KPMG

Regulatory Alert

Regulatory Insights for Financial Services

October 2023

Expanded Risk Governance and Management: FDIC Proposed Guidelines

Regulatory Insights:

- ***Heightened Risk Standards:*** *Extending applicability to banks over $10B*
- ***Cross-Agency Focus****: Aligning across FRB, FDIC, and OCC*
- ***Clear Accountability****: Guiding banks to set clear responsibilities, incentives, and deterrents for boards and management*

In concert with the banking regulators' (FRB, FDIC, OCC) focus on expanding expectations for bank risk governance and management to a larger number of banks (see KPMG Regulatory Alerts here, here, and here), the FDIC proposes to establish new corporate governance and risk management guidelines (Guidelines). The Guidelines, which would be enforceable under the FDIC's safety and soundness authority, describe expectations for a board of directors to drive effective corporate governance as well as expectations for board and management responsibilities regarding risk management and internal audit.

The proposed Guidelines cover:

Scope:

FDIC-supervised institutions (insured state nonmember banks, state-licensed insured branches of foreign banks, and insured state savings associations) that have reported total consolidated assets of $10 billion or more in their two most recent consecutive quarterly Call Reports would be deemed to be Covered Institutions (note: FDIC estimated 57 institutions currently meet this requirement). FDIC expects institutions would be aware of their potential to exceed the $10 billion threshold prior to doing so and to proactively develop compliance programs in advance or plan to reduce their total asset size.

Corporate Governance:

- ***Duties/Obligations of the Board***. At a minimum, to carry out the board's overall responsibility for risk management of the Covered Institution, holding executives and management accountable, and ensuring ethical operations. the board of directors should:
  - Set an appropriate "tone at the top" to promote responsible, ethical behavior. This would include developing and implementing a Code of Ethics and a Compensation and Performance Management Program.
  - Approve a strategic plan (including overall mission, strategic objectives, and assessment of risks) and policies (to govern operations in accordance with the risk profile and laws and regulations).
  - Select and supervise qualified executive management (including active oversight of management's adherence to the strategic plan

and policies), provide credible challenge, develop succession plans for key personnel.

- Provide for a formal, ongoing training program for directors, to include products, services lines of business and risks with significant impact to the Covered Institution; applicable laws, regulations, and supervisory requirements; and other topics identified by the board.
- Conduct annual self-assessments of the board's effectiveness in meeting the standards in the Guidelines.

— ***Duties/Obligations of Individual Directors***. At a minimum, each director is expected to exercise sound, independent judgment and the board should ensure that it is not "excessively influenced" by a dominant policymaker. Further each director has a duty to safeguard the interests of the Covered Institution and to oversee and confirm its operation in a safe and sound manner, considering the interests of all stakeholders (shareholders, depositors, creditors, customers, regulators, and the public).

— ***Committee Structure***. Board committees to help keep the board informed and provide a framework to oversee the Covered Institution would include an Audit Committee, a Compensation Committee, a Trust Committee (as appropriate), and a Risk Committee. Other committees might include Compliance, Lending, Information Technology, Cybersecurity, and Investments.

Risk Management Responsibilities:

The board should establish, and management should implement and manage, a comprehensive and independent risk management function and effective programs for internal controls, risk management, and audit.

— ***Risk Management Program***. The Risk Management Program should address identifying, measuring, monitoring, and managing risks of the Covered Institution through a framework appropriate for the current and forecasted risk environment, meeting the minimum standards of the Guidelines. The program should be appropriate for the size, complexity, business model, and risk profile of the Covered Institution and cover the following risk categories, as applicable: credit, concentration, interest rate, liquidity, price, model, operational (e.g., conduct, IT, cybersecurity, AML/CFT compliance, third party), strategic, and legal. The board or the Risk Committee should review and approve the risk management program and any changes made to it.

— ***Risk Profile and Risk Appetite Statement***. On a quarterly basis, the Covered Institution should review and update a risk profile that identifies current risks, as well as risk appetite limits, both in the aggregate and for lines of business and material activities or products. Both qualitative components and quantitative limits should be included.

— ***Three Lines of Defense Model***. Three distinct units should have the responsibility and be held accountable by the CEO and the board or monitoring and reporting on the Covered Institutions compliance with the Risk Management Program (front line; the independent risk management unit; and the internal audit unit). Monitoring and reporting should be performed as often as necessary based on the size and volatility of risks and any material change in the Covered Institution's business model strategy, risk profile, or market conditions.

— ***Communication***. The Covered Institution should communicate the risk appetite statement and risk management program on an ongoing basis to management and all employees to encourage alignment between their risk-taking decisions and the risk appetite statement.

— ***Processes Governing Risk Limit Breaches and Violations of Law or Regulations***. Front line units and the independent risk management unit, consistent with their respective responsibilities, would be expected to:

- Identify breaches of risk appetite, concentration risk limits, front line unit risk limits.
  - Report to front line unit management, CRO, Risk Committee, Audit Committee, CEO, and the FDIC on the severity of the breach, impact to the Covered Institution, and resolution.
  - Establish accountability and consequences for risk limit breaches even if no loss is realized.
- Identify known or suspected violations of law or regulations, distinguishing between those that "appear to be technical, inadvertent, or insignificant and those that appear willful or may involve dishonesty or misrepresentation."
  - Notify the CEO, Audit Committee and the Risk Committee of all violations and actions taken.
  - Report violations of law involving dishonesty, misrepresentation, or willful disregard for requirements to the relevant law enforcement and federal and state agencies.

- Establish accountability and consequences for violations even if no loss is realized.

Supervision and Enforcement

The Guidelines would be issued as Appendix C to the FDIC's regulations at Part 364, Standards for Safety and Soundness, pursuant to its authority under Section 39 of the FDI Act (which authorizes the FDIC to issue safety and soundness standards by guideline or regulation); they would be enforceable by the FDIC under Section 39. Notably, the FDIC states:

- In the event a Covered Institution fails to meet a safety and soundness standard, issuing the standards as Guidelines rather than as a regulation provides the agency with supervisory flexibility "to pursue the course of action that is most appropriate" given the Covered Institution's specific circumstances, including self-corrective and remedial responses. In some instances, the FDIC may require the submission of a plan.
- If a Covered Institution fails to submit or implement an acceptable plan, the FDIC, by order, may require the institution to correct the deficiency and may take additional enumerated actions, including growth restrictions, increased capital requirements, and restrictions on interest rates paid on deposits.

The Guidelines would align the FDIC's supervisory framework more closely with the OCC heightened standards (applicable to OCC-supervised institutions with assets of $50 billion or more) and the corporate governance and risk management requirements in the FRB Regulation YY and Supervision and Regulatory Letters (applicable to FRB-supervised bank holding companies and institutions with assets of $50 billion or more).

For more information, please contact Todd Semanco or Amy Matsuo.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialme