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

REEVALUATING OPERATIONAL RISK MANAGEMENT

July 2023

Last month, in June 2023, we published an article entitled, "Risk Management- Managing Third-Party Risks," which focused on the final regulatory guidance relating to managing the risks related to third-party relationships that was issued then. However, considering that in addition to third-party risks, operational activities which span across all functions, systems and business lines have risk exposures that require to be managed, this article focusses on this broader aspect of this operational risk management. The consequences of not identifying a risk can result in devastating consequences as was the case with the unexpected deposit runs earlier this year.

While the circumstances and control failures associated with the recent deposit runs will continue to be evaluated and debated including ongoing regulatory deliberations over potential changes to capital requirements and deposit insurance regulations, one alarming fact that stood out was the speed at which the deposits were able to be withdrawn before any intervention could begin – a reflection of technological advances and digital banking capabilities in banks today. Of course, there were other factors, e.g., risk exposures caused by large deposit concentrations related to commercial account relationships. Certainly, banking industry leaders are wondering if risk management could have been better at identifying and mitigating these risk exposures. This poses the question as to how well-prepared banks are for future unexpected crises.

Executive Management and Board of Directors need to consider the readiness and effectiveness of their operational risk management practices and consider whether their bank has adequate process for timely identification of risk exposures. It should be remembered that operational risks can arise or increase at any time due to uncontrollable external factors, such as increasing fraud risk due to the use of sophisticated new tools attributable to Artificial Intelligence. Therefore, it is important to reevaluate the effectiveness of internal controls and processes, the strength of resources, completeness of data analysis and reporting, and the operational risks associated with legacy systems periodically.

Some of the fundamental and innovative actions that can be taken to identify gaps in risk management providing opportunities for strengthening controls to better manage operational risk are mentioned hereunder.

REEVALUATING OPERATIONAL RISK MANAGEMENT

Fundamental Actions

Operational activities span across the entire enterprise including the front office, middle office, and back-office functions. Therefore, optimizing resources and efforts to effectively identify and manage operational risks is undoubtedly challenging. Two following core pillars form the foundation for a successful process, a sound risk management framework, and a detailed operational risk assessment:

- Risk Management Framework – to include an organizational structure, policies and procedures and information reporting protocols. Obviously, the extent and depth of the framework is guided by the institution's size, complexity of business lines, products, services, geographies served and the supporting systems used. As a result, there are varied approaches to organizing an operational risk management structure. The diversity of approaches is not an issue, the key part is to review the current structure to determine its effectiveness and completeness. At a minimum, irrespective of the approach, it is important to ensure the following:

    - Adequate board and management oversight of operational risk exists that includes but not limited to:
        - evaluation of the risks through quality risk assessments,
        - review of policies and procedures,
        - documented response plans to threat scenarios,
        - resource and talent management – a risk that has evolved considerably since recent global pandemic,
        - assess the use of models and tools, and
        - effective internal audit and model validations.

    - Appropriate levels of board and management reporting includes, amongst others:
        - performance reporting and metrics,
        - trend analysis,
        - early warning reporting such as "red flags" of potential threats.

- Operational Risk Assessment - to include all operational activities and systems. Notably the universe of risks and controls to be evaluated depends on the complexity of business

lines, services, and products offered, etc. Nevertheless, base line risk factors to be evaluated should, at a minimum, include:

- External Factors – market conditions, interest rates, competition, legal, reputational, fraud, cyber and regulatory,
- Internal Factors – governance, policies and procedures, data management and reporting, data security and access, resources, third-party risk and fraud.

After sufficient analysis of the risk management framework and an updated determination of operational risks and controls, various gaps and required enhancements are likely to become evident. Based on our experience, areas for improvements that often surface include but are not be limited to:

- The need for more frequent updates to the operational risk assessment as operational changes occur or different external threats arise,
- Updating operational policies and procedures,
- Increasing collaboration with operational management to improve monitoring activities and reporting,
- Improving alignment and review of the business continuity and recovery planning process, and related testing cycles,
- Stepping up monitoring of third-party risk management practices ensuring that these are current and reflective of priorities and include all mission critical systems,
- Enhancing on-going review of cyber security controls and timely addressing of penetration testing issues,
- Revamping processes for the monitoring of data security controls,
- Ensuring that the internal and external audit functions provide appropriate coverage and assessment of the internal control framework, and
- Expanding the reporting of operational performance and tracking metrics.

Innovative Actions

In addition to traditional approaches to operational risk management practices, the following suggested actions should be considered that can further enhance operational risk management. Options include but are not limited to the following:

REEVALUATING OPERATIONAL RISK MANAGEMENT

1. Expansion of Risk Management Oversight – in this approach operational risk management takes on a more active second-line role partnering more closely with operational functions (first line); effectively assuming a role to challenge and support the effectiveness of operational processes. Actions that can be taken include:
    - Monitor controls in real time to identify outliers or unusual activity,
    - Review resource planning to better match processes with technology skills,
    - Reinforce positive behaviors through communications, training, performance measures and incentives, and
    - Provide timely feedback related to issues and root causes.

2. Use of Analytical Tools – analytics create improvements in detecting operational risks and reducing false positive alerts. Examples of how advancing analytics can help identify risks include but are not limited to:
    - Analytical tools that can identify potential fraudulent transactions, by recognizing outliers and transactions inconsistent with expected trends and behaviors,
    - Analytical techniques that can improve assessments of vendor risk and selection, and
    - Use of machine learning techniques to track threats and the root causes of issues, providing opportunities for enhancing model rules and scenarios for false positive alert reduction.

Conclusion

Operational Risk Managers, Executive Management and Board of Directors should gain updated perspective of the operational risk environment as suggested above so that they can reevaluate the effectiveness of their current risk management practices. This process should enable identification of both the strengths and weaknesses so that the Management and Board can take timely initiatives and actions to enhance processes, implement effective early warning techniques and timely risk reporting for ensuing continued effectiveness of the Operational Risk Management process at the institution.