FDIC's Corp. Governance Proposal: What Banks Should Know

By **Grant Butler and Robert Tammero** (October 31, 2023)

Grant Butler

Robert Tammero

On Oct. 5, the Federal Deposit Insurance Corporation issued a notice of proposed rulemaking seeking comment on proposed corporate governance and risk management guidelines.

The guidelines would apply to all insured state nonmember banks, state-licensed insured branches of foreign banks and insured state savings associations with total consolidated assets of $10 billion or more, i.e., covered institutions.

The FDIC may also apply the guidelines in whole or in part to any institution with less than $10 billion in total consolidated assets if the FDIC determines that such institution's operations are highly complex or present heightened risk.

The guidelines would be in addition to the existing operational and managerial standards set forth in the interagency guidelines establishing standards for safety and soundness.[1]

The $10 billion asset threshold will be measured as the total assets reported on an institution's call report for the two most recent quarters.

For institutions approaching $10 billion in assets, the FDIC believes that two quarters will provide institutions a sufficient on-ramp for compliance.

The FDIC stated that it is proposing the guidelines in light of its observation that during the global financial crisis and the bank failures earlier this year, "financial institutions with poor corporate governance and risk management practices were more likely to fail."[2]

Although the guidelines will only explicitly apply to covered institutions, it is important for all FDIC-supervised institutions to be aware of the standards proposed in the guidelines as both a best practice and given that regulatory guidance targeted at larger institutions often influences supervisory expectations for smaller institutions.

Standards Proposed in the Guidelines

The guidelines are intended to clarify the FDIC's minimum expectations for corporate governance of covered institutions, which the FDIC believes will promote ethical business practices, prudent risk-taking, consumer protection and effective risk management.

Further, the guidelines are intended to improve the safe and sound operation of covered institutions by promoting active engagement by boards of directors, strong management of risks applicable to institutions, and a culture of compliance with applicable laws and regulatory requirements.

Specifically, the guidelines:

- Articulate certain obligations of the board of directors of a covered institution, including setting an appropriate tone from the top, approving a strategic plan and policies, establishing a code of ethics, selecting and appointing qualified executive officers, providing ongoing director training, conducting annual self-assessments, and establishing compensation and performance management programs;

- Establish certain duties of board members of a covered institution;

- Direct covered institutions to consider how diversity among board members may best promote effective, independent oversight of institutions;

- Discuss the organization of the board of directors, including by setting standards for the board's committee structure, including an audit committee — in compliance with Section 36 of the Federal Deposit Insurance Act and Title 12 of the Code of Federal Regulations, Section 363 — a compensation committee, a trust committee if the covered institution has trust powers, and a risk committee with an independent director as chair;

- 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;

- Require a covered institution to establish the three lines of defense model of risk management for monitoring and reporting risks consisting of a first line of defense composed of business units, a second line of defense composed of an independent risk management function led by a chief risk officer and a third line of defense composed of the covered institution's internal audit unit led by a chief audit officer;

- State that a 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; and

- Would be enforceable under Section 39 of the Federal Deposit Insurance Act, 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.

Key Takeaways

Many of the corporate governance and risk management standards set forth in the guidelines are already in practice at covered institutions.

However, covered institutions vary in how they currently implement these standards. The more prescriptive of the guidelines may pose challenges for certain covered institutions.

For example, the three lines of defense risk management model is widely adopted and has been implemented by nearly all larger financial institutions.

However, applying the three line of defense risk management model to smaller regional institutions may be challenging as it requires independence and separation of function across departments and some duplication of effort.

Further, there is long-standing diversity of opinion as to whether certain functions, particularly the legal function, should be considered a control function within such risk management models.

The guidelines also may be interpreted to subsume the compliance function into the risk management function, whereas many existing financial institutions have separate compliance and risk management functions that comprise their second line of defense.

The guidelines also raise questions about whether the FDIC would be imposing new substantive legal duties on directors of covered institutions.

For directors of state-chartered institutions, state law generally defines directors' fiduciary duties.

The guidelines would impose on directors of a covered institution affirmative duties to safeguard the interests of the covered institution and confirm that it operates in a safe and sound manner and in compliance with all laws and regulations.

The board of a covered institution, the guidelines state, "should consider the interests of all its stakeholders, including shareholders, depositors, creditors, customers, regulators, and the public."

Such duties would be in addition to, and particularly in the latter case might be viewed as not entirely consistent with, directors' fiduciary duties under applicable state law.

