Davis Polk

Corporate process supercharged: The role of the board under the FDIC's proposed guidelines

October 16, 2023 | Client Update

The FDIC proposed enforceable guidelines on corporate governance and risk management that would apply to all state non-member banks with assets greater than $10 billion. The proposal would impose a number of very detailed and highly prescriptive governance requirements on banks and, in doing so, blurs the line between board and management responsibilities.

Key takeaways

The Federal Deposit Insurance Corporation (FDIC) has proposed enforceable guidelines on corporate governance and risk management that would apply to all state non-member banks with assets greater than $10 billion (the Proposed FDIC Guidelines). The proposal was issued over two dissents.[1] Among the issues the dissents highlighted is that the proposal would seek to impose an enforceable federal overlay on state fiduciary duty standards, which would extend beyond the scope of the Office of the Comptroller of the Currency's (OCC) governance guidelines[2] and of the Federal Reserve Board's (FRB) governance guidance.[3] The proposal also would muddy the waters between board and management responsibilities and impose a number of very detailed and highly prescriptive governance requirements.

It is understandable that, after the March turmoil in the banking sector, the FDIC would want to encourage state non-member banks to have high-quality corporate governance. But it is an open question whether the Proposed FDIC Guidelines, which have a heavy emphasis on process, strike the right balance between process and core safety and soundness concerns,[4] especially when viewed in light of the traditional oversight role of a board and the more modulated viewpoints of the other banking agencies.

Our key takeaways are:

- **Significant new duties for directors.** The proposal would impose sweeping duties on directors by, for example, stating that a director should consider "the interests of all its stakeholders, including shareholders, depositors, creditors, customers, regulators, and the public." This directive may be at odds with the typical fiduciary duty focus on shareholder value. Moreover, the directive may also conflict with duties applicable to directors under stakeholder standards because, although those standards broaden duties beyond shareholder value, the particular formulation can vary by state. Whether and how the proposed standards would be enforced by various parties could lead to confusion and related litigation risk.

[1] Statement by FDIC Vice Chairman Travis Hill on the Proposed Corporate Governance Expectations for Large and Midsize Banks (Oct. 3, 2023); Statement by FDIC Director Jonathan McKernan on the Proposed Guidelines Establishing Standards for Corporate Governance and Risk Management (Oct. 3, 2023).
[2] Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches (Sep. 11, 2014) (the **OCC Guidelines**). *See also* Davis Polk's Visual Memorandum on Risk Governance Guidelines Adopted by the OCC (Nov. 7, 2014).
[3] Supervisory Guidance on Board of Directors' Effectiveness (Feb. 26, 2021) (the **FRB Guidance**). *See also* Davis Polk's Visual Memorandum on The Federal Reserve's Final Board Effectiveness Guidance for Large Financial Institutions (Mar. 3, 2021).
[4] *See* Statement by FDIC Vice Chairman Travis Hill*, supra* note 1.

 © 2023 Davis Polk & Wardwell LLP

Insights

- Other banking agencies have dealt with this issue. For example, the OCC states in its Director's Book that the corporate governance provisions discussed in the book are not intended to, nor do they, exceed applicable state law requirements.
- Given the significance of the duties and obligations that the Proposed FDIC Guidelines would impose, one question is whether such standards should be subject to an interagency policy process to encourage consistency across the banking system.

— **Overuse of "ensure" and other similar verbs would muddy the waters between board and management responsibilities.** The proposal frequently states the board would be required to "ensure" actions take place, rather than oversee management's actions or hold management accountable.

- For example, the proposal would require that the board "ensure" that management corrects deficiencies that auditors or examiners identify in a timely manner. Aside from the fact that this enforceable requirement does not take into account the possibility of an appeal of identified deficiencies, or the possibility that an examination team or auditor might not be correct, it is not feasible for a board to "ensure" such actions by management. The FHFA's similar requirement,[5] which requires that a board "assure its oversight" of the "responsiveness" of executive officers in "addressing all supervisory concerns" is a much more sensible formulation that takes into account the role of the board in holding senior management accountable without muddying the role of the board and the role of management.
- The proposal would also assign other types of actions to the board that do not fully appreciate the oversight role of a board, such as requiring the board to "establish" a corporate culture and policies more generally.
- The overuse of "ensure" was also part of the OCC proposal in 2014 but, in response to extensive comments, the OCC eliminated this aspect of the proposal in the final OCC Guidelines. In addition, the most recent OCC Director's Book eliminated the "ensure" concept. Similarly, the FRB Guidance avoids use of such a standard.

— **Requirement of majority independent directors is broader than the OCC's requirement for two independent directors.** The proposal would require a majority independent board and, for this purpose, an independent director of the bank's holding company does not automatically count as an independent director of the bank, contrary to the commonly used model of total overlap between directors of a holding company and a state non-member bank.

- In order for a director of the bank's holding company to count as an independent director of the bank, the holding company must conduct *limited or no additional* business operations outside of the bank. It is unclear how the FDIC would define "limited or no additional."
  - Many non-member state banks could be affected by this difference.
- In addition, the FDIC should clarify that it does not mean to prohibit an independent director from serving on the board of "any other institution" but instead only the board of "an affiliate of the institution" (here, the bank). The FDIC should also clarify that serving on the board of an operating subsidiary of the bank would not prevent a director from being considered independent; such a clarification would be consistent with the definition of "affiliate" in Regulation W, which addresses similar policy concerns.
- Banks with insider boards or that do not have a majority of outside directors at the bank level may find that they need to make board level changes.

— **Dominant Policymaker.** The Proposed FDIC Guidelines contain a caution about a board being influenced by a "dominant policymaker," whether this is management, a shareholder or a director. The dominant-policymaker concept is unique to the FDIC. Although this term may make sense for a privately held or family-controlled company, its application to a non-member bank whose parent is publicly traded risks creating confusion.

- The FDIC has previously addressed the concept of a "dominant official" in its RMS Manual of Examination Policies – Management, where it describes "the risks associated with institutions controlled by an official that has material influence over virtually all decisions involving the bank's policies and operations."

