Third-Party Risk Management – Guidance for Community Banks

In June 2023 RGS issued a paper[1] discussing the final interagency risk management guidance on third-party relationships that was issued earlier that month. Additional guidance has since been issued this month, when the Federal Banking Regulators issued additional interagency guidance specifically aimed at Community Banks[2].

The new guidance does not replace the prior guidance but expands on it by providing pertinent information and points of consideration for Third-Party Risk Management ("TPRM"). Although this release is only a "Guide", it increases the expectations for banks to better identify, assess, monitor, and control the risks associated with third-party relationships. The Guide includes many considerations and examples of the type of processes and controls that should occur at each of the life cycle phases of a third-party relationship. Evaluating these details will require time and effort and may result in identifying control gaps that need to be addressed to strengthen TPRM activities.

To help navigate the Guide, we have identified key takeaways for each of the phases that need to be managed during the life cycle of a third-party relationship. However, an important first step is to update the population of third-party relationships and reassess which relationships present higher risks, including given gaps in existing due diligence. In that regard, those third parties that provide essential technology and business service support and/or have access to confidential customer data present the highest risk, are mission critical and require increased supervision and monitoring.

Life Cycle Phases – Key Takeaways

Planning – entering into a third-party relationship will have a greater chance of success if careful planning is performed. Key considerations during the planning phase should include:

- How the services or support provided by the third-party align with the strategic /business plan

[1] https://rgsglobaladvisors.com/risk-management-managing-third-party-risks/
[2] https://www.occ.gov/news-issuances/news-releases/2024/pub-third-party-risk-management-guide-for-community-banks.pdf

- What are the potential resource impacts such as internal expertise requirements and potential disruption to staff
- Understanding what internal controls and oversight will be needed
- How current systems and processes will be impacted
- Understanding what system back up will exist in event of failure or disruption
- Determining the information security and system access implications
- Performing cost-benefit analysis to understand the costs versus the savings/benefits that will be derived
- Review the various options and bids available
- Review the legal and compliance requirements from a risk management perspective as well as from a regulatory compliance standpoint.

Due Diligence and Third-Party Selection - before signing the contract with a third-party, due diligence is essential and needs to be performed with appropriate in-depth analysis so that the strengths and weaknesses of the third-party service can be fully evaluated. The following are key items that need to be reviewed in the process, as applicable and appropriate given the risks involved:

- Financial strength and operational capacity
- Operational procedures and controls
- Technology and applications used
- Information security and system access
- System back-up and data recovery
- Resource expertise, staffing model and depth of resources
- Training program information
- Communication and information sharing protocols
- Compliance with Bank procedures and compliance with laws and regulations
- Potential BSA/AML/OFAC impacts
- Validations performed
- Independent Audit Reports such as SOC reports, or Internal Audit Reports, as applicable
- Prior litigation
- References

Contract Negotiation – a contract should accurately reflect the expectations and obligations of both parties to the agreement. In addition, management needs to understand the risks embedded in the contract and whether there are adequate contract provisions to protect the interests of the bank. While a contract may be reviewed by in-house or outside counsel; management should be satisfied that key elements that drive the execution of the relationship are clearly defined. These should include:

- Responsibilities and operational framework, for example,
  - ✓ Reporting requirements,
  - ✓ Timelines and frequency of reports,
  - ✓ Data access and information,
  - ✓ Communication and information sharing protocols,
  - ✓ Performance metrics,
  - ✓ Escalation protocols
- Costs associated with contract and potential liabilities as well as the risk of additional expenses
- Disruption, data back up and business continuity
- Cyber security threats and protections
- Data breaches and responses
- Incident reporting
- Audit requirements

Ongoing Monitoring – risk management activities need to include monitoring third-party service performance and ensuring compliance with obligations in accordance with the terms of the contract. However, establishing a monitoring program requires careful planning and the scope and frequency of procedures need to correlate with the third-party's risk profile and attributes. Obtaining updated information from third parties is also important such as current financial data, details of business strategic changes, staffing changes, and system upgrades. Other key tasks that should be part of a monitoring program include:

- Confirm any changes that occurred in the relationship, and if any, that these were reviewed and approved in accordance with policies and procedures
- Review performance metrics and reporting thereof
- Determine the extent of complaints and the follow up to resolve any issues
- Review audit reports, SOC reports, and system/model validation reports, as applicable

- Determine if any disruptions occurred and that actions taken were responsive and timely
- Determine if any security breaches occurred and follow up to validate that appropriate corrective action was taken
- If applicable, review results of any disaster recovery testing performed
- Review the service level agreement to ensure that it is applicable and updated for current activities
- Evaluate and review satisfaction with the services received to ensure that service level activities are being completed timely and in compliance with contractual terms.

Termination – a contract termination and transition to either an in-house or alternative third-party solution requires careful planning both in identifying the risk exposures and the necessary actions required to mitigate them. Matters that need to be evaluated when planning for a termination include:

- Operational disruption and impacts for customers
- Customer communications
- Customer data protection and prior access removal
- Resource planning for the transition period
- Financial consequences including any contractual penalty issues
- Ongoing compliance requirements especially any regulatory compliance or Cybersecurity concerns
- Internal controls and monitoring during the transition both pre and post transition

In conclusion, it is important to remember that engaging outsourced services has its benefits, including for staying competitive, offering new products or services, managing costs and increasing efficiencies, etc., Management and the Board's responsibility and accountability remain, irrespective of the outsourced nature of the activities. This recently issued guidance is also an indication that the regulatory agencies view third-party risk management as a high priority expectation at all banks irrespective of size and risk profile.

RGS Global Advisors is a leading cost-effective provider of Internal Audit, Risk Management, IT/IS/Cybersecurity and BSA/AML/OFAC Compliance Consultancy services for Financial Institutions.

For further guidance or assistance contact us at: info@RGSGlobalAdvisors.com