The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 31816

June 21, 2019

OCC Publishes Its Semiannual Risk Perspective

[31816]

June 21, 2019

TO: Bank, Trust and Retirement Advisory Committee
Chief Risk Officer Committee
Internal Audit Committee
Risk Advisory Committee

RE: OCC Publishes Its Semiannual Risk Perspective

The National Risk Committee (NRC) of the Office of the Comptroller of the Currency (OCC) has published its *Semiannual Risk Perspective* (the "Report").[1] While the Report does not address registered investment companies, its findings mirror concerns of our members and therefore its insights may be of interest to the Institute's members.

The NRC monitors the activities of national banks and savings associations, in part, to identify key risk and emerging threats that may impact the safety and soundness of our national banking system. Twice a year, it publishes information derived from such monitoring. These publications highlight credit, operational, compliance, and interest rate risks that pose threats to the safety and soundness of national banks and savings associations. The findings in the NRC's current Report are based on the OCC's data as of December 31, 2018. The Report is broken down into five sections: (1) The Operating Environment; (2) Bank Performance; (3) Special Topics in Emerging Risks; (4) Trends in Key Risk Themes; and (5) Supervisory Actions. Because Sections (3) and (4) are likely to be of greatest interest to the Institute's members, only these two sections are summarized below.

Special Topics in Emerging Risks

This section of the Report is divided into five subsections, each of which is summarized below.

Assessing Financial Innovation and Related Impacts to Strategic Risks

The NRC defines "strategic risk" to mean "the risk to current or projected financial condition and resilience arising from adverse business decisions, poor implementation of business decisions, or lack of responsiveness to changes in the banking industry and operating environment."[2] According to the NRC, changing business models or offering

new products and services can elevate a bank's strategic risk "when pursued without appropriate corporate governance and risk management."[3] Also, deploying new products, services, or technologies can result in greater reliance on third parties and a concentration of service provides to the industry, which, in the view of the NRC, management should consider in assessing risks. The NRC cautions banks to ensure that any decisions involving incrementally or fundamentally changing a bank's operations should be aligned with the bank's business strategy and risk appetite to avoid increasing the bank's risk exposure.

Strategic Risk Poses Challenge for Many Banks

According to the OCC, 29% of banks exhibited moderate and increasing or high levels of strategic risk as of the end of 2018. This is a slight increase from previous years. Drivers of this higher strategic risk include rapid industry changes, poor business decisions, imprudent or incomplete change management plans, pressure to reduce expenses and control costs, the burdens associated with legacy technology systems, resource limitations, and the need for scale of operations.

Changes in the Federal Banking Industry

The Report notes the recent trend of banks investing in and leveraging technology that is more efficient, reduces costs, and increases speed to market, such as cloud computing and mobile banking applications. Also, distributed ledger technology may have the potential to transform how transactions are processed and settled. However, because the transition from legacy systems can be complex and expensive, some banks have been reluctant to make the change and move critical activities to unproven solutions.

Operational Efficiency Remains a Challenge for Small Banks

A key strategic issue for banks is operational efficiency through expense management and finding or expanding revenue sources. Not surprisingly, the Report notes that larger banks may have the greatest ability to invest directly in the technology, staff, and controls to develop and introduce new products and services. The use of third parties – such as service providers and fintech firms – has enabled even smaller community banks to leverage technical expertise and gain the economies of scale necessary to offer increasingly sophisticated products and services.

Implications for the Federal Banking Industry

According to the Report, rapid changes in the industry are forcing banks to re-evaluate their business strategies. "A slow-adopter strategy adds risk because the speed of change, combined with the lengthy process to evaluate and implement newer technology solutions, can result in loss of customers or market share before the bank can respond."[4] Factors that will made adapting to the current environment challenging for banks are: the lack of resources to invest in technology; the burden of legacy systems; the reliance on core processing; and the competition for talent. "Overall, banks should focus on their core competencies and identify compatible opportunities and technologies that increase efficiency and reach customers effectively."[5]

Corporate Governance and Risk Management

According to the Report, "Strategic risk management is now in the forefront as the financial services industry continues a decades-long process of disintermediation aided by new

entrants and more powerful technology. Strategic risk increases not only when innovation is pursued without appropriate planning and governance, but also when banks fail to keep pace with change."[6] In the view of the NRC, "[g]ood corporate governance and effective risk management are fundamental for banks to adapt to change" and all banks, regardless of size, "should verify that corporate governance and risk management are effective when considering new products, services, and processes."[7] Additionally, the bank's board and management should ensure that new or revised business practices are aligned with the bank's risk appetite. Among other things, this evaluation should consider, from end-to-end, the resources, skill sets, technology, and operational support required for new products and services. If the bank is collaborating with a nonbank firm to offer products and services, management should conduct proper due diligence, both initially and on-going, and involve proper oversight. This is important because "the lack of proper due diligence, oversight, and controls over third-party relationships can result in elevated reputation strategic, operational, and compliance risk."