[5] 12 CFR § 1239.4.

 © 2023 Davis Polk & Wardwell LLP

- While the examination manual refers to this scenario using the terms "control" and "official," the Proposed FDIC Guidelines refer to a "dominant policymaker." It is unclear whether the FDIC intends to broaden the scope with its use of "policymaker."

— **Highly prescriptive, with more governance and process.** The Proposed FDIC Guidelines are highly prescriptive and would require more director time and management process to achieve the same result as the OCC Guidelines and FRB Guidance.[6]

- Where the OCC made a conscious decision not to require approval of many policies by the board, the FDIC would impose a more burdensome requirement on boards to approve a broad swath of policies on an annual basis.
- The FDIC also would impose more frequent reviews and updates with certain requirements imposed quarterly as opposed to annually by the OCC.
- The guidelines also contain highly prescriptive requirements with respect to the board's involvement in the selection of executive officers and their competence.
- The FDIC's requirement that the board, as part of its yearly self-assessment, also evaluate whether it has met the guidelines, means that boards may find themselves engaging in a check-the-box exercise that would not be necessary under the more principles-based approach of the OCC and the FRB. This type of exercise could undermine the spirit of qualitative and dynamic self-assessments, whose focus may change from year to year depending on a board's priorities and focus.

— **Guidelines, Guidance and Enforcement.** *Guidance* does not create enforceable, binding legal obligations. *Guidelines* issued under Section 39 of the Federal Deposit Insurance Act (FDIA), however, are enforceable by the agency.[7] As such, the FDIC has chosen to propose guidelines that "would be enforceable under Section 39." This technique is in contrast to the FRB's approach of adopting principles-based guidance. It is also in contrast to the OCC which has chosen the path of enforceable guidelines, but carefully calibrated its corporate governance guidelines to be general principles. The FDIC's combination of enforceable guidelines, very detailed and highly prescriptive requirements and an obligation for a board to assess, on a yearly basis, whether it is meeting the guidelines, risks imposing burdens on boards that do not further the spirit of seeking to encourage and to facilitate robust, dynamic and healthy governance. For example, if an institution does not meet the guidelines promulgated under Section 39, the agency has the option of requiring a plan to do so. If an institution fails to submit a timely, acceptable plan, the agency can issue a "safety and soundness order." This is the legal equivalent of a cease-and-desist order, i.e., it is public and legally enforceable, including through the assessment of civil monetary penalties. Accordingly, a board may become more focused on a check-the-box exercise to avoid such a result, rather than the more important work of robust, dynamic and healthy governance.

The attached chart is a deep dive that compares the Proposed FDIC Guidelines with the OCC Guidelines and the FRB Guidance. If the Proposed FDIC Guidelines are finalized as proposed, it would not be surprising if they are a factor in many state non-member banks beginning to consider whether they should become a national bank or a Federal Reserve member bank. Comments on the Proposed FDIC Guidelines are due on December 11, 2023.

Law clerk Mitch Murphy contributed to this update.

[6] Recently, after many years of minor differences among them, the three banking agencies aligned on one standard for their risk management guidance for third-party relationships. *See* Davis Polk's Client Update on Bank Risk Management of Third-Party Relationships – Final Interagency Guidance. A similar approach may be useful for corporate governance.

[7] Guidance and guidelines under Section 39 of the FDIA are very different despite the similarity of the words. Banking agencies issue guidance—typically general, principles-based instructions which are not, as a technical legal matter, enforceable (although many banking organizations will rationally act as if they are and follow them). The point is to permit variations if warranted by the circumstances. *See, e.g.*, Role of Supervisory Guidance (Mar. 2, 2021). Guidelines issued under Section 39 of the FDIA are enforceable. 12 U.S.C. 1831p—1(e).

 © 2023 Davis Polk & Wardwell LLP

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your usual Davis Polk contact.

Ning Chiu	+1 212 450 4908	ning.chiu@davispolk.com
Jennifer S. Conway	+1 212 450 3055	jennifer.conway@davispolk.com
Andrew Ditchfield	+1 212 450 3009	andrew.ditchfield@davispolk.com
Mary Jane Dumankaya	+1 212 450 3654	maryjane.dumankaya@davispolk.com
Ledina Gocaj	+1 202 962 7054	ledina.gocaj@davispolk.com
Kyoko Takahashi Lin	+1 212 450 4706	kyoko.lin@davispolk.com
Eric McLaughlin	+1 212 450 4897	eric.mclaughlin@davispolk.com
Margaret E. Tahyar	+1 212 450 4379	margaret.tahyar@davispolk.com
David L. Portilla	+1 212 450 3116	david.portilla@davispolk.com
Daniel P. Stipano	+1 202 962 7012	dan.stipano@davispolk.com

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.

Davis Polk

Comparison of the Corporate Governance Frameworks: Proposed FDIC Guidelines, the OCC Guidelines and FRB Guidance

The following table compares the FDIC's Notice of Proposed Rulemaking on Guidelines Establishing Standards for Corporate Governance and Risk Management against the supervisory expectations described in the OCC's Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches and FRB's Supervisory Guidance on Board of Directors' Effectiveness. The breadth of the FDIC's document goes far beyond that of the OCC Guidelines and FRB Guidance. The OCC and FRB supplement their frameworks with additional detail in supervisory letters and policy statements that do not themselves create binding legal requirements. By contrast, the FDIC has chosen to make a detailed list of highly prescriptive tasks enforceable through its proposed guidelines.

The text of the agency materials below provides near-quotations of the relevant text unless noted otherwise. Text in red font marks the most distinctive differences among the three agencies with a focus on where the FDIC is proposing new or more prescriptive standards. The fourth column is our commentary. We have noted in *italics* where topics covered by the Proposed FDIC Guidance are covered in more informal letters or guidance outside of the OCC Guidelines and FRB Guidance.

