Key Takeaways from the FDIC's Proposed Guideline for Corporate Governance and Risk Management

October 18, 2023

On October 11, 2023, the Federal Deposit Insurance Corporation (the "FDIC") published in the Federal Register for comment a notice of proposed rulemaking to establish new guidelines (the "Proposed Guidelines") for governance and risk management at FDIC-supervised insured depository institutions (i.e., state non-member banks) with $10 billion or more in consolidated assets ("covered institutions").[1] The Proposed Guidelines would be issued as Appendix C to the FDIC's standards for safety and soundness regulations in part 364 and would be enforceable under Section 39 of the Federal Deposit Insurance Act (the "FDI Act").

The Proposed Guidelines seek to improve the safety and soundness of covered institutions through governance and risk management following the bank failures this past spring. The preamble, referring to the post-mortem evaluations of the Signature Bank and Silicon Valley Bank ("SVB") failures created by the FDIC and the Federal Reserve Board (the "FRB"), asserts that poor governance and risk management practices were contributing factors leading to the failure of those banks.[2]

In developing the Proposed Guidelines, the FDIC considered and drew from the principles set forth in both the Office of the Comptroller of the Currency (the "OCC")'s Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches (the "Heightened Expectations")[3] and the FRB's Regulation YY (the "Enhanced Prudential Standards") and are intended to align the FDIC's supervision framework more closely with the other federal banking regulators. Notably, however, the FDIC sets its threshold for application ($10 billion or more in consolidated assets) much lower than the OCC or FRB. The Heightened Expectations only apply to federally chartered banks with at least

---

1 *Guidelines Establishing Standards for Corporate Governance and Risk Management for Covered Institutions with Total Consolidated Assets of $10 Billion or More*, 88 Fed. Reg. 70391 (Oct. 11, 2023).

2 For more information on regulators' post-mortem evaluations of the Signature Bank and SVB failures, please see our prior FinReg and FinTech Blog post, *Key Takeaways from Bank Failure Reports* (May 1, 2023), *available here*.

3 *OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations*, 79 Fed. Reg. 54518 (Sept. 11, 2014).

$50 billion in consolidated assets, and the risk management requirements of the Enhanced Prudential Standards only apply to bank holding companies with consolidated assets exceeding $100 billion and foreign banking organizations with combined U.S. assets of $100 billion or more.

The Proposed Guidelines also would codify prior FDIC guidance and supervisory expectations, including regarding the role of the board of directors. As we note below, however, certain expectations set out in the Proposed Guidelines would exceed the Heightened Expectations in prescriptiveness and stringency, while others appear different from the guidance set forth in the Heightened Expectations.

The Proposed Guidelines were released over the dissent of two Republican Board members FDIC Vice Chairman Travis Hill and Director Jonathan McKernan. In his dissenting statement, Director McKernan opined that some of the Proposed Guidelines may "conflate the roles of board and management, preempt state corporate law, and potentially conflict with regulatory expectations applicable to parent companies."

On December 4, 2023, the period for public comment on the on the Proposed Guidelines was extended from December 11, 2023 to February 9, 2024.

KEY TAKEAWAYS

Below we discuss some key takeaways from the proposal. As a general matter, the Proposed Guidelines would increase compliance burdens on covered institutions and would increase the possibility of FDIC enforcement actions.

Content of Proposed Guidelines

The Proposed Guidelines would set standards for corporate governance, risk management practices and board oversight. As discussed further below, there are some specific instances where a covered institution may leverage its parent company's risk management program or board to meet these standards.

1. Board of Directors

a. ***Composition***. The Proposed Guidelines set out minimum standards for board composition, requiring a majority of its members to be independent and outside directors (consistent with the FDIC's guidance for applications for deposit insurance).[4] In terms of director independence between a covered institution and its

[4] *Applying for Deposit Insurance: A Handbook for Organizers of De Novo Institutions, Division of Risk Management Supervision (Dec. 2019), available here.*

parent company, where the business of a covered institution's parent is consolidated predominantly in the covered institution, an independent director of the parent may also be an independent director of the covered institution, provided that the director is not a principal, member, director, officer or employee of any other institution or affiliates of the parent. The Proposed Guidelines also emphasize the importance of diversity and caution against excessive influence from a "dominant policymaker."[5]

b. ***Committees***. The Proposed Guidelines also require boards to maintain a risk committee and compensation committee in addition to the audit committee required by Section 36 of the FDI Act and part 363 of the FDIC's regulations. Risk committees would need to meet at least quarterly and maintain records of its proceedings, including risk management decisions. The Proposed Guidelines are unclear on the issue of whether the would-be requirement of an audit committee can be satisfied by the audit committee of a covered institution's bank holding company (as is permitted under certain circumstances by part 363).

c. ***Compensation Oversight***. The Proposed Guidelines reflect the FDIC's focus on board oversight of compensation programs, including through the requirement that a covered institution establish a dedicated, standalone compensation committee, and by requiring that the board adopt and oversee a Compensation and Performance Management Program.

d. ***Policies and Board Approvals***. The Proposed Guidelines envision a covered institution's board taking an active role in establishing key components of the risk management program in addition to overseeing management. The board would approve a covered institution's strategic plan and Code of Ethics, among other policies. While the FDIC's Pocket Guide for Directors indicates that the board should ensure a bank has certain policies (including a Code of Ethics), it does not explicitly require approval of such policies by the board.[6] The Proposed Guidelines also require at least an annual review by the board of these policies. Additionally, the board would have to review and approve a covered institution's risk appetite statement at least quarterly (or more frequently, as necessary, depending on the size and volatility of risks and any material changes in the covered institution's business model, strategy, risk profile or market conditions). In contrast, the Heightened Expectations require review of the risk appetite statement at least annually and only by the board's risk committee.