The Report encourages banks to consult OCC guidance relating to strategic planning, evaluating new products and services, collaborating, and managing third-party relationships, and provides cites to OCC guidance in each of these areas.[8]

Trends in Key Risk Themes

The discussion in this section of the Report includes the following:

Credit Quality is Strong, but Risk Has Been Building

While this portion of the report is largely focused on credit quality and risk that would be relevant for the banking segment, it notes that "uncertain interest rate and economic forecasts have the potential to elevate credit risk."[9] This discuss continues:

Recently . . . there has been an increased economic consensus for a slowing economy and a higher probability of recession. Such a slowdown could adversely affect borrowers through weaker revenue or income, higher unemployment, and lower asset values. Banks should plan for this economic uncertainty by identifying potentially vulnerable borrowers, reviewing the quality and thoroughness of credit control functions, and ascertaining any experience or operational gaps in collections and workout functions.[10]

Cyber Threats Continue to Increase and Evolve

According to the Report, cyber threats continue to target vulnerabilities in bank and third-party systems. The objectives of the attackers may be obtaining or exposing large quantities of personally-identifiable information and intellectual property, facilitating misappropriation of funds or data, corrupting information, or disrupting business operations. While banks are generally responding well to common cyber events, malicious actors continue to improve their tools and tactics, thereby requiring banks to continually reassess and validate their cyber controls.

Social engineering, such a spear phishing, is the primary method for targeting banks and actors continue to refine their tactics to target key personnel with access to highly sensitive information. The Report notes that user awareness training and testing are "essential" to reducing the risk of unauthorized access and preventing breaches. Another key control is deploying strong authentication mechanisms and user access controls.[11]

Another vulnerability is the use of unpatched or unsupported software and hardware by the

bank or its third parties. To address this vulnerability, banks need a strong process for managing system and software inventories as well as a sound development life cycle that requires regular maintenance, patching, timely updates, and proper disposition of systems no longer required. Also important is the bank's identification of those vendors with access to data and control systems and that perform key operations.

With respect to vendors, the Report notes that cyber crime and espionage is increasingly targeting third-party service providers because of the potential to access multiple networks from a single point. In response, banks should understand remote access, system interfaces, access entitlements, the third-party's ability to implement the appropriate controls to manage risk and security, and responsibilities of the third party and bank in the case of an incident. The Report also encourages banks to regularly validate the operational resiliency of the enterprise to ensure customer service continuity as well as to fulfill interdependent operations of the financial system.

Use of Third-Party Service Providers Is Increasing

According to the Report, banks are increasingly relying on third-party service providers for technology and other solutions to compete in a rapidly evolving financial market. Bank management need to properly manage the risks that result from these relationships. In light of the fact that the consolidation in the bank technology service provider industry has resulted in fewer entities providing certain critical services, the OCC is working with interagency partners to examine the services offered by these providers to banks to ensure appropriate supervisory oversight of this risk.

Advances in Technology Pose Challenges for BSA/AML/OFAC

The Report notes that risk associated with complying with the Bank Secrecy Act (BSA) and regulatory requirements addressing Anti-Money Laundering (AML) "remains high," in part due to the complex and dynamic money laundering by terrorists and other criminals.[12] The three primary causes of BSA/AML-related deficiencies identified by the OCC stem from inadequate customer due diligence, insufficient customer risk identification, and ineffective processes related to suspicious activity monitoring and reporting, including filing Suspicious Activity Reports (SARs) timely. In response, bank management should periodically assess and adjust as necessary, the BSA/AML compliance risk management systems. Banks should also recognize that virtual currency and crypto assets present novel vulnerabilities that criminals can exploit. In addition, the Report notes the importance of banks maintaining effective policies and procedures for screening against the Specially Designated Nationals and Blocked Persons List of the Office of Foreign Assets Control (OFAC). Banks that enter into collaborative arrangements to share resources to manage their BSA/AML obligations may want to review guidance the OCC has issued on this topic.[13]

Tamara K. Salmon
Associate General Counsel

endnotes

[1] The Report is *available at* https://www.occ.gov/publications/publications-by-type/semiannual-risk-perspective/pub-semiannual-risk-perspective-fall-2018.pdf.

[2] Report at p. 12.

[3] *Id.*

[4] Report at p. 16.

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *See* footnotes 14-17.

[9] Report at p. 19.

[10] *Id*.

[11] Report at p. 21.

[12] Report at p. 22.

[13] The Report cites the *Bank Secrecy Act/Anti-Money Laundering: Interagency Statement on Sharing Bank Secrecy Act Resources* (OCC Bulleting 2018-36) and *Bank Secrecy Act/Anti-Money Laundering: Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (OCC Bulletin 2018-44). The OCC's Bulletins are available on the OCC's website at: https://www.occ.treas.gov/news-issuances/bulletins/index.html.