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
Scope and Asset Size			
Scope. State non-member banks, state-licensed insured branches of foreign banks, and insured state savings associations. **Asset size**. $10 billion or more in total consolidated assets, as reported in the two most recent consecutive quarters of the institution's Call Report (**FDIC Covered Institutions**).	**Scope**. Insured national banks, federal savings associations, and federal branches of foreign banks. **Asset size**. $50 billion or more, or smaller if the bank's parent company controls an OCC Covered Institution with average total consolidated assets of $50 billion or more, as reported on the institution's Call Report, for the four most recent consecutive quarters (**OCC Covered Institutions**).	**Scope**. Bank holding companies and savings and loan holding companies. **Asset size**. $100 billion or more in total consolidated assets. Excludes U.S. IHCs of FBOs and nonbank SIFIs (**FRB Covered Institutions**).	Expansion in application, especially for small and mid-size state non-member banks.
Reservation of Authority			
The FDIC may apply the guidelines to a bank that has total consolidated assets less than $10 billion.	The OCC may apply the guidelines to a bank that has average total consolidated assets less than $50 billion.	Unclear.	

 © 2023 Davis Polk & Wardwell LLP

Davis Polk

<table>
<tr><th>Proposed FDIC Guidelines</th><th>OCC Guidelines</th><th>FRB Guidance</th><th>Commentary</th></tr>
<tr><td colspan="4">Enforcement</td></tr>
<tr><td colspan="2">Codified guidelines enforceable under Section 39 of the FDIA, which authorizes the federal banking agencies to prescribe safety and soundness standards in the form of guidelines. If an institution does not meet the guidelines promulgated under Section 39, the agency has the option of requiring a plan. If an institution fails to submit a timely, acceptable plan, the agency can issue a “safety and soundness order.” This is the legal equivalent of a cease-and-desist order, i.e., it is public and legally enforceable, including through the assessment of civil monetary penalties.</td><td>Guidance, not enforceable guidelines. Sets forth supervisory expectations for boards and follows a principles-based approach.</td><td>See cover note for discussion of how the Proposed FDIC Guidelines shifts the landscape because it would make the highly detailed and prescriptive requirements enforceable.</td></tr>
<tr><td colspan="4">Fiduciary Duties</td></tr>
<tr><td>Each member of the board has a duty to safeguard, through the lawful, informed, efficient, and able administration of the FDIC Covered Institution, the interests of the FDIC Covered Institution and to oversee and confirm that the FDIC Covered Institution operates in a safe and sound manner, in compliance with all laws and regulations. The board, in supervising the FDIC Covered Institution, should consider the interests of all its stakeholders, including shareholders, depositors, creditors, customers, regulators, and the public.</td><td>Relies on state law as chosen in the by-laws of the national bank or federal savings association.</td><td>Relies on the state law of the holding company.</td><td>Would impose sweeping duties on directors and may be at odds with the typical fiduciary duty focus on shareholder value. The directive may also conflict with duties applicable to directors under stakeholder standards. Whether and how the proposed standards would be enforced by various parties could lead to confusion and related litigation risk.

The OCC Director’s Book states that the corporate governance provisions are not intended to, nor do they, exceed applicable state law requirements.</td></tr>
<tr><td colspan="4">Composition</td></tr>
<tr><td>The board should consider how the selection of and diversity among board members collectively and individually may best promote effective,</td><td>The ideal board is well diversified and composed of individuals with a mix of knowledge and expertise in line with the bank’s size, strategy, risk profile, and</td><td>Factor #5. Maintain a Capable Board Composition and Governance Structure. An effective board considers whether its composition, governance</td><td>The use of “should consider” in the Proposed FDIC Guidelines appropriately mitigates enforceability risk here.</td></tr>
</table>

 © 2023 Davis Polk & Wardwell LLP

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
independent oversight of an FDIC Covered Institution's management and satisfy all legal requirements for outside and independent directors.	*complexity. Although qualifications of individual directors will vary, the directors should provide the collective expertise, experience, and perspectives necessary for effectively overseeing the bank.* (*Corporate and Risk Governance, Comptroller's Handbook*)	structure, and practices support the firm's safety and soundness and the ability to promote compliance with laws and regulations based on factors such as the firm's asset size, complexity, scope of operations, risk profile, and other changes that occur over time.	
Diversity			
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 requirements for outside and independent directors. Important aspects of diversity may include: social, racial, ethnic, gender, and age differences; skills, differences in experience, perspective, and opinion (including professional, educational, and community or charitable service experience); and differences in the extent of directors' ownership interest in the covered institution . . .	*Diversity among directors is an important aspect of an effective board. The board should actively seek a diverse pool of candidates, including women and minorities, as well as candidates with diverse knowledge of risk management and internal controls. (Corporate and Risk Governance, Comptroller's Handbook)*	Effective boards establish processes designed to identify and select potential director nominees with a mix of skills, knowledge, experience, and perspectives, which may take into account, a potential nominee's expertise, availability, integrity, and potential conflicts of interest, and consider a diverse pool of potential nominees, including minorities and women.	The use of "should consider" and "may include" by the FDIC appropriately mitigates enforceability risk here. For banks, with a full overlap board and a public holding company, these requirements are not new. Item 407(c)(2)(iv) of the SEC's Regulation S-K, adopted in 2009, requires public companies to disclose whether and, if so, how, the nominating committee (or board) considers diversity in connection with identifying and evaluating persons as nominees for director. The disclosure must also include, if the company has a diversity policy, a description of how its policy is implemented, as well as how the nominating committee (or the board) assesses the effectiveness of its policy.

