Deloitte.

# FDIC focuses on bank boards for governance and risk enhancements

Center *for* Regulatory Strategy US

**October 2023**

# FDIC draws a line in the sand

With a new proposal on standards for corporate governance and risk management (Proposed Rule), the Federal Deposit Insurance Corporation (FDIC) would require boards of directors of its **supervised banks with at least $10 billion** in consolidated assets to comply with corporate governance requirements that aim to enhance the oversight of risk management, ensure management accountability for an effective governance and risk management program, and support the overall safety and soundness of the organization. The Proposed Rule is part of actions the FDIC has taken after a string of large bank failures earlier this spring.[1]

**This Proposed Rule is further evidence that regulatory tailoring for banks based on their size, risk, and complexity is being rolled back in response to recent market events.** As new rulemaking is issued, the regulation applicable to banks based on their size, risk, and complexity continues to narrow. The impact is that regulations and requirements that were once applicable only to large, complex institutions are now flowing downhill to affect midsize banks.

Passed in May 2018, the Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA) provided tailored relief to banks of all sizes, banks between $10 billion and $50 billion were exempted from Dodd-Frank Act stress testing and the requirement to have a risk committee, and banks between $50 billion and $100 billion were exempted from some aspects of Dodd-Frank enhanced prudential standards.[2] Recent interagency proposals (e.g., Basel III Endgame, resolution planning, and long-term debt requirements) from the FDIC, Federal Reserve Board (FRB), and Office of the Comptroller of the Currency (OCC) have nearly removed the tailoring framework set out by EGRRCPA.[3]

The Proposed Rule **contains standards for corporate governance and risk management for covered institutions.**[4] The Proposed Rule states that banks should have:

✓ A risk management program commensurate with the size and complexity of the institution.

✓ A three-lines-of-defense model with an independent risk management function led by a chief risk officer and an internal audit unit led by a chief audit officer.

✓ Boards that establish and oversee written risk profiles and risk appetite statements, among other requirements.

The **core corporate governance and risk management elements of the Proposed Rule are reflective of prior efforts that the FRB and OCC enacted through Enhanced Prudential Standards** (Reg YY) and Heightened Standards, respectively, though the proposed $10 billion threshold the FDIC is looking to establish is lower than the related FRB and OCC guidance (both established with some specifics at $50 billion).[5]

# Key takeaways for boards and senior management

**Regulatory scrutiny is linked to regulation, but regulatory expectations remain implicit and vague:** Although the Proposed Rule is now explicitly grounded in regulation, much of the regulatory scrutiny and assessment will reside in the realm of implicit expectations.[6] Significant work will remain in translating requirements into expected capabilities at the board and management level across corporate governance and risk practices.

**Governance as a 'system':** Demonstrating a robust board and corporate governance system that encompasses a set of capabilities and processes for effective risk oversight of an organization through authorities, committee charters, membership structures, and agendas to enable identification, assessment, monitoring, and response to a range of governance matters will be key not only for complying with the Proposed Rule, but also for maintaining trust and confidence among stakeholders, including regulators. Please refer to page 7 for further details on governance.

**Board reporting will be a critical focus:** The quality of board reporting is the linchpin of an effective governance system within a bank. It serves as the vital channel through which the board can stay informed about and make decisions regarding the institution's performance, risk exposure, and compliance status. Significant focus will be on the quality and nature of what is reported, and whether the board and management are focused on the right information.

**Latitude with enforcement:** Boards should recognize the significant latitude that the FDIC will have when these guidelines are treated as law and enforced. While the Proposed Rule will apply to specific institutions, it is crucial to recognize that the FDIC possesses the flexibility to adapt and enforce these guidelines based on an institution's unique complexities and risk profiles, regardless of total asset size.

**Guidelines allow for flexibility:** The FDIC's approach is narrower than the FRB's and OCC's, concentrating on the board's overarching accountability and oversight without delving into the intricacies of day-to-day management and independent risk management as extensively as Reg YY or Heightened Standards. This distinction suggests that while the FDIC's guidelines provide a strong governance framework, they may allow for a degree of flexibility in how institutions meet these responsibilities, recognizing the unique nature of each bank's risk profile and operations. We compare FRB Enhanced Prudential Standards (Reg YY), OCC Heightened Standards, and the FDIC Proposed Rule on the pages that follow

# Summary of risk management and corporate governance requirements

The table below summarizes at a high level the board requirements and risk management activities described in Enhanced Prudential Standards (Reg YY), Heightened Standards, and the Proposed Rule. Depending on the legal entity structure, size, and whether the bank is a domestic bank or foreign banking organization (FBO), additional requirements may apply.

