One Size Fits All: The FDIC's Proposed Corporate Governance and Risk Management Guidelines

Max Bonici, Ellen Berge, Andrew Bigart, Michael Aphibal, and Connor Webb

October 2023

The FDIC has proposed guidelines that would establish corporate governance and risk management expectations for FDIC-regulated banks with $10 billion or more in total assets. The FDIC is doing so in a rulemaking under its safety and soundness powers in Section 39 of the Federal Deposit Insurance Act. The new guidelines are the latest in the FDIC's string of regulatory responses to the 2023 spring bank failures.

The FDIC's proposed guidelines are based on similar OCC guidelines, but with key differences. The proposed guidelines include more details on what the FDIC expects from the boards of directors as well as the banks that the FDIC regulates. The proposed guidelines also use a notably lower minimum asset threshold (five times lower) than the OCC's guidelines to determine which banks are covered.

The proposed guidelines were approved 3-2: Chairman Gruenberg, CFPB Director Chopra, and acting Comptroller Hsu voted in support; Vice Chairman Hill and Director McKernan voted against the proposal.

Comments on the proposed guidelines are due by December 11, 2023.

Key Takeaways

- **Guidelines as regulation.** The FDIC's proposed guidelines would be promulgated by rulemaking as an appendix to Part 364 of the FDIC's regulations, and thus would not be mere guidance. The FDIC explained in the preamble that this approach allows it to leverage its enforcement powers.
- **Greater clarity is the goal.** The proposed guidelines would seek to clarify the FDIC's expectations for boards of directors and management of banks. While certainly more detailed, the proposed guidelines would fundamentally move to a more prescriptive model, rather than a principles-based framework.
- **Tailoring is practically gone.** The guidelines would apply to all insured state-chartered banks that are not members of the Federal Reserve System with $10 billion or more in total assets. One-size-fits-all prescriptive rules are the very essence of non-tailored rulemaking. The new guidelines are the latest in an anti-tailoring trend that has followed the spring 2023 bank failures.
- **Board composition—independence.** The proposal would expect a majority of the directors to be independent. Members of the parent bank holding company who are on the bank's board may not always be "independent" for purposes of this expectation, which would appear to be in tension with the Federal Reserve's controlling influence framework.
- **Board composition—social and age diversity, among others.** Boards would also be expected to "consider" the diversity of their members, including "social," age, and educational differences, among others.
- **Non-shareholder constituencies.** The FDIC would introduce an expectation that a board consider the interests of all of its so-called stakeholders, beyond shareholders and depositors, to include creditors and even the regulators themselves. As Director McKernan's statement notes, that expectation may conflict in some respects with state law.

- **Self-reporting of violations of law.** Boards would be expected to establish processes for reporting all violations of law and regulation to law enforcement or the appropriate regulatory agency. As written, this proposed expectation would appear to significantly interfere with the way banks assess legal and compliance risks and their remediation efforts.

Applicability of the Proposed Guidelines

General Coverage

The proposed guidelines would apply to all insured state-chartered nonmember banks, state-licensed insured branches of foreign banks, and insured state savings associations with total consolidated assets of $10 billion or more (which we generally refer to as "banks" or "covered banks" in this alert) on or after the proposed guidelines' effective date.

A bank would be covered under the proposed guidelines once its total assets, as reported on its call report, meet the threshold for two consecutive quarters. Covered banks, however, would need to demonstrate four consecutive quarters of their total assets being below the threshold, as reported on their call reports, in order to escape being covered. The FDIC estimates that 57 banks would be affected if the guidelines were to be adopted as proposed.

The Federal Reserve or the OCC generally regulates most banks that are large or complex, while most FDIC-regulated banks are relatively smaller and not particularly complex. That the FDIC is issuing these guidelines at all may reflect a need for the FDIC to demonstrate a robust response to the 2023 bank failures, as we have seen in other recent developments. The FDIC's proposed guidelines would close a perceived gap in regulatory coverage, insomuch as the OCC currently has agency-specific, additional guidelines.