 © 2023 Davis Polk & Wardwell LLP

Davis Polk

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
Director Independence			
The board should include a majority of outside and independent directors. – An independent director is generally a director that is (a) not a principal, member, officer, or employee of the institution, and (b) not a principal, member, director, officer, or employee of any affiliate or principal shareholder of the institution. – In instances where an affiliate or a principal shareholder is a holding company, and the holding company conducts limited or no additional business operations outside the institution, an independent director of the holding company may also be an independent director of the institution, as long as they are not a principal, member, director, officer, or employee of any other institution or holding company affiliates.	An OCC Covered Institution's board of directors should include at least two independent directors who satisfy the same independence standards used in the Federal Reserve's enhanced prudential standards final rule under Section 165 of the Dodd–Frank Act. An independent director should: – Not be an officer or employee of the bank or parent company, currently or during the previous three years; – Not be members of the "immediate family" of a person who is, or has been within the last three years, an "executive officer" of the parent company or bank; and – Qualify as independent under the listing standards of a national securities exchange.	An effective board has independent directors who are sufficiently empowered to serve as an effective check against firm executives who sit on the board and senior management.	Requirement of majority independent directors is broader than the OCC's requirement of two independent directors. The Proposed FDIC Guidelines do not automatically protect overlapping directors, contrary to the dominant model in the mid-size banking sector of total overlap between directors of a holding company and bank. It is unclear how the FDIC would define "limited or no additional." This requirement will be new for those state non-member banks who have insider boards or majority insider boards. Moreover, the FDIC should clarify that it does not mean to prohibit an independent director from serving on the board of "any other institution" but instead only the board of "an affiliate of the institution" (here, the bank). The FDIC should also clarify that serving on the board of an operating subsidiary of the bank would not prevent a director from being considered independent; such a clarification would be consistent with the definition of "affiliate" in Regulation W,

 © 2023 Davis Polk & Wardwell LLP

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
			which addresses similar policy concerns.
Set an Appropriate Tone			
The board should establish a corporate culture and work environment that promotes responsible, ethical behavior. . . . The board's actions should reflect its commitment to integrity, honesty, and ethical conduct.	*The board is responsible for setting the tone at the top and overseeing management's role in fostering and maintaining a sound corporate culture and risk culture. (Corporate and Risk Governance, Comptroller's Handbook)*	*The culture, expectations, and incentives established by the highest levels of corporate leadership set the tone for the entire organization and are essential determinants of whether a banking organization is capable of maintaining fully effective risk management and internal control processes. (Bank Holding Company Supervision Manual)*	Goes beyond tone setting, and requires the board to "establish" a corporate culture, blurring the line of board and management, although the words "should" and "promote" mitigate the risk somewhat. The OCC and the FRB text is much more appropriate for the role of a board.
Strategic Plan			
The board is responsible for providing clear objectives within which the FDIC Covered Institution's management can operate and administer its affairs. The board should direct the chief executive officer (**CEO**) to develop a written strategic plan with input from front line units, independent risk management, and internal audit. At least annually, the board should evaluate and approve the strategic plan . . . and ensure the strategic plan is consistent with policies the board has approved. (See Proposed FDIC Guidelines for the specific requirements of the strategic plan.)	The board of directors should evaluate and approve the strategic plan and monitor management's efforts to implement the strategic plan at least annually. The CEO should be responsible for the development of a written strategic plan with input from front line units, independent risk management, and internal audit. (See OCC Guidelines for the specific requirements of the strategic plan.)	**Factor #1. Set Clear, Aligned, and Consistent Direction Regarding the Firm's Strategy and Risk Appetite**. An effective board oversees the development of, reviews, approves, and periodically monitors the firm's strategy and risk appetite. . . . The board evaluates senior management's execution of the firm's strategic plan.	All three are similar.

© 2023 Davis Polk & Wardwell LLP

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
Policies			
The board is responsible for establishing and approving the policies that govern and guide the operations of the FDIC Covered Institution in accordance with its risk profile and as required by law and regulation. (See Proposed FDIC Guidelines for list of potential policies.)	The OCC Guidelines do not require the board or risk committee to review and approve any material policies established under the risk management framework. In the adopting release, the OCC noted that "board or risk committee approval of material policies under the [Risk Management Framework] would be burdensome, and these policies should be approved by management instead."	An effective board reviews and approves significant policies, programs, and plans based on the firm's strategy, risk appetite, risk management capacity, and structure. (See FRB Guidance for examples of policies, programs, and plans.) An effective board might review summarized forms of policies, programs, and plans, with the summarized form including sufficient detail and context for the board to make an informed decision and to consider consistency with the firm's strategy, risk appetite, and risk management capacity.	The Proposed FDIC Guidelines set a much broader mandate for the board to review a much broader range of policies than either the FRB Guidance or OCC Guidelines. The OCC made a determination not to require approval of all policies, while the FRB requires approval only of significant policies. The FDIC's requirement is potentially much more burdensome because the review of multiple policies, in the time constraints facing already overburdened board agendas, means less time for key risk indicators, financial metrics and strategy. It also contains enforceability risk.
Code of Ethics			
The board should establish a written code of ethics for the FDIC Covered Institution, covering directors, management and employees. The code of ethics should be reviewed and updated at least annually.	*The board should adopt a written code of ethics (or code of conduct) to set expected standards of behavior and professional conduct for all employees. Ethics policies should include a process for the annual review and discussion of ethics rules at all levels of the bank, including the board. (Corporate and Risk Governance, Comptroller's Handbook)*	None.	The FDIC has had a long-standing Financial Institutions Letter addressing its Guidance on Implementing an Effective Ethics Program. Item 406 of Regulation S-K requires a public company to disclose whether it has adopted a code of ethics that applies to the company's principal executive officer, principal financial officer, principal accounting officer or controller, or persons performing similar functions,

 © 2023 Davis Polk & Wardwell LLP

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
			and if it has not adopted a code of ethics, to explain why it has not done so. While the Proposed FDIC Guidelines are enacting an existing requirement for most companies, they do so by increasing the burden upon boards. Under the proposal, the code of ethics must be established by the board, reviewed and updated at least annually, and incorporated into the annual self-assessments completed by the board, in addition to the enforceability risk.
Oversight of Management			
The board should actively oversee the FDIC Covered Institution's activities, including all material risk-taking activities. . . . The board also must ensure that management corrects deficiencies that auditors or examiners identify in a timely manner.	The board should actively oversee the OCC Covered Institution's risk-taking activities and hold management accountable for adhering to the risk governance framework.	**Factor #3. Oversee and Hold Senior Management Accountable**. An effective board oversees and holds senior management accountable for effectively implementing the firm's strategy, consistent with its risk appetite, while maintaining an effective risk management framework and system of internal controls. . . . (See FRB Guidance for additional detail, including on boards providing sufficient time for discussion, robust inquiry, evaluation of management performance and compensation.)	The Proposed FDIC Guidelines impose a new burden on boards to "ensure" that management corrects deficiencies identified by auditors or examiners. This obligation is enforceable and appears to be required whether or not the board or management agrees with the deficiencies.

