FINANCIAL SERVICES BOARD INSIGHTS

Regulatory Outlook for 2024

Complying with a rapidly evolving regulatory landscape can be a challenging task for board members charged with oversight responsibilities. Ever-changing geopolitical conflicts and persistent global economic turmoil are expected to continue to influence supervisory guidance and increase expectations.

Fitch Ratings released its 2024 Outlook: Global Banking Regulation report recently, noting that worldwide, bank supervision may tighten due to increasing concerns about the impact of interest rates on rate-risk-sensitive assets and debt service burdens. This would certainly indicate that financial services companies need to prepare to meet higher risk standards, regulatory expectations, and possible supervisory and enforcement actions.

Key concepts to keep in mind for 2024 are resiliency, model-driven data analysis, accountability, security, privacy, and technology integration. How can board members prepare to meet their oversight obligations? We encourage a focus on the following considerations:

- Consumer impact. Expect stringent review of the impact of products and pricing on customers, considered under the umbrella of challenging economic conditions with emphasis on consumer protections, financial institution transparency, and fairness.
- Liquidity risk management using stronger metrics like stress testing that considers non-financial risks, such as the ways emerging technologies influence consumer behavior, and provides insight into how to assess and address vulnerabilities to minimize customer disruption.
- Resilient operational frameworks that strengthen out-of-date legacy systems to ensure transparency and accountability and protect consumers while meeting compliance requirements. Consider investments in IT systems, outsourced solutions, and cybersecurity risk management technologies that drive efficiencies, enhance service throughout multiple delivery channels, and support timely incident resolution to protect operations and marketplace reputations.
- Preventing fraudulent transactions, particularly bank transfers at the retail level — increasingly the cause of scam payments. Persistent transaction monitoring and detailed analysis may be accomplished with the careful application of AI and other automated workflow solutions.

Looking ahead, we expect regulators will continue to focus on enforcement actions that address these weaknesses in systems, policies, and procedures from the dual perspective of consumer protections and management accountability. Board members have an opportunity to make a significant contribution in these areas with informed, strategic decisions that influence processes enterprise-wide.

For more information, contact your Rehmann advisor or Liz Ziesmer at liz.ziesmer@rehmann.com or 616.975.2855.

Mitigate Ransomware Risks with R-SAT 2.0 *(Ransomware Self-Assessment Tool)*

Ransomware is malware that encrypts data on a device, making it difficult to recover without the ability to restore from backups or a decryption key that may (or may not!) be provided by a cybercriminal after the ransom is paid. According to Cybercrime Magazine, global ransomware costs are predicted to exceed $265 billion by 2031, when businesses, consumers, and devices could be attacked every two seconds. Ransomware is a particularly menacing form of malware because attackers often threaten to publicly disclose stolen company or customer information if the ransom isn't paid.

The R-SAT 2.0 tool helps financial institutions assess how well their procedures and processes are designed to reduce the risk of becoming a ransomware victim. It was developed in collaboration with the Bankers Electronic Crimes Task Force, state bank regulators, and the U.S Secret Service and was updated in October 2023 to address today's banking environment.

The importance of proper use of R-SAT was validated in a study conducted by the Conference of State Bank Supervisors in collaboration with several state banking departments to identify lessons learned from state-chartered banks and credit unions that experienced ransomware attacks between January 1, 2019, and December 31, 2022. The study found three significant findings:

- R-SAT: The majority had not completed the R-SAT and, therefore, didn't use it to guide initiatives to reduce ransomware risks. However, all institutions began using it fully after their ransomware incident.
- Multi-factor Authentication (MFA): When properly configured and implemented, MFA makes a difference. While MFA may seem to be a fairly simple security feature, the various forms of MFA require a thorough understanding of their features and benefits in relation to each financial institution's unique situation, operations, and risks. The R-SAT now includes expanded sections to address MFA.
- Fast Identity Online Authentication (FIDO): Using public key cryptography, FIDO provides more security than traditional password-based authentication where it's required, such as online and mobile banking. FIDO is mentioned in the latest FFIEC guidance, which is gaining popularity in the banking industry.