The FDIC's minimum asset threshold marks a notable difference between the proposed guidelines and the applicability of comparable OCC guidelines. The OCC's guidelines apply to national banks, federal thrifts, and federal branches with total consolidated assets of $50 billion or more. (We note that none of the banks that failed in spring 2023 had a federal charter.) By setting a lower threshold, the FDIC would be continuing its anti-tailoring trend by essentially treating any bank other than a community bank as a large—and therefore riskier—financial institution.

Backup Discretion to Cover Any FDIC-Regulated Bank

Under the proposed guidelines, the FDIC would reserve the authority to impose the proposed guidelines on any bank it regulates, including those under the minimum asset threshold. The FDIC would need to give notice before applying the guidelines to any bank under the minimum asset threshold, but the details about how the FDIC would identify such banks are not entirely clear. Because the proposed guidelines ultimately bear on safety and soundness concerns, however, we expect that these requirements may be imposed through the supervisory process.

The FDIC would similarly reserve the right to except banks that meet the threshold from the proposed guidelines, depending on the complexity and level of risk that the bank's operations present.

Corporate Governance Standards

The FDIC's proposed guidelines delve into legal issues that typically—in the case of banks that do not have a federal charter—have been determined by state law, such as the duties and responsibilities of banks' boards, directors, and management.

Stakeholder Interests

The proposed guidelines would also push banks' boards to consider more than just the interest of the bank's shareholders. These provisions would expect boards to consider the interests of a bank's so-called stakeholders,

including those of its shareholders, depositors, and customers, but also of its creditors and regulators, among others. The inclusion of "creditors" is particularly striking, as Director McKernan's statement notes, given that creditors are typically understood to have rather limited rights beyond those provided in contract.

- We have identified only one express reference to "stakeholders" in all of the FDIC's current regulations: within the context of a vote to convert an insured mutual state savings bank to the stock form of ownership. The use of this expansive term is likely due to the mutual form of these banks and the anticipation that different individuals, despite varying titles, may be able to vote on such a conversion. That context is very different from the general expectations for boards of FDIC-supervised banks, other than community banks.
- We did not identify any instance of the OCC regulations using this term, including in its counterpart guidelines.
- Federal Reserve regulations use the term, but in its liquidity requirements under the Enhanced Prudential Standards that generally apply to banks that are at least 10 times the size of the threshold used in the FDIC's proposed guidelines.

These provisions in the proposed guidelines may create conflicts between a covered bank's safety and soundness expectations and the state laws governing directors' fiduciary duties. As noted in Director McKernan's statement, many states' laws permit the boards of banks and corporations chartered under their laws to consider the interests of non-shareholder constituencies when making decisions, but few require boards to do so. Furthermore, among the more permissive states, some allow non-shareholder constituencies' interests to be considered only if the benefits of doing so are expected to accrue to the bank's shareholders.

Directors

Unsurprisingly, boards would be expected to establish a certain tone at the top that promotes responsible, ethical behavior. But the FDIC would further expect that each director has a duty—not just to safeguard the bank's interests and oversee its compliance efforts, but also to confirm that the bank operates in a safe and sound manner and in compliance with all applicable laws. The proposed guidelines would also expect directors to receive formal, ongoing training that keeps them informed of general industry trends, statutory and regulatory developments, and the proposed guidelines' standards, and directors to conduct annual self-assessments of the board's effectiveness in meeting all standards set forth by the proposed guidelines.

Standards for the Composition of Boards of Directors

Diversity

The proposed guidelines would expect boards to reevaluate their numbers and composition. Boards would be expected to "consider" how the diversity of the board as a whole and among its individual directors can promote effective oversight and best help the bank achieve its compliance goals. The proposed guidelines note that diversity may include—besides racial, ethnic, and gender differences—"social," age, and educational differences, among others.

While various studies have demonstrated that diversity can lead to less risky, or even better, decision making in organizations, some aspects of this proposed standard may be difficult to implement in practice. For example, some of the diversity categories that the standard lists are ill defined, such as "social" (perhaps, "socioeconomic") differences. It may ultimately prove practically difficult for a board of a bank of any appreciable size to include directors who represent a range of various age, socioeconomic, and educational backgrounds. Additionally, the guideline is silent on what it means for a board to "consider" diversity among its members.