 © 2023 Davis Polk & Wardwell LLP

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
Independent Judgment			
When carrying out his or her duties, each director should exercise sound, independent judgment.	When providing active oversight of management, each member of the board of directors should exercise sound, independent judgment.	Relies on state laws which often have similar statements.	The general obligation for independent judgement is similar across all three agencies and is similar to state laws.
Dominant Policymaker			
To the extent possible, the board should ensure that it is not excessively influenced by a dominant policymaker, whether management, a director, a shareholder, or any combination thereof.	None.	None.	The FDIC is the only agency to address the risks posed by a dominant policymaker who excessively influences the board, which is a scenario more likely to occur with the community banks and mid-size banks that the FDIC supervises. The FDIC has previously addressed the concept of a “dominant official” in its examination manual, where it describes “the risks associated with institutions controlled by an official that has material influence over virtually all decisions involving the bank’s policies and operations.” While the examination manual refers to this scenario using the terms “control” and “official,” the Proposed FDIC Guidelines refer to a “dominant policymaker.” It is unclear whether the FDIC intends to broaden the scope with its use of policymaker and how it intends this provision to be applied in banks above $10 billion in assets.

 © 2023 Davis Polk & Wardwell LLP

Davis Polk

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
Select and Appoint Qualified Executive Officers			
The board must select and appoint executive officers who are qualified to administer the FDIC Covered Institution's affairs effectively and soundly. The selection criteria should include integrity, technical competence, character, and experience in financial services. (See Proposed FDIC Guidelines for additional requirements.)	An OCC Covered Institution should establish and adhere to processes for talent development, recruitment, and succession planning to ensure that management and employees who are responsible for or influence material risk decisions have the knowledge, skills, and abilities to effectively identify, measure, monitor, and control relevant risks. The board of directors or an appropriate committee of the board should: Appoint a CEO and appoint or approve the appointment of a Chief Audit Executive and one or more Chief Risk Executives with the skills and abilities to carry out their roles and responsibilities within the risk governance framework. . . . (See OCC Guidelines for additional requirements.)	**Factor #3. Oversee and Hold Senior Management Accountable**. An effective board should: – Oversee and regularly evaluate the performance and compensation of senior management, . . . – Oversee succession plans for the CEO and, depending on the size, complexity and nature of the firm, the Chief Risk Officer (**CRO**) and Chief Audit Executive (**CAE**) or other senior management officials.	The Proposed FDIC Guidelines imply the board must appoint all executive officers, which is broader than the OCC Guidelines and probably broader than the FRB Guidance. The Proposed FDIC Guidelines specify that selection criteria for executive officers should include "integrity, technical competence, character, and experience in financial services," which is not found in either the FRB Guidance or OCC Guidelines. All of these attributes make good sense but query whether they need to be that prescriptive. For example, can a board be criticized or subject to a remediation plan if, later on, it turns out that the person was not as competent or ethical as thought during the interview stage? It might be wiser to think of these in terms of patterns of hiring or move to the other agencies' more principles-based approaches.

 © 2023 Davis Polk & Wardwell LLP

Davis Polk

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
Director Training			
The board should establish and adhere to a formal, ongoing training program for directors to ensure each member of the board has the knowledge, skills, and abilities needed to stay abreast of general industry trends and any statutory and regulatory developments pertinent to their institution and to meet the standards set forth in these Proposed FDIC Guidelines. (See Proposed FDIC Guidelines for a list of topics to be covered in director training.)	The board should establish and adhere to a formal, ongoing training program for all directors that considers the knowledge and experience of directors and the bank's risk profile. (See OCC Guidelines for a list of topics to be covered in director training.)	**Factor #2. Direct Senior Management Regarding the Board's Information Needs**. Director training is another way directors may learn more about topics relevant to their responsibilities and may highlight the need for further director inquiries.	Most boards already have extensive director training. The use of the word "should" mitigates enforceability risk.
Self-assessments			
The board should conduct an annual self-assessment evaluating its effectiveness in meeting the standards of these guidelines.	An OCC Covered Institution's board of directors should conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting the OCC's risk governance guidelines.	An effective board evaluates on an ongoing basis its strengths and weaknesses, including the performance of the board committees, particularly the risk, audit, and other key committees. An effective board adapts its structure and practices to address identified weaknesses or deficiencies and as the firm's asset size, scope of operations, risk profile, and other characteristics change over time.	Most boards already engage in self-assessments as a general matter, looking at their composition, skill sets and how they work together. The OCC, but not the FRB, also requires that the board assess how it is meeting the governance guidelines. The FDIC's highly detailed and more prescriptive guidelines will make this exercise challenging. This type of exercise could undermine the spirit of qualitative and dynamic self-assessments, whose focus may change from year to year depending on a board's priorities and focus.