The guidelines suggest that the board of a covered institution be composed of diverse membership. The guidelines refer to diversity broadly for this purpose, to include not just demographic factors such as age, race, ethnicity, gender or social background, but also differences in experience, perspective, opinion and level of ownership of the covered institution's stock.

Notably, the guidelines do not propose to set any standard for professional competencies or other qualifications for board members.

The guidelines also provide that the board of a covered institution should include a majority of outside and independent directors.

The impact of this would appear to be that board composition could not be mirrored between a holding company and its insured depository subsidiary unless the holding company conducts limited or no additional business operations and the independent directors are not affiliated with any other institution or holding company affiliate.

Comparison to Other Agencies' Corporate Governance Guidance

The guidelines are similar to existing corporate governance and risk management guidance issued by the Office of the Comptroller of the Currency[3] and the Board of Governors of the Federal Reserve System.[4]

An important distinction between the guidelines and the guidance issued by the OCC and the Fed is that these other regulators apply their heightened corporate governance and risk management standards to institutions with over $50 billion in assets.

The guidelines differ in other significant ways. The guidelines are generally more specific and prescriptive regarding corporate governance than the OCC and the Fed guidance.

Neither the OCC nor the Fed guidance provides for the board diversity considerations discussed in the guidelines nor set forth standards for board committee structures.

The OCC's guidance only requires two board members of a covered bank be independent, rather than the majority of the board as proposed in the guidelines.

Dissension on the FDIC Board

The guidelines were approved by a three-two notational vote outside the FDIC board's customary meeting schedule.

The two Republican appointees to the FDIC board each voted against the guidelines and issued statements expressing concerns with the proposal.

Travis Hill, vice chairman of the FDIC, expressed skepticism that violating the standards in the guidelines should be deemed a violation of safety and soundness, and further stated that FDIC examiners should focus on banks' core financial condition.

He also expressed concerns over the focus on diversity in selecting board members as opposed to focusing on relevant experience and qualifications.

FDIC Director Jonathan McKernan issued a statement listing a litany of concerns regarding the guidelines as proposed, including his view that the guidelines would undermine accountability for risk ownership, conflate the roles of board and management, preempt state law, and potentially conflict with regulatory expectations at parent companies.

Takeaways for Community Banks With Under $10 Billion in Assets

Community banks with less than $10 billion in consolidated assets would not be subject to the guidelines unless deemed by the FDIC to be highly complex or presenting heightened risk.

However, community banks have often experienced that guidance intended for larger institutions affects supervisory expectations for all institutions.

Unlike the corporate governance and risk management guidance issued by the OCC and the Fed, which apply to considerably larger institutions, the guidelines would apply to banks that in some cases have business models that are very similar, if not identical, to those of many community banks.

Thus, community banks should expect some or all of the standards in the guidelines, if adopted, to become viewed as industry best practice. This may have an impact on how boards of directors are composed and function, such as with respect to diversity of membership and committee structure.

Community banks should consider whether to adopt codes of ethics and risk management programs that incorporate those standards in the guidelines that are applicable to the bank's operations.

For smaller community banks it would be difficult to fully implement the three lines of defense model, however, all banks should consider incorporating aspects of that model, such as front line unit responsibility to manage risk, into their risk management models.

The Final Guidelines May Differ From the Proposed Guidelines

The proposed guidelines are likely to attract a significant number of comments from the banking industry and other interested groups.

Financial institutions concerned by the scope or some of the more prescriptive requirements of the proposed guidelines should consider submitting their own comments.

Given the dissension on the FDIC board regarding the proposal, and its wide-reaching effects, there is a strong possibility the final guidelines may differ in important ways from the proposed guidelines.

Grant F. Butler and Robert M. Tammero Jr. are partners at K&L Gates LLP.

[1] 12 C.F.R. pt. 364, app. A.

[2] 88 F.R. 70391 (October 10, 2023).

[3] 12 C.F.R. pt. 30, app. D.

[4] See 12 C.F.R. § 252.22; SR Letter 16-11, Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $100 Billion (Feb. 17, 2021), https://www.federalreserve.gov/supervisionreg/srletters/sr1611.htm; SR Letter 95-51, Rating the Adequacy of Risk Management Processes and Internal Controls at State

Member Banks and Bank Holding Companies (Feb. 26, 2021), https://www.federalreserve.gov/boarddocs/srletters/1995/sr9551.htm.