None of these concepts is in the OCC guidelines.

Independence

Boards of banks would also need to ensure that, at a minimum, their majorities comprise outside and independent directors. The proposed guidelines define an independent director to generally be one who is neither (1) a principal, member, officer, or employee of the bank, nor (2) a principal, member, director, officer, or employee of *any affiliate* or principal shareholder of the bank. In many cases, this second prong would affect a holding company's representation on a bank's board. Because bank holding companies are affiliates of the banks they own, these holding companies would not be considered "independent." The proposed guidelines would provide an exception only for a "holding company [that] conducts limited or no additional business operations outside the institution" (as long as they are not a principal, member, director, officer, or employee of any other institution or holding company affiliates).

This limitation appears restrictive, in light of the Federal Reserve's controlling influence framework in Regulation Y, which implements the Bank Holding Company Act. To avoid being deemed to control a bank—and therefore becoming a bank holding company subject to comprehensive Federal Reserve regulation and supervision—a company that invests in a bank may limit its board representation at the bank, among other factors. However, once a company is deemed to control a bank, it presumably will want all benefits afforded to it by having control, such as board representation to the extent it does not conflict with other laws, such as the Depository Institution Management Interlocks Act. While the FDIC's concern that a bank's board may put the interests of a parent ahead of the bank's interests is legitimate, directors have fiduciary duties to their banks, and bank holding companies must serve as a source of strength to their bank subsidiaries.

Relatedly, the proposed guidelines would also call for each director to exercise independent judgment to the extent possible. This means that a director's decision making would be expected to be free from excessive influence by a "dominant policymaker," whether that policymaker is a member of management, another director, a shareholder, or any such combination.

Board Structure Standards

The proposed guidelines would, in some cases, expressly articulate the FDIC's expectation that boards establish and delegate responsibilities to various board committees, including: (1) audit (entirely composed of outside and independent directors); (2) compensation; (3) trust (if the bank has trust powers); and (4) risk (chaired by an independent director and including at least one member with experience managing risk exposures of large firms).

The proposed guidelines would also expressly encourage boards to establish other committees reflecting the bank's risk profile, such as for lending, information technology, and cybersecurity, among other topics.

Standards for Risk Management

The proposed guidelines heavily emphasize the importance of banks' adopting written policies and procedures that govern their risk management efforts, as well as the board's active involvement either in those efforts or overseeing them.

First, the proposed guidelines contemplate that boards take a firm leadership role in determining how banks identify, evaluate, and respond to risks. Among other things, boards would be expected to approve:

- **An organization-wide ethics statement** that is updated annually and addresses topics such as compliance with applicable laws, certain ethical and integrity issues, how to elevate issues concerning or report illegal and unethical behavior within the bank, and non-retaliation policies for such reporting.
- **A risk profile** that is reviewed and updated quarterly, as well as a **risk appetite statement** reviewed and updated quarterly by the board that establishes the bank's risk appetite limits based on the risk profile. The risk appetite statement should address both quantitative and qualitative metrics, and the limits it contains should take into account appropriate capital and liquidity buffers. It should also be incorporated into policies

and procedures governing other parts of the bank's overall compliance program(s) that are expected to be established and approved by the board as well.

- **A comprehensive strategic plan** developed by management that addresses the bank's goals and objectives over a three-year period (at a minimum) and includes:
    - Explanations for how the bank will reach those objectives
    - A comprehensive assessment of the bank's current risk and the risks it will likely face during the period covered by the plan
    - Explanations for how the bank's risk management program will be updated as necessary to account for unexpected changes in those risks
    - Explanations for how the strategic plan will be updated as necessary to account for other unexpected changes to the bank's risk profile, risk appetite, or operating environment