 © 2023 Davis Polk & Wardwell LLP

<table>
<tr><th>Proposed FDIC Guidelines</th><th>OCC Guidelines</th><th>FRB Guidance</th><th>Commentary</th></tr>
<tr><td colspan="4">Compensation and Performance Management Programs</td></tr>
<tr><td>The board should establish, and the FDIC Covered Institution should adhere to, compensation and performance management programs, which are reviewed and updated at least annually to:
– Ensure the CEO, front line, independent risk management and internal audit units implement and adhere to an effective risk management program;
– Ensure front line compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by independent risk management and internal audit; and
– Attract and retain competent staff needed to design, implement and maintain an effective risk management program.</td><td>The OCC Guidelines provide a similar list of requirements as the Proposed FDIC Guidelines for compensation and performance management programs, but the former provide that they must be established by the OCC Covered Institution rather than its board.</td><td>Factor #3. Oversee and Hold Senior Management Accountable. An effective board approves clear financial and nonfinancial performance objectives that are aligned with the firm's strategy and risk tolerance for the CEO, CRO and CAE and other members of senior management as appropriate. The board should also hold senior management accountable for the implementation of performance management and compensation programs that promote sound risk management and compliance with laws, regulations and internal standards.</td><td>Most boards oversee risk management, including with respect to compensation programs and performance management, but the FDIC (like the OCC) is requiring that the board "ensure" this. The FDIC also suggests that these programs not only be annually reviewed but also "updated."</td></tr>
<tr><td colspan="4">Committees of the Board</td></tr>
<tr><td>The board should implement an organizational structure to keep members informed and provide an adequate framework to oversee the FDIC Covered Institution, and should have these committees, as applicable:
1. Audit Committee;
2. Compensation Committee;</td><td>The OCC Guidelines refer only to risk and audit committees.</td><td>Risk and audit committees should assess and support the independence and stature of the independent risk management and internal audit functions.</td><td>The Dodd–Frank Act, as amended by EGRCCPA, requires that a BHC of $50 billion or more establish a risk committee. For banks below $10 billion, the risk and audit committees are often combined; for banks between $10–$50 billion the seem to split the risk and audit</td></tr>
</table>

 © 2023 Davis Polk & Wardwell LLP

Davis Polk

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
3. Trust Committee—if the FDIC Covered Institution has trust powers; 4. Risk Committee; and 5. Other Committees as required to perform duties, such as compliance, lending, information technology, cybersecurity, and investments.			committees. There is otherwise not much net new in this requirement, especially because, until 2018, a separate risk committee requirement applied under Dodd–Frank to BHCs at the $10 billion level.
Board and Management Responsibilities Regarding Risk Management and Audit			
Independent Risk Management			
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. (See Proposed FDIC Guidelines for additional details on Risk Management Program.)	An OCC Covered Institution should establish and adhere to a formal, written risk governance framework that is designed by independent risk management and approved by the board of directors or the board's risk committee.	An effective board of directors, through its risk and audit committees, assesses and supports the stature and independence of the firm's independent risk management and internal audit functions.	
Three Lines of Defense			
Three distinct units should have responsibility and be held accountable by the CEO and the board for monitoring and reporting on the covered institution's compliance with the risk management program: front line units, the independent risk management unit, and the internal audit unit.	Stipulates that an effective risk governance framework should include three lines of defense, each with separate roles and responsibilities: front line units, the independent risk management unit, and the internal audit unit.	The FRB does not mandate the implementation of the three lines of defense.	Virtually all banking organizations have, since the financial crisis, adopted a three lines of defense model. It is noteworthy that, until the Proposed FDIC Guidelines, the only official place it occurs in the U.S. banking regulatory framework is the OCC Guidelines. It is not in the FRB Guidance. The FDIC has placed requirements on

 © 2023 Davis Polk & Wardwell LLP

Davis Polk

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
			the CEO in the board guidelines.
Risk Profile and Appetite Statement			
The board should review and approve the FDIC Covered Institution's risk appetite statement at least quarterly, or more frequently, as necessary, based on the size and volatility of risks and any material changes in the firm's business model, strategy, risk profile, or market conditions. (See Proposed FDIC Guidelines for specific content of risk statement and its use by management.)	An OCC Covered Institution should have a comprehensive written statement that articulates the OCC Covered Institution's risk appetite and serves as the basis for the risk governance framework. (See OCC Guidelines for specific content of risk statement and its use by management.) The OCC Covered Institution's board of directors or risk committee should review and approve the risk appetite statement at least annually or more frequently, as necessary, based on the size and volatility of risks and any material changes in the OCC Covered Institution's business model, strategy, risk profile, or market conditions.	An effective board oversees the development of, reviews, approves, and periodically monitors the firm's strategy and risk appetite. An effective board should set a clear, aligned, and consistent direction regarding the firm's strategy and risk appetite.	The Proposed FDIC Guidelines require quarterly review of risk appetite statement by the board; the OCC Guidelines require review only annually.
Risk Management Program Standards - Governance			
The independent risk management unit should design a formal, written risk management program that implements the FDIC Covered Institution's risk appetite statement and ensures compliance with applicable laws and regulations. The unit should review the risk management program at least annually, and as often as necessary, to address changes in the FDIC Covered Institution's risk profile caused by	An OCC Covered Institution should establish and adhere to a formal, written risk governance framework that is designed by independent risk management and approved by the board of directors or the board's risk committee.	An effective board oversees the development of, reviews, approves, and periodically monitors the firm's strategy and risk appetite. *Board of directors are responsible for understanding the nature of the risks significant to their organization and overseeing and holding senior management accountable for maintaining an effective risk management framework. (Supervisory Letter*	

 © 2023 Davis Polk & Wardwell LLP

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
internal or external factors or the evolution of industry risk management practices. The board or the risk committee should review and approve the risk management program and any changes to the program.		*SR 95-51, applicable to state member banks and BHCs with $100 billion or more in total assets.)*	
Risk Management Program Standards – Scope of risk management program			
The risk management program, at a minimum, should cover the following risk categories as applicable: credit, concentration, interest rate, liquidity, price, model, operational (including, but not limited to, conduct, information technology, cyber-security, AML/CFT compliance, and the use of third parties to perform or provide services or materials for the institution), strategic, and legal risk. (See Proposed FDIC Guidelines for additional details on what the risk management program should include.)	The risk governance framework should cover the following risk categories that apply to the OCC Covered Institution: Credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk, and reputation risk. (See OCC Guidelines for other components included in risk governance framework.)	Relies on general statement above.	The Proposed FDIC Guidelines are more prescriptive.
Risk Management Standards – Responsibilities			
Three distinct units should have responsibility and be held accountable by the CEO and the board for monitoring and reporting on the FDIC Covered Institution's compliance with the risk management program: front line units, the independent risk management unit, and the internal audit unit.	The risk governance framework should include well-defined risk management roles and responsibilities for front line units, independent risk management, and internal audit.	The FRB does not mandate the three lines of defense but elsewhere requires an analysis of risks that is similar. *Although the FRB has not finalized its proposed supervisory guidance, Core Principles of Effective Senior Management, Management of Business Lines, and Independent Risk Management (IRM) and Controls, its proposal in 2018 stated that it*	