Download R-SAT 2.0: https://www.csbs.org/sites/default/files/other-files/R-SAT%202.0%20%281%29_0.pdf

To learn how proper and consistent implementation of R-SAT and other risk management techniques can help protect your financial institution from damaging ransomware attacks, contact your Rehmann advisor or Jessica Dore at jessica.dore@rehmann.com or 989.797.8391.

Audit Committee Oversight Responsibilities

The Audit Committee performs an essential oversight function by ensuring management is providing accurate and transparent financial reports to investors and other interested parties. The Committee is not responsible for preparing the information, but it is responsible for oversight of the processes and procedures in place to protect stakeholders' interests. The main method to accomplish this goal is the oversight of the financial reporting process, including the financial statements, annual reports, call reports, and earnings releases.

While the Audit Committee role continues to evolve with changing regulatory requirements and stakeholder expectations, it primarily has oversight responsibility for:

Financial Reporting Process

- Reviewing financial statements including management's discussion of results to understand and seek clarification of significant variances from prior reports, budgets, and forecasts.
- Reviewing independent auditor communications including their recommendations and management's responses.
- Assessing the impact that accounting and reporting requirements may have on financial and regulatory reporting.
- Discussing succession plans for the CFO and financial reporting staff.

Compliance Changes, Best Practices for Bank Directors

Transitioning References from BSA (Back Secrecy Act) to CFT (Countering the Financing of Terrorism)

Since it was enacted in 1970, the BSA has sought to combat money laundering and the financing of terrorism by requiring financial transparency and the detection and prohibition of activities that misuse the U.S. financial system to move funds for illicit purposes.

Although the Anti-Money Laundering Act of 2020 (the AML Act) modified the BSA to require financial institutions to have in place risk-based programs with stringent recordkeeping, the AML Act did not change the goals or expectation of compliance with BSA. However, the FDIC now uses the term AML/CFT rather than BSA/AML for consistency with wording in the AML Act.

While there are no current requirements to update policies, procedures, and standards to reflect the preferred reference, bank leadership should consider these changes as resources allow.

Revised Community Reinvestment Act (CRA)

The CRA was enacted in 1977 to prevent redlining, expand financial access and inclusion, and encourage banks and savings associations to meet the credit needs of all segments of the communities they serve, with a particular focus on low- and moderate-income (LMI) neighborhoods and individuals.

In October 2023, a final rule issued by the Federal Reserve Board, FDIC, and OCC modernized and strengthened CRA regulations to adopt more objective, data-driven techniques to better understand, evaluate, and incentivize lending and investments in LMI communities. Rollout of the new features begins on April 1, 2024, and includes:

- Adapting to changes in the banking industry and evaluating lending beyond traditional branch and ATM activities to include digital delivery channels such as online and mobile banking, branchless banking, and hybrid banking models.
- Applying CRA regulations with greater clarity and consistency including a new metrics-based evaluation of retail lending and community development financing based on peer and demographic benchmarks for deeper insight into performance.
- Clarifying eligible CRA activities, such as affordable housing, that are focused on LMI, underserved, native, and rural communities.
- Reducing compliance burdens with CRA evaluations and data collection customized to bank size and business model. For instance, banks with assets under $2 billion are exempt from new data requirements.

Click here for more details: https://www.federalreserve.gov/aboutthefed/boardmeetings/files/cra-key-objectives-20231024.pdf

Have more questions? Rehmann advisors are uniquely experienced and qualified to help your bank leadership navigate regulatory and compliance requirements. For more information, contact Beth Behrend at beth.behrend@rehmann.com or 616.975.2823.

(Audit Committee Oversight Responsibilities – continued frrom page 2)

- Reviewing critical accounting policies, including those over significant estimates, internal controls, and compliance with FDICIA and/or SOX (if applicable).

Independent Auditor and Internal Audit Function

- Approving the internal audit department charter and ensuring it follows the Institute of Internal Auditors International Standards for Professional Practice of Internal Auditing.
- Approving the internal audit annual plan and scope.
- Evaluating and appointing the independent auditor annually and ensuring periodic rotation of the audit partner (if applicable).
- Evaluating the chief audit executive and ensuring the reporting structure is appropriate.
- Conducting private sessions with the independent auditor during regularly scheduled Committee meetings.