---

[5] The Proposed Guidelines would codify in regulation a concept already present in the FDIC's "RMS Manual of Examination Policies – Management" (the "RMS Manual"), stating that "a dominant policymaker may inhibit the directors' exercise of independent judgment or prevent the board from fulfilling its responsibilities." 88 Fed. Reg., *supra* note 1, at 70405. Under the RMS Manual, examiners are expected to consider the risks associated with a "dominant management official."

[6] *Pocket Guide for Directors*, FDIC (Dec. 13, 2007), *available* here.

2. Risk Management Program

a. ***Three Lines of Defense Model***. The Proposed Guidelines would require covered institutions to adopt a three-lines-of-defense risk management framework with a front line unit (which is exclusive of a covered institution's legal department), an independent risk management unit led by a Chief Risk Officer and an internal audit unit led by a Chief Audit Officer.

i. Director McKernan's dissenting statement notes that the Proposed Guidelines would appear to expect "all second-line risk management responsibilities, including with respect to compliance-risk management, [to] be overseen by the Chief Risk Officer and the Risk Committee," suggesting that a separate compliance function would be precluded.[7]

ii. The Proposed Guidelines are more prescriptive than the Heightened Expectations in that they would require more responsibility on the part of the independent risk management unit, requiring that the unit ensure that the front line meets risk management standards and establish compliance procedures and processes.

b. ***Use of Parent Company Structure***. The Proposed Guidelines would permit a covered institution to use all or part of its parent company's risk governance framework to satisfy the Proposed Guidelines in instances where the covered institution has a substantially similar risk profile to its parent company, provided that (i) parent company decisions do not jeopardize the safety and soundness of the covered institution; and (ii) the covered institution's risk profile is easily distinguishable and separate from that of its parent for risk management and supervisory reporting purposes.

c. ***Types of Risk to be Addressed in Risk Management Program***. The Proposed Guidelines provide that the following risks would need to be covered and addressed in a covered institution's risk management program: operational (including, but not limited to, conduct, information technology, cybersecurity, AML/CFT compliance and the use of third parties to perform or provide services or materials for the covered institution), strategic, credit, concentration, interest rate, liquidity, price, model and legal risk.

d. ***Focus on Data Architecture and IT Infrastructure***. A covered institution's independent risk management unit would need to establish policies, procedures and processes that provide for the design, implementation and maintenance of a data

---

[7] *Statement by Jonathan McKernan, Director, FDIC Board of Directors, on the Proposed Guidelines Establishing Standards for Corporate Governance and Risk Management*, FDIC (Oct. 3, 2023), *available* here.

architecture and IT infrastructure that supports the covered institution's risk aggregation and reporting needs both during normal and stressed times. Further, material risks, concentrations, breaches of risk limits and emerging risks would need to be reported in a timely manner to the board and the CEO.

3. Identifying and Reporting Violations of Law

a. ***Internal Escalation***. The Proposed Guidelines would require a covered institution's board to establish processes by which personnel in front line and risk management units would identify, document and notify the chief executive officer and the board's audit and risk committees of violations of law or regulation. The requirement for documenting and notifying violations of law and regulation in writing would be a new requirement not currently present in existing FDIC guidance (e.g., the FDIC's Pocket Guide for Directors or the Heightened Expectations. Further, this requirement appears to directly address some of the observations made by the FDIC and FRB in their post-mortem reports regarding SVB.

b. ***Reporting to Relevant Agency***. The Proposed Guidelines would require the covered institution to timely report these violations to the agency with jurisdiction over those matters. This would represent a shift from the FDIC's current practice of encouraging, but not requiring, self-reporting of violations.

Collectively, the escalation of burdens of reporting requirements imposed by the proposal would appear to increase the likelihood of FDIC enforcement actions, even if issues identified are promptly remediated. Moreover, if the FDIC and a covered institution differ as to whether a violation has occurred, the FDIC could nonetheless cite the covered institution for failure to report it.

4. Enforceability

Section 39 of the FDI Act provides that, in the event of a covered institution's failure to abide by standards prescribed by guidelines, the FDIC may, in its discretion, require the covered institution to submit a plan for the FDIC's approval detailing steps it will take to comply with such standards. The Proposed Guidelines and the Heightened Expectations share Section 39 as their basis for enforceability.

5. Questions

The FDIC asks multiple questions regarding the scoping of banks that should be subject to the Proposed Guidelines, including whether FDIC-supervised institutions with $10 billion or more in total consolidated assets is an appropriate threshold and whether other financial institutions should fall under the definition of a covered institutions.

As mentioned above, the period for comment was extended to close on February 9, 2024.

* * *

Please do not hesitate to contact us with any questions.

Satish M. Kini
Partner, Washington, D.C.
+1 202 383 8190
smkini@debevoise.com

Courtney M. Dankworth
Partner, New York
+1 212 909 6758
cmdankworth@debevoise.com

Gregory J. Lyons
Partner, New York
+1 212 909 6566
gjlyons@debevoise.com

Caroline N. Swett
Partner, New York
+1 212 909 6432
cnswett@debevoise.com

Courtney Bradford Pike
Associate, New York
+1 212 909 6757
cbpike@debevoise.com

Tejas N. Dave
Associate, New York
+1 212 909 6155
tndave@debevoise.com

Tara R. Holzer
Law Clerk, New York
+1 212 909 6494
trholzer@debevoise.com