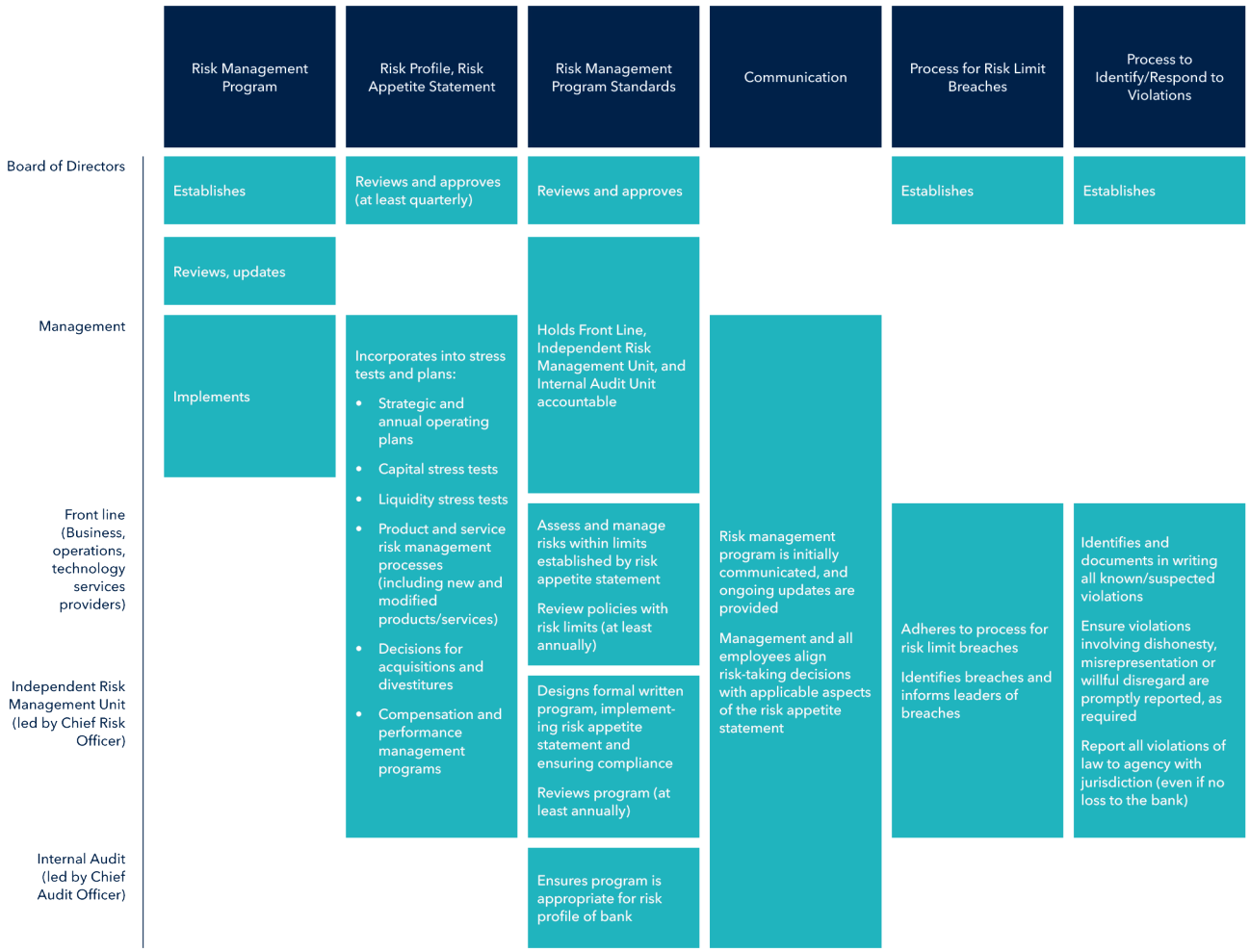
Second, the proposed guidelines contemplate that boards will establish and approve formal, written, and comprehensive risk management programs for their banks. The FDIC would expect each bank's risk management program to cover a wide variety of potential risk categories, ranging from interest rate and liquidity risks to anti-money laundering and third-party partnership and outsourcing risks. Risk management policies, procedures, and processes appropriate for the bank's structure, risk profile, complexity, and size should be in place to address each potentially applicable risk category.