 © 2023 Davis Polk & Wardwell LLP

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
		intended to consolidate and clarify its existing supervisory expectations regarding risk management; the FRB in doing so delineated the roles and responsibilities of business lines, independent risk management, and internal audit, which make up the three lines of defense.	
Front Line Units			
Front line units should appropriately assess and effectively manage all of the risks associated with their activities to ensure that front line units do not create excessive risks and, when aggregated across front line units, these risks do not exceed the limits established in the FDIC Covered Institution's risk appetite statement. In fulfilling this responsibility, each front line unit should: – Establish and adhere to a set of written policies that include front line unit risk limits as approved by the board. – Monitor compliance with their respective risk limits and report at least quarterly to the independent risk management unit. – Develop, attract, train, retain, and maintain competent staff at levels required to carry out the unit's role and responsibilities effectively.	Front line units should take responsibility and be held accountable by the CEO and the board of directors for appropriately assessing and effectively managing all of the risks associated with their activities. In fulfilling this responsibility, each front line unit should: – Establish and adhere to a set of written policies that include front line unit risk limits . . . – Establish and adhere to procedures and processes, as necessary, to maintain compliance with the policies . . . – Adhere to all applicable policies, procedures, and processes established by independent risk management. – Develop, attract, and retain talent and maintain staffing levels required to carry out the unit's role and responsibilities effectively.	*Although the FRB has not finalized its proposed supervisory guidance, Core Principles of Effective Senior Management, Management of Business Lines, and Independent Risk Management (IRM) and Controls, its proposal in 2018 stated the following:* – *Business line management should identify, measure, and manage current and emerging risks that stem from the business line's activities and changes to external conditions.* – *Business line management should incorporate appropriate feedback from IRM on business line risk positions, implementation of the risk tolerance, and risk management practices, including risk mitigation.* – *Business line management should subject any exceptions to risk limits to the firm's formal approval process.*	The Proposed FDIC Guidelines are more prescriptive.

© 2023 Davis Polk & Wardwell LLP

Davis Polk

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
– At least annually, each front line should review and update, as necessary, the written policies that include risk limits. (See Proposed FDIC Guidelines for additional tasks consistent with the OCC Guidelines.)	(See OCC Guidelines for additional tasks consistent with the Proposed FDIC Guidelines.)	– *Business line management should provide a business line with sufficient resources and infrastructure, including personnel with appropriate training and expertise, to meet strategic objectives while maintaining financial and operational strength and resilience over a range of operating conditions.* – *Business line management should establish policies and guidelines that specify accountability, set forth clear lines of management authority within the business line, and clearly align desired behavior with the firm's performance management incentives.*	
Independent Risk Management			
Under the direction of the CRO, the independent risk management staff should oversee the FDIC Covered Institution's risk-taking activities and assess risks and issues independent of the CEO and front line units. (See Proposed FDIC Guidelines for list of requirements for independent risk management that are consistent with the OCC's list, with several changes, including quarterly or annual reporting.)	Independent risk management should oversee the OCC Covered Institution's risk-taking activities and assess risks and issues independent of front line units. (See OCC Guidelines for a list of requirements for independent risk management similar to the list in the Proposed FDIC Guidelines.)	*Independent risk management should effectively evaluate whether the firm's risk appetite appropriately captures material risks and is consistent with the firm's risk management capacity; establishes and monitors risk limits that are consistent with the firm's risk appetite; identifies and measures the firm's risks; and aggregates, assesses and reports on the firm's risk profile and positions. (Supervisory Letter SR 19-3)*	Although very similar to the OCC Guidelines, the Proposed FDIC Guidelines are more prescriptive about the frequency of reporting and reporting of instances of noncompliance with laws or regulations.

 © 2023 Davis Polk & Wardwell LLP

Davis Polk

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
Internal Audit Unit			
In addition to meeting the standards for and fulfilling its obligations of internal audit otherwise required, the internal audit unit should ensure that the FDIC Covered Institution's risk management program complies with these Guidelines and is appropriate for the size, complexity, and risk profile of the FDIC Covered Institution. (See Proposed FDIC Guidelines for list of responsibilities for internal audit that largely align to the OCC requirements, with some changes denoted in red.) In carrying out its responsibilities the internal audit unit should: – Establish and adhere to an audit plan, updated quarterly or more often, as necessary, that takes into account the FDIC Covered Institution's risk profile and emerging risks and issues. . . . Changes to the audit plan should be communicated to the audit committee as they occur. – Report in writing, conclusions, issues, recommendations, and management's response from audit work carried out under the audit plan. The internal audit unit's reports to the audit committee should identify the root cause of any	In addition to meeting the standards set forth in the OCC's existing safety and soundness regulations, internal audit should ensure that the OCC Covered Institution's risk governance framework complies with the OCC Guidelines and is appropriate for the size, complexity, and risk profile of the OCC Covered Institution. (See OCC Guidelines for list of responsibilities for internal audit.) In carrying out its responsibilities, internal audit should: – Establish and adhere to an audit plan that is periodically reviewed and updated that takes into account the OCC Covered Institution's risk profile, emerging risks, and issues, and establishes the frequency with which activities should be audited. . . . Significant changes to the audit plan should be communicated to the board's audit committee. – Report in writing, conclusions and material issues and recommendations from audit work carried out under the audit plan to the board's audit committee. Internal audit's reports to the audit committee should also identify the root cause of any material issues and include: . . .	*Internal audit should have an understanding of the institution's strategy and operating processes as well as the potential impact of current market and macroeconomic conditions on the financial institution. Internal audit's risk-assessment methodology is an integral part of the evaluation of overall policies, procedures, and controls at the institution and the development of a plan to test those processes.* *In carrying out its responsibilities, internal audit should:* – *Ensure that it has a well-developed risk-assessment methodology that drives its risk-assessment process.* – *Have effective processes to identify all auditable entities within the audit universe.* – *A risk assessment should document the internal audit staff's understanding of the institution's significant business activities and the associated risks.* – *Develop and periodically revise its comprehensive audit plan and ensure that audit coverage for all identified, auditable entities within the audit universe is appropriate for the size and complexity of the institution' s activities.*	Although very similar to the OCC Guidelines, the Proposed FDIC Guidelines increase the frequency and breadth of reporting.