Ethics and Compliance

- Monitoring management for compliance with legal, regulatory, and Code of Conduct requirements, and ensuring reported violations are investigated.
- Ensuring a chief ethics and compliance officer or equivalent is in place.
- Reviewing the whistleblower policy and investigative process for reported complaints, suspected fraud, or other illegal acts.
- Focusing on financial risk to oversee and assess enterprise risk management activities and to ensure a member of the management team or separate risk committee is responsible for each risk category.

Ensure your Audit Committee activities are on target to strengthen oversight by filling gaps in processes and procedures. Consult with your Rehmann advisor for expert guidance or contact Kristy Clark at kristy.clark@rehmann.com or 248. 614.6446.

Funds Transfer Fraud Losses Often Result From Insufficient Internal Controls

The first "online" transfer of money dates back more than 150 years ago. The sender would make a payment at a Western Union office, which then sent a message over the company's existing telegraph network, using passwords and code books to authorize the release of funds to the recipient waiting at the receiving location. Since then, wire transfers have been a fast and reliable way to send funds to businesses and individuals, domestically and internationally. Recently, however, wire transfers have become a target for scammers who use emails, phone calls, and a myriad of other tactics to trick people into sending money to them instead of the intended recipient.

According to the FBI, about $2 billion is lost annually in funds transfer fraud. Some cases involve third-party payment apps like Zelle and Venmo, while others abuse more traditional services. In any scenario, fraudulent activity must be mitigated with strong oversight and tight internal controls at financial institutions both large and small.

In mid-2022, a $6.4 billion asset bank holding company in the Midwest was the victim of international wire fraud that cost the company more than $18 million in losses. The transaction involved a "foreign threat actor" who used a forged wire transfer form to steal the funds, targeting a general ledger at the bank, which was discovered by hacking a single employee email account outside of the company's network.

A forensic technology investigation firm analyzed the incident and concluded that the bank's network was not compromised, and no attempts were made to access client accounts. In other words, the crime was committed by pilfering information from an employee email and by forging documents. This is just one of many examples where insufficient controls, data protection protocols, and verification procedures can have a major detrimental impact on financial performance, not to mention reputational marketplace risk.

Take a Multipronged Approach to Prevent Wire Fraud

- **Secure employee end-user devices.** Keep computers and mobile devices protected with updated antivirus and security software.
- **Control access.** Require the use of strong, unique passwords or passphrases to log in to a device, an email account, and the bank networks — especially important in a remote work environment. Implement multifactor authentication (MFA), password vaults, and other technologies for additional security. Read more: https://www.rehmann.com/resource/strong-end-user-security-protects-against-data-compromise/
- **Train often**. Employees at every level, from the front line to the back office to the C-suite, should be consistently and frequently educated about common scams, red flags, language, and tactics used by scammers and the best practices to spot a potential threat before it happens.

Take Fast Action When an Incident Occurs

As the financial institutions that become victims of wire fraud quickly learn, acting fast to identify and attempt to mitigate losses is critical. Yet, that may not be enough. Rehmann's team of forensic accountants and investigators work closely with bank leadership to identify internal control gaps that may expose the organization to fraud opportunities, help uncover why and how the gaps may have been overlooked, and develop a detailed, feasible plan to address these gaps and lower future risk.

Our team of financial, IT, cybersecurity, and forensic investigations advisors have the skills, experience, and access to the latest technologies to provide expert guidance to design, implement, and test internal controls that serve your unique risk profile. Talk with your Rehmann advisor or contact Bill Edwards, director of financial investigations, at bill.edwards@rehmann.com or 248.267.8445.

Rehmann is a financial services and business advisory firm. We excel at helping clients because we take a collaborative, personalized approach and build a customized team of specialists to help them achieve their objectives. We focus on the business of business — allowing people to focus on what makes them extraordinary. The firm started as a CPA firm more than 75 years ago. Now, we are a multifaceted advisory firm that helps businesses and high-net-worth families maximize potential. Clients who work with us want us to be more than a vendor. They want collaboration, innovation, and continuous improvement.

Rehmann
EMPOWER YOUR PURPOSE®