| | FRB Enhanced Prudential Standards (Reg YY) | OCC Heightened Standards | FDIC Proposed Rule |
|---|---|---|---|
| **Board committees** | **Risk committee:** Domestic banks and foreign banking organizations7 are required to have a risk committee that approves and periodically reviews the risk-management policies of the bank and oversees the operation of its risk management framework. Depending on the legal entity structure, size, and whether the bank is a domestic bank or FBO, additional requirements may apply. | **Risk committee:** While not explicitly required, the board or the board's risk committee reviews and approves the risk governance framework. | **Risk committee:** The bank board is required to have a risk committee that meets quarterly and that approves and at least annually reviews the bank's risk management framework.<br><br>**Other committees:** The board is required to establish an audit committee (composed entirely of outside and independent directors), a compensation committee, and a trust committee (if applicable). The board is expected to establish other committees, as needed, to support the risks and operations of the institution (e.g., credit committee, cyber committee). |
| **Independent board members** | The risk committee must (1) include at least one member having experience in identifying, assessing, and managing risk exposures of large, complex financial firms, and (2) be chaired by an independent director. | Boards of banks should include at least two independent members that do not hold management positions in the bank or its parent holding company. | The majority (at least) of the board should be made up of independent directors. The audit committee must be composed entirely of outside counsel and independent directors, while the risk committee must have an independent director as the chair. |
| **Independent risk and audit executives** | Must appoint a chief risk officer (CRO) with experience in identifying, assessing, and managing risk exposures of large, complex financial firms. The CRO reports to both the risk committee and the chief executive officer (CEO). | Expected to have a CRO and a chief audit executive (CAE) to assess and monitor risk activities and have independent escalation channels to the board. | The independent risk management function is to be led by a CRO, and the internal audit unit is to be led by a CAE. |
| **Strategic planning** | The board has responsibility for the strategic direction of the banking organization. | The CEO has responsibility for the development of a written strategic plan with input from the three lines of defense. At a minimum, the plan should cover a 3-year period and be evaluated and approved by the board at least annually. | The board is responsible for strategic planning. The plan should be developed by the CEO with input from the three lines of defense and should then be reviewed and approved by the board. At a minimum, the plan should cover a 3-year period and be reviewed and approved annually. |

# Summary of risk management and corporate governance requirements (cont'd)

| | FRB Enhanced Prudential Standards (Reg YY) | OCC Heightened Standards | FDIC Proposed Rule |
|---|---|---|---|
| **Risk governance/ management framework** | A bank's global risk-management framework must be commensurate with its structure, risk profile, complexity, activities, and size. | Banks need to establish a formal risk governance framework approved by the board and updated at least annually. | Banks need to have and maintain a risk management program and are required to establish a three-lines-of-defense model business unit (frontline units), independent risk management unit, and internal audit unit. |
| **Risk appetite** | While Reg YY does not explicitly mention risk appetite, the bank is required to develop a risk management framework that has processes and systems for establishing managerial and employee responsibility for risk management. | Written statement that articulates the bank's risk appetite and is approved by the board at least annually. The risk appetite statement should include qualitative components that describe risk culture and quantitative limits that incorporate sound stress-testing processes for all material risk types. | The bank's risk management program should include a risk profile and risk appetite statement. The board should establish written limits and levels of risks that the institution is willing to accept, based on the foundational documents mentioned above. The board should review and approve the risk appetite statement at least quarterly, or more frequently, as necessary. |
| **Concentration risk management** | The CRO is responsible for overseeing the establishment of risk limits on an enterprise-wide basis and the monitoring of compliance with such limits. | The risk governance framework should include concentration risk limits. Banks should continually enhance their concentration risk management processes to strengthen their ability to effectively identify, measure, monitor, and control concentrations that arise in all risk categories. | This risk management program should identify, measure, monitor, and manage key risks, including concentration risk. Concentration risk limits should be incorporated into key operations and risk activities, such as strategic and annual operating plans, capital stress testing, and liquidity stress testing. |
| **Risk-based compensation** | The bank must ensure that the compensation and other incentives provided to the CRO are consistent with the CRO's objective assessment of the risks taken by the bank. | Compensation structure should be aligned with the risk-reward expected to be in place. Deviations from established policy will raise concerns, e.g., the owner of a major problem receives no consequence for the failure. | The bank's compensation and performance management programs should not incentivize imprudent risk-taking, and the proposed guidance suggests that |

# Coverage of additional Reg YY and Heightened Standards expectations against the FDIC Proposed Rule

The table below summarizes the applicability and coverage of key components of FRB Enhanced Prudential Standards (Reg YY) and OCC Heightened Standards regulations against the FDIC Proposed Rule for banks $10 billion and larger.