 © 2023 Davis Polk & Wardwell LLP

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
investigated issue and include: . . . – Establish and adhere to processes for independently assessing, at least annually, the design and effectiveness of the risk management program. The internal audit unit, an external party, or the internal audit unit in conjunction with an external party may conduct the assessment. . . . – Identify and communicate to the audit committee significant instances where front line units or independent risk management are not adhering to the risk management program. This communication should document instances of identified or suspected non-compliance with applicable laws or regulations.	– Establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework on at least an annual basis. . . . – Identify and communicate to the board's audit committee significant instances where front line units or independent risk management are not adhering to the risk governance framework.	– *Utilize formal continuous monitoring practices as part of the function's risk-assessment processes to support adjustments to the audit plan or universe as they occur.* *(Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing)*	
Communication Processes			
The risk management program should require that the FDIC Covered Institution initially communicate and provide ongoing communication and reinforcement of the FDIC Covered Institution's risk appetite statement and risk management program throughout the institution in a manner that ensures management and all employees align their risk-taking decisions	Risk governance framework should require the initial communication and ongoing reinforcement of the OCC Covered Institution's risk appetite statement throughout the institution in a manner that causes all employees to align their risk-taking decisions with applicable aspects of the risk appetite statement.	None, although communication is expected as a supervisory matter.	

 © 2023 Davis Polk & Wardwell LLP

Davis Polk

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
with applicable aspects of the risk appetite statement.			
Processes Governing Risk Limit Breaches			
The board should establish, and the FDIC Covered Institution should adhere to, processes that require front line units and the independent risk management unit to: – Inform front line unit management, the CRO, the risk committee, the audit committee, the CEO, and the FDIC in writing of a breach of a risk limit or noncompliance with the risk appetite statement or risk management program describing the severity of the breach, its impact on the FDIC Covered Institution, and how the breach will be, or has been, resolved. – Establish accountability for reporting and resolving breaches that include consequences for risk limit breaches that take into account the magnitude, frequency, and recurrence of breaches, even if the FDIC Covered Institution did not realize a loss from such breaches. At least annually, the board should review and update, as necessary, the processes related to risk limit breaches.	An OCC Covered Institution should establish (and should adhere to) processes that require front line units and independent risk management to: – Establish protocols for when and how to inform the board of directors, front line unit management, independent risk management, internal audit, and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the OCC Covered Institution. – Establish accountability for reporting and resolving breaches that include consequences for risk limit breaches that take into account the magnitude, frequency, and recurrence of breaches. (See OCC Guidelines for tasks related to risk appetite.)	An effective risk committee and an effective audit committee engage in robust inquiry into the causes and consequences of material or persistent breaches of the firm's risk appetite and risk limits. *Although the FRB has not finalized its proposed supervisory guidance, Core Principles of Effective Senior Management, Management of Business Lines, and Independent Risk Management (IRM) and Controls, its proposal in 2018 contained the following:* *Senior management is responsible for ensuring resolution of risk management issues (including those identified by the firm and outstanding supervisory matters), escalating issues to the board, and communicating issues when appropriate. Senior management should regularly report to the board on responses to, and remediation of, material audit and supervisory findings, risk management and control deficiencies, material compliance issues (including those related to consumer protection), and the outcomes of risk reviews which may result in remedial action.*	The FDIC seems to want the board to be involved in every risk limit breach, not just material, significant or persistent breaches. There may be a balance to be struck here, especially given that the risk limit breaches can be driven by market events and may be different depending upon size and complexity.

 © 2023 Davis Polk & Wardwell LLP

Davis Polk

Proposed FDIC Guidelines	OCC Guidelines	FRB Guidance	Commentary
(See Proposed FDIC Guidelines for tasks related to risk appetite, including some with key differences from OCC text.)			
Processes Governing Identification of and Response to Violations of Law and Regulations			
The board should establish, and the FDIC Covered Institution should adhere to, processes that require front line units and the independent risk management unit to: 1. Identify known or suspected violations of law or regulations applicable to the activities conducted by their units. . . . 2. Ensure that known or suspected violations of law involving dishonesty, misrepresentation or willful disregard for requirements . . . are promptly reported as required by law or regulation and to relevant law enforcement and federal and state agencies, and take prompt action to cease such activity and prevent its recurrence. (See Proposed FDIC Guidelines for list of additional requirements.) At least annually, the board should review and update, as necessary, the processes related to identification of and response to violations of law or regulations.	Identification and reporting of violations of law or regulations are an implicit part of safe and sound banking practices. *The board is responsible for complying with applicable laws, regulations, and for understanding the legal and regulatory framework applicable to the bank's activities. (Corporate and Risk Governance, Comptroller's Handbook)*	Identification and reporting of violations of law or regulations are an implicit part of safe and sound banking practices.	The Proposed FDIC Guidelines list specific requirements for processes related to identifying violations of law or regulations to be "established" by the board. The identification and reporting of violations of law or regulations are an implicit part of safe and sound banking practices that are captured in a myriad of business-as-usual processes, so it is unclear what the FDIC is trying to draw out in this requirement. Generally much more prescriptive than the FRB Guidance and OCC Guidelines.

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.