September 21, 2023

MEMORANDUM TO: Board of Directors

FROM: Doreen R. Eberley, Director
Division of Risk Management Supervision

SUBJECT: Notice of proposed rulemaking: *Proposed Guidelines Establishing Standards for Corporate Governance and Risk Management for Covered Institutions with Total Consolidated Assets of $10 Billion or More to be added as Appendix C to Part 364 of the FDIC's Rules and Regulations Standards for Safety and Soundness*

Summary: The FDIC is proposing to amend sections 364.101 and 308.302 of the FDIC's regulations and add as Appendix C to Part 364 *Guidelines Establishing Standards for Corporate Governance and Risk Management for Covered Institutions with Total Consolidated Assets of $10 Billion or More* (Guidelines) under its safety and soundness authority provided by Section 39 of the Federal Deposit Insurance Act (FDI Act). Specifically, the proposed Guidelines:

1. Contain standards for corporate governance and risk management that would apply to all insured state nonmember banks, state-licensed insured branches of foreign banks, and insured state savings associations subject to the provisions of Section 39 of the FDI Act, with total consolidated assets of $10 billion or more (covered institutions). The Guidelines would apply based on total assets of the institution as reported on the Consolidated Reports of Condition and Income (Call Report) for the two most recent consecutive quarters.

Concur:

Harrel M. Pettway
General Counsel

2. Describe the general obligations of the board of directors (board) of covered institutions and establish standards that encourage an active and involved board to protect the interests of the covered institution and oversee and confirm that it operates in a safe and sound manner.
3. Emphasize the importance of the board and management adopting and implementing a code of ethics requiring high ethical standards in the covered institutions' operations.
4. Discuss the organization of the board, including a committee structure designed to permit the board to actively oversee the affairs of the covered institution.
5. Describe the general obligations of individual directors.
6. State that the board should establish, and management should implement, an effective risk management program that identifies, measures, monitors, and manages risk appropriate for the size, complexity, business model, and risk profile of the covered institution.
7. Include a three-line-of-defense model of risk management for monitoring and reporting risks consisting of business units (front line units), an independent risk management function (led by a chief risk officer), and the covered institution's internal audit unit (led by a chief audit officer).
8. State that the covered institution should effectively communicate its risk appetite and policies to encourage compliance by all employees, identify breaches of policies and procedures, and establish consequences even if the covered institution does not realize a loss from the breach.
9. Would be enforceable under Section 39, which authorizes the FDIC to take formal action if an institution fails to submit and implement, upon FDIC request, an acceptable plan to achieve compliance with safety and soundness standards.

Recommendation: That the Board of Directors authorize the publication of the Proposed Rule and Guidelines in the *Federal Register* for a 60-day public comment period.

Discussion

Background

The FDIC observed during the 2008 financial crisis and more recent bank[1] failures in 2023 that financial institutions with poor corporate governance and risk management practices were more likely to fail.[2] Reports reviewing the recent 2023 bank failures noted that poor corporate governance and risk management practices were contributing factors.[3] Failures of insured depository institutions (IDIs) impose costs on the Deposit Insurance Fund (DIF) and negatively affect a wide variety of stakeholders including the institution's depositors and shareholders, employees, customers (including consumers and businesses that rely on the institution's services and the availability of credit), regulators, and the public as a whole. The proposed standards would serve to improve corporate governance and risk management practices at covered institutions by:

- Clarifying the FDIC's minimum expectations for corporate governance in covered institutions to promote ethical business practices, prudent risk taking, consumer protection, and effective risk management; and
- Helping to improve the safe and sound operation of covered institutions by

[1] The term "bank" is used to mean the same thing as "insured depository institution" as defined in Section 3 of the FDI Act.

[2] *Lessons Learned and a Framework for Monitoring Emerging Risks and Regulatory Response*, GAO Report to Congress, GAO-15-365, June 2015; FDIC OIG Reports – Bank Failures, https://www.fdicoig.gov/reports-publications/bank-failures; Remarks by Martin J. Gruenberg, Chairman, FDIC to the American Association of Bank Directors, May 12, 2015, https://archive.fdic.gov/view/fdic/1717; *Review of the Federal Reserve's Supervision and Regulation of Silicon Valley Bank,* April 2023, https://www.federalreserve.gov/publications/files/svb-review-20230428.pdf; *FDIC's Supervision of Signature Bank,* April 2023, https://www.fdic.gov/news/press-releases/2023/pr23033a.pdf.

[3] The FDIC report on the failure of Signature Bank in 2023 found that the root cause of the failure was poor management without adequate risk management practices and controls. The institution's management did not prioritize good corporate governance practices (*FDIC's Supervision of Signature Bank*, April 28, 2023, p. 2). The Board of Governors of Federal Reserve System's report on the failure of Silicon Valley Bank also identified governance and risk management deficiencies that led to the failure. (*Review of the Federal Reserve's Supervision and Regulation of Silicon Valley Bank,* April 2023, p. 1).

providing guidelines for good management with an active board, strong risk management for all risks applicable to the institution, and a corporate culture that emphasizes compliance with applicable laws and regulatory requirements (including consumer protection laws and regulations and the Community Reinvestment Act), and high ethical standards.

