RGS GLOBAL ADVISORS
1441 Broadway, Suite 6137, New York, NY 10018
390 North Orange Avenue, Suite 2300, Orlando, FL 32801
1150 NW 72nd Ave, Tower I, Suite 455, Miami, FL 33126

Risk Management – Managing Third-Party Risks

June 2023

The recent bank failures have brought risk management protocols into focus as Management and Boards have had to reevaluate deposit concentration risks, mismatched balance sheets, and liquidity risks, etc. However, the increased usage of technology and third parties, and risks associated with artificial intelligence ("AI') continue to elevate operational, compliance and strategic risks which need enhanced risk management oversight.

For some time, the regulatory agencies, both federal and state, have been issuing guidance and regulations to address cyber security and third-party risks within financial institutions. E.g., the Computer-Security Incident Notification Requirements for Banking Organizations and their Bank Service Providers that came into effect in 2022, and which was discussed in our article entitled 'The Cost of Managing Cybersecurity Risks and Related Incident Reporting'. The increasing threat due to technological and operational vulnerabilities were also discussed by the FDIC, in its 2022 Risk Review, which recognized that 'Operational risk in banking is one of the most critical risks to banks'. In this review report, the FDIC noted that cyber-attacks continued to evolve and increase with bad actors using creative ways to exploit technological and operational vulnerabilities. The review discussed various contributing factors for increased risk, including greater reliance on technology and third-party service providers.

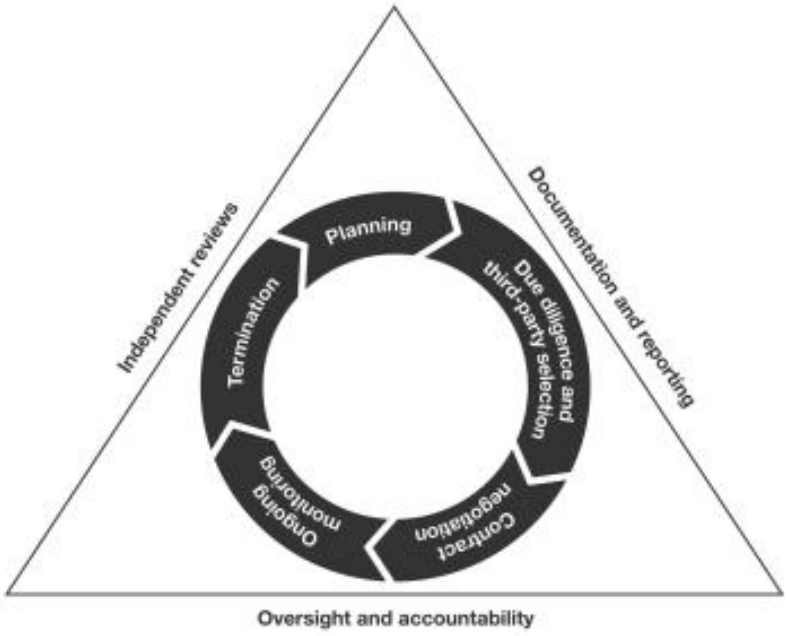
Within the framework of sound governance and risk management, the Board of Directors and Management are responsible for ensuring that the bank operates in a safe manner and in compliance with applicable laws and regulations irrespective of whether transaction activities are performed in-house or by third-party service providers. As such, third party transaction activities and control dependencies need to be regularly evaluated and monitored as part of ongoing risk management practices so that potential deficiencies or non-compliant matters are identified and rectified in a timely manner.

The federal regulators had issued their proposed guidance on managing risks related to third-party service providers on July 19, 2021. The guidance was based on a proposed framework of sound risk management principles for banking organizations to be considered in developing risk management practices for all stages in the life cycle of third-party relationships at the banks. The "Interagency Guidance on Third-Party Relationships: Risk Management" has now been finalized and was issued by the Federal Banking Regulators on June 6, 2023.

Risk Management – Managing Third-Party Risks

These guidelines acknowledge the likely benefits derived by banks through use of third-party services and recognize that certain services may also be received without formal contracts being in place. Irrespective of the existence of a contract, the use of third parties can reduce the bank's direct control over activities and may introduce new risks or increase existing risks, including operational, compliance, and strategic risks. The guidelines are applicable to all business arrangements that banks may have, irrespective of the existence of a formal contract and address various key risk management areas. Highlights from the regulatory guidance include:

- Defining characteristics of critical operational activities, requiring the identification of these activities and the related third-party relationships to be determined by the banks.
- Addressing all stages of risk management across the third-party relationship life cycle: planning; third-party due diligence and selection; contract negotiation; ongoing monitoring of relationship and contract termination with a third-party, as shown in the following diagram -



Source: Board, FDIC, and OCC

- Addressing various governance and reporting matters, including accountability, independent reviews, and documentation, etc.

Risk Management – Managing Third-Party Risks

- As expected, acknowledging the need for a risk-based approach based on specific facts and circumstances concerned.
- Providing granularity on due diligence and vendor selection, including vendor qualification, experience, competence, controls, operational resilience, etc. The process is expected to include consideration of:
    - legal and regulatory compliance
    - information security
    - Cyber security risk, and
    - insurance coverage, etc.
- Addressing various considerations for contracts, including clarity on legal jurisdictions, transition, termination and regulatory reviews and oversight.
- Ongoing risk-based monitoring covering the duration of the relationship to ensure that the bank identifies increasing risk and concerns, if any, and is receiving quality services in accordance with the terms of the third-party obligations.

While the scope of the supervisory review depends on the degree of risk and the complexity associated with bank's activities and their third-party relationships, the regulatory examiners are expected to focus on evaluating the risks and effectiveness of bank's risk management program and associated bank's management oversight in managing risks associated with third-party relationships throughout their lifecycle.

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

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