically to assess the adequacy of all third-party risk management processes and align with the banking organization's business strategy and internal policies, monitoring, and control of third-party risks.
- Documentation and Reporting – Develop an inventory of third-party relationships and identify those with "higher-risk" activities.

THIRD-PARTY RELATIONSHIP LIFE CYCLE

- Planning – Evaluate and consider risk management before entering into third-party relationships—strategic business purpose, benefits, risks, costs, potential information security implications, and contingency planning.
- Due Diligence and Selection – Helps management identify, monitor, and control risks associated with third-party relationships. Factors include, but are not limited to, business strategies, compliance, resources, ownership structure, financial condition or reliance to subcontractors.
- Contract Negotiation – Periodic reviews of executed contracts and tailor the level of detail and comprehensiveness of contract provisions.
- Ongoing Monitoring – Confirm the quality and sustainability of third-party's controls, escalate significant issues, and respond when needed.
- Termination – Assess and execute termination and consider timeframes, data related risks, retention, and destruction.

Third-Party Risk Management Elements

A successful third-party risk management program includes four (4) basic elements, which will help organizations build a solid strategy to identify and reduce risks of using third parties in their business operations. Whether an globally scaling growth company or Fortune 500, a third party risk management program is a continuous process and must be an integral part of the business. Below are the key elements of a successful third-party risk management program.

Best Practices to a Successful Third-Party Risk Management

THIRD-PARTY RISK MANAGEMENT PROGRAM

THIRD-PARTY DUE DILIGENCE

Discover what Stratis Advisory can do for you

Third-Party Service Provider Program

A properly documented third-party service provider program ensures that there is alignment and understanding of all third-party elements, such as policies, procedures, processes and scope of responsibility within the organization. Program documentation should also be approved by management and reviewed at least annually. Stratis can assist you with program documentation on operational and monitoring procedures, third-party service provider inventory maintenance, and compliance requirements and success measurements.

Third-Party Service Provider Risk Assessment

A third-party service provider risk assessment is an evaluation used by organizations to assess risks and benefits associated with outsourcing to external entities. Regular risk assessments for each third-party relationship can help determine whether risks have evolved and are sufficiently mitigated. Stratis can execute your third-party service provider risk assessment for broader risk identification and control mitigation across key activities that may impact your organization, agreements, customers, and operations.

Outsourced Third-Party Due Diligence

A sound risk management involves conducting third-party due diligence before selecting and entering a third-party relationship. Due diligence must be commensurate with the risk level and complexity of the third-party relationship and must evaluate the third-party's ability to deliver services, meet expectations, adhere to your business goals, as well as comply with laws and regulations. Stratis can perform your third-party due diligence to provide you with recommendations or actionable insights prior onboarding or evaluating existing third-party service providers.

Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com