Proposed Rule and Guidelines

The FDIC would issue the proposed Guidelines pursuant to Section 39 of the FDI Act. Section 39 authorizes the FDIC to issue safety and soundness standards by guideline or by regulation. By issuing the proposed standards as guidelines, if a covered institution fails to meet a proposed standard, the FDIC may require the covered institution to submit a compliance plan and may take other corrective action depending upon the circumstances. If a covered institution fails to submit an acceptable compliance plan requested by the FDIC, or fails to implement an acceptable plan, the FDIC shall require by order, pursuant to Section 39, that the covered institution correct the deficiency and may take other action against the institution. In addition to the Guidelines, the rule proposes amendments to sections 308.302 and 364.101 of the FDIC's regulations to reference the proposed Guidelines.

The proposed Guidelines contain standards for corporate governance and risk management at covered institutions.[4] The proposed Guidelines include a description of the general obligations of the board to ensure good corporate governance. The FDIC expects covered institutions to have good corporate governance, including the key component of an active and involved board protecting the interests of the covered institution rather than the interests of the

[4] Under the Guidelines, the FDIC reserves authority to modify or extend the time for compliance for any covered institution and modify the Guidelines, as needed to address their applicability to insured branches of foreign banks because those institutions typically do not have a board.

parent or affiliates of the covered institution. The proposed Guidelines emphasize setting goals, approving a strategic plan, approving policies, and selecting and supervising senior management so that the covered institution will operate in a safe and sound manner. The proposed Guidelines also emphasize the importance for the board and management to adopt and implement a code of ethics and to demonstrate and require high ethical standards in the covered institutions' operations.

For a covered institution that has a parent company, if the risk profiles of each entity are substantially similar, the covered institution may adopt and implement all or any part of its parent company's risk management program that satisfies or exceeds the minimum standards of these Guidelines. However, the safety and soundness of the covered institution should not be jeopardized by the parent company's decisions, and the covered institution's risk profile should be easily distinguished from that of its parent for risk management and supervisory reporting purposes.

The proposed Guidelines provide that in determining the appropriate number of directors and the board's composition, the board should consider how the selection of and diversity among board members collectively and individually may best promote effective, independent oversight of covered institution management and satisfy all legal and regulatory requirements for outside and independent directors.[5]

The proposed Guidelines discuss the organization of the board, including a committee structure designed to permit the board to actively oversee the affairs of the covered institution. Committees include Audit, Compensation, Trust (if the institution has trust powers), Risk, and

[5] For example, 12 CFR Part 348 implements the Depository Institution Management Interlocks Act. That Act prohibits interlocking relationships of management officials of various nonaffiliated depository institutions, depending on the asset size and geographical proximity of the organizations.

any other committees that might be necessary or appropriate (for example, Information Technology/Cybersecurity). Under the proposed Guidelines, board and committee meetings should be well documented.

The proposed Guidelines describe the general obligations of individual directors.

The proposed Guidelines note that both the board and management of the covered institution share responsibility for the covered institution's risk management. Under the proposed Guidelines, the board should establish an effective risk management program that identifies, measures, monitors, and manages risk appropriate for the size, complexity, and risk profile of the covered institution. The board should approve a risk profile and risk appetite statement to direct management in taking only appropriate risks. The proposed Guidelines include a three-line-of-defense model of risk management for monitoring and reporting risks. Front line business units are the first line of defense; they are responsible for limiting their risk-taking activities to those approved by management within the risk appetite statement. Covered institutions also should have as a second line of defense an independent risk management function, led by a Chief Risk Officer, with appropriate safeguards to ensure independence from front line units and senior management, reporting directly to the board Risk Committee or the board as a whole.

The third line of defense is the covered institution's internal audit unit, led by a Chief Audit Officer, with appropriate safeguards to ensure independence, which in addition to its other duties, should make sure that the risk management program complies with the proposed Guidelines and that the risk management program is appropriate for the size, complexity, and risk profile of the covered institution. The internal audit function should report directly to the Audit Committee or the board. The proposed Guidelines state that the covered institution should effectively communicate the institution's risk appetite and policies to encourage compliance by

all employees. The covered institution also should identify and report breaches of risk limits, with consequences even if the covered institution does not realize a loss from the breach.[6]

Conclusion

FDIC staff recommends that the FDIC Board authorize the publication of the Proposed Rule and Guidelines in the *Federal Register* for a 60-day comment period.

Staff Contacts:

RMS		Legal	
Judy Gross	ext. 8-7047	Jennifer Jones	ext. 8-6768
		Catherine Topping	ext. 8-3975
		Nicholas Simons	ext. 8-6785
		Kimberly Yeh	ext. 8-6514

[6] The proposed guidelines are generally consistent with corporate governance and risk management guidelines issued by Office of the Comptroller of the Currency. *See* 12 CFR Part 30 (App. D) (*Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches)*. *See also* the Board of Governors of the Federal Reserve System's Regulation YY, 12 CFR 252.22, Subpart C, *Risk Committee Requirements for Bank Holding Companies with Total Consolidated Assets of $50 Billion or More and Less Than $100 Billion*.