| | FRB Enhanced Prudential Standards (Reg YY) | OCC Heightened Standards | FDIC Proposed Rule |
|---|---|---|---|
| **Applicability -Size** | $100 billion[7] | $50 billion[8] | $10 billion[9] |
| **Applicability - Type** | Domestic bank holding companies (BHCs) and noninsurance, noncommercial savings and loan holding companies (SLHCs), FBOs, or any international holding company (IHC) of an FBO. | Insured national banks, insured federal savings associations, and insured federal branches of FBOs. | Insured state nonmember banks, state-licensed insured branches of FBOs, and insured state savings associations. |
| **Board and risk management requirements** | | | |
| **Corporate Governance** | Covered | Covered | Covered |
| **Risk management** | Covered | Covered | Covered |
| **Capital requirements** | | | |
| **Long-term debt** | Covered and proposal recently issued[10] | N/A | N/A |
| **Stress testing** | Covered | N/A | N/A |
| **Risk-based capital** | Covered and proposal recently issued[11] | N/A | N/A |
| **Leveraged capital** | Covered and proposal recently issued[12] | N/A | N/A |
| **Liquidity requirements** | | | |
| **Internal liquidity** | Covered | N/A | N/A |
| **Standardized liquidity** | Covered | N/A | N/A |
| **Other requirements** | | | |
| **Single-counterparty credit limit (SCCL)** | Covered | N/A | N/A |

# Roles and responsibilities of the board

The FDIC's proposed duties for the Board[13] of covered institutions focus on accountability for providing oversight of the overall risk management of the organization and the three lines of defense. It also includes minimum expectations to formalize and clarify existing guidance, and to align with related expectations outlined by the FRB and OCC.[14] Organizations may be adhering to these duties already, based on related or informal regulatory expectations and alignment to industry practices:

- Set an appropriate tone
- Approve strategic plan
- Approve policies
- Establish a Code of Ethics
- Provide active oversight of management
- Exercise independent judgment
- Select and appoint qualified officers
- Provide ongoing training to directors
- Conduct annual self-assessments
- Establish compensation and performance management programs

# The system of governance

Simply put, we view governance as a "system" composed of four layers:

1. **Board of directors** through the structure and hierarchy, committees, mandates, compositions, agendas, reporting, escalation
2. **Management** through organizational structure, roles, responsibilities, accountabilities, three lines of defense
3. **Framework and infratructure** that management has put in place to govern the day-to-day activities of the organization
4. **Governance enablers** that support effective governance and drive strong risk and compliance culture across the organization

**BOARD GOVERNANCE & OVERSIGHT**

| Board of Directors | Board Committees | Parent/Subsidiary/Legal Entity Boards as applicable |
|---|---|---|

**CORPORATE GOVERNANCE & OVERSIGHT**

Management Committees

| CEO | Executive Manager | Business & Function Heads | Independent Risk & Compliance | Internal Audit |
|---|---|---|---|---|

Three lines of Defense Model

**FRAMEWORK & INFRASTRUCTURE**

| | | | | |
|---|---|---|---|---|
| Strategy & Innovation | Financial Plan & Performance | Risk Appetite & Risk Management | Capital Management | Technology & Resiliency |
| Internal Controls | Compliance | Internal Audit | Policy Management | Issue & Escalation |

**GOVERNANCE ENABLERS**

| Data | Metrics & MIS Reporting | Authority, Accountability & Reporting Lines | Culture & Ethics | Performance & Compensation | Talent & Training | Change & Communication |
|---|---|---|---|---|---|---|

**Legend:** Role of the Board | Role of Management

# Next steps for impacted organizations

In conclusion, this Proposed Rule represents a **significant 'line in the sand' from the FDIC that covered institutions at, near, or above the $10 billion threshold will be subject to additional governance and risk management requirements** that are similar to regulatory requirements of larger, riskier, and/or more complex organizations. Tailoring is no longer the theme, and covered institutions **need to take action to be prepared for the increased regulatory requirements.**

In our view, it is paramount that organizations "take the high ground" and demonstrate how they comply with this regulation (including a detailed control to regulation mapping).

- **Are you ready?** Conduct a readiness assessment of the bank's governance and risk management frameworks to the Proposed Rule to identify enhancement areas and define a plan of action.
- **Is the three lines of defense (3LOD) model working?** Assess the effectiveness of the 3LOD model, including clarity of roles, responsibilities, and accountabilities across businesses and functions; independent risk management; and internal audit.
- **Is risk appetite clearly defined and understood?** Evaluate the bank's risk profile, risk appetite, and limit framework, including alignment to strategy and impact of market conditions.
- **Is data and reporting accurate and timely?** Review the quality of data and management information system (MIS) to produce accurate and timely risk reports that aid in decision-making by both the board and management.
- **Does a strong risk culture exist?** Consider how the risk and compliance culture is demonstrated and reinforced, including issue management, conduct and/or consequence management, and performance management and incentive compensation.
- How do governance and risk management policies, frameworks, and processes **align between legal entity, businesses, and the consolidated holding company** (which could align across FRB, OCC, or FDIC regulated entities)?