Furthermore, the proposed guidelines would expressly adopt a three-lines-of-defense model for monitoring and reporting risks. This model of risk management under the proposed guidelines would divide risk management responsibilities into three categories within the bank:

1. **Front Line Units:** Comprising a bank's revenue-generating or cost-saving business units, the front line units are primarily responsible for managing day-to-day risks
2. **Independent Risk Management Unit:** Comprising independent risk management staff, the Independent Risk Management Unit reports directly to the CEO and manages more long-term and enterprise-wide risks
3. **Internal Audit Unit:** An internal but independent auditing unit that reports directly to the board's Audit Committee, it assesses the bank's risk management efforts, and issues reports evaluating the success of those efforts and the bank's compliance with applicable laws and other requirements, which may include recommendations for further improvements to the risk management program

Under the three-lines-of-defense model endorsed by the proposed guidelines, a board would be responsible for ensuring accountability and communication between these three units.

Key Responsibilities for Risk Management and Audit



Self-Reporting of Violations of Law

Boards would be expected to establish and annually review processes that would require either front line units or the independent risk unit (consistent with their respective responsibilities) to report *all* violations of applicable laws and regulations to law enforcement or any appropriate federal or state regulatory agency. These processes would need to address:

1. Identifying known or suspected violations
2. Distinguishing violations that appear technical or inadvertent from those that may be willful or involve dishonesty or misrepresentation
3. Documenting the violation, its escalation to the CEO and proper board committees, and any efforts to remediate the violation
4. Ensuring that known or suspected violations involving dishonesty, misrepresentations, or willfulness, regardless of who commits them, are promptly reported *as required by law or regulation*
5. Reporting *all other violations* within a period acceptable to the applicable agency

It is not clear how the last expectation, as written, is grounded in law. Legal violations are serious developments for which banks should take responsibility. To that end, banks and their attorneys regularly work to conduct internal investigations and remediate issues. The decision when and how to disclose violations of law outside of a bank or banking organization is the subject of legal and strategic analyses as well as attorney-client and possibly other privileges, as noted in Director McKernan's statement.

In addition, while the proposed guidelines prescribe self-reporting standards, they are not clear about how those standards should be implemented. For example, the proposed guidelines do not specify the point at which a violation of law is deemed to have occurred, nor do they include any materiality or *de minimis* evaluations. Should banks merely determine for themselves that a violation of law occurred? Or is some finding (by a court or otherwise) that a violation of law occurred required before the bank is obligated to report the violation? If the former, as Director McKernan noted in his statement, a requirement to self-report any and all violations of law may act as a disincentive for a bank to conduct investigations to self-identify and remediate compliance issues.

Furthermore, if a covered bank commits a technical or other violation of a consumer financial protection law, do these guidelines anticipate that the bank always self-reports to the CFPB, which is primarily an enforcement agency, not a prudential regulator? If a bank violates a law of a foreign country, do the guidelines require that the violation be reported to the applicable foreign regulator (e.g., European data privacy law)? Does the analysis change for any and all violations of the laws or requirements of the People's Republic of China?

As written, the scope of this proposed guideline is broad without a clear allowance for how banks and their boards might grapple with these nuanced issues.

Final Thoughts

Many of the proposed guidelines are well intentioned. In the aftermath of the 2023 bank failures, it is understandable that the FDIC would want to clarify and seek to bolster corporate governance and risk management at the banks it regulates and supervises.

But in taking such a prescriptive approach, the FDIC would appear to move away from principles-based corporate governance and toward a much more rule-based framework. In doing so, the FDIC has raised issues that may require more careful explanations of certain guidelines and their components, as well as a reconciliation of those guidelines with certain practicalities, state banking and corporate law, and other federal law, including the laws applicable to bank holding companies.

And as Vice Chairman Hill explained in his statement, it is difficult to see how many of the provisions should rise to the level of enforceable safety and soundness standards, let alone how a one-size-fits-all approach is in fact a best practice for each bank in its unique circumstances.

We would add that a one-size-fits-all approach may not, in all cases, be safe or sound.

Keep track of financial regulatory reform efforts and anti-tailoring trends in the wake of the 2023 bank failures with Venable's Financial Regulatory Reform Tracker.

VENABLE LLP