As the Proposed Rule evolves throughout the notice and comment period, institutions should diligently prepare for the **anticipated compliance efforts, ensuring their boards are well-informed and well-equipped to effectively challenge senior management.** As demonstrated through the "tone at the top" references, organizations should focus on not only establishing the required capabilities and documentation, but also **embedding the intent** behind this Proposed Rule into the day-to-day operations, risk management, and overall culture. This proactive approach is about not only compliance but a fundamental transformation in corporate governance and risk management practices, enabling institutions to thrive in an ever-changing environment.

# Contacts

**Richard Rosenthal**
Principal | Deloitte & Touche LLP
rirosenthal@deloitte.com

**Michele Crish**
Managing Director | Deloitte & Touche LLP
mcrish@deloitte.com

**Naresh Nagia**
Independent Senior Advisor to Deloitte & Touche LLP
nnagia@deloitte.com

**Alexandra Rankin**
Manager| Deloitte & Touche LLP
alrankin@deloitte.com

## Deloitte Center for Regulatory Strategy

**Irena Gecas-McCarthy**
FSI Director, Deloitte Center for Regulatory Strategy US
Principal | Deloitte & Touche LLP
igecasmccarthy@deloitte.com

**Kyle Cooke**
Manager| Deloitte Services LP
kycooke@deloitte.com

**Vignesh Venkatesan**
Manager | Deloitte & Touch Assurance & Enterprise Risk Services India Private Limited
vigvenkatesan@deloitte.com

# Endnotes


1. Federal Deposit Insurance Corporation (FDIC), "Guidelines Establishing Standards for Corporate 1. Governance and Risk Management for Covered Institutions With Total Consolidated Assets of $10 Billion or More," October 11, 2023.

2. US Congress, "S.2155 - Economic Growth, Regulatory Relief, and Consumer Protection Act," May 24, 2018.

3. Deloitte, "US Basel III Endgame: Key changes, impacts and where to begin," August 2023; Deloitte, "Federal banking agencies propose new resolution planning requirements," September 2023.

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

5. Deloitte, "Federal Reserve Board finalizes tailoring prudential standards for large banking institutions," October 21, 2019; Deloitte, "Federal Reserve Board finalized tailoring prudential standards for foreign banking organizations," October 21, 2019; Office of the Comptroller of the Currency (OCC), "OCC finalizes its heightened standards for large financial institutions," news release, September 2, 2014.

6. Within the NPR, the FDIC cites its history of issuing guidance for IDIs on corporate governance and risk management, and expectations relating to boards of directors, with all guidance and expectations scaled to the size, complexity, and risk profile of the IDI. These examples include the Pocket Guide for Directors, Corporate Codes of Conduct: Guidance on Implementing an Effective Ethics Program, and its regular Supervisory Insights program.

7. Depending on the legal entity structure, size, and whether the bank is a domestic or foreign banking organization (FBO), additional requirements may apply. The risk committee and risk management requirements apply to any US bank holding company or covered savings and loan holding company with more than $50 billion of total consolidated assets; foreign banking organizations with $50 billion or more but less than $100 billion in total consolidated assets; and foreign banking organizations with total consolidated assets of $100 billion or more but less than $50 billion in combined US assets. FBOs with total consolidated assets of $100 billion or more and $50 billion or more in combined US assets are required to comply with the more detailed risk committee and risk management requirements under the enhanced prudential standards rule, which include the chief risk officer (CRO) requirement.

8. OCC reserves the authority to apply the guidelines to a bank whose average total consolidated assets are less than $50 billion if the OCC determines that such bank's operations are highly complex or otherwise present a heightened risk as to require compliance with the guidelines. OCC, "OCC finalizes its heightened standards for large financial institutions."

9. FDIC reserves the authority to apply the guidelines, in whole or in part, to institutions with less than $10 billion in total consolidated assets if they are highly complex or present heightened risk. FDIC, "Guidelines Establishing Standards for Corporate Governance and Risk Management for Covered Institutions With Total Consolidated Assets of $10 Billion or More."

10. Deloitte, "Federal banking agencies propose new long-term debt requirement," September 2023.

11. Deloitte, "US Basel III Endgame: key changes, impacts and where to begin."

12. Ibid.

13. FDIC, "Guidelines Establishing Standards for Corporate Governance and Risk Management for Covered Institutions With Total Consolidated Assets of $10 Billion or More."

14. Board of Governors of the Federal Reserve System (FRB), "SR 21-3 / CA 21-1: Supervisory Guidance on Board of Directors' Effectiveness," February 26, 2021; OCC, "OCC finalizes its heightened standards for large financial institutions."

Center *for*
**Regulatory Strategy**
**US**

**About the Center**
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services industry keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends. Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media, including thought leadership, research, forums, webcasts, and events.



Deloitte.