FED

12 CFR Parts 308 and 364

RIN 3064-AF94

Guidelines Establishing Standards for Corporate Governance and Risk Management for Covered Institutions with Total Consolidated Assets of $10 Billion or More

AGENCY: Federal Deposit Insurance Corporation.

ACTION: Notice of proposed rulemaking and issuance of guidelines.

SUMMARY: The Federal Deposit Insurance Corporation (FDIC) is seeking comment on proposed corporate governance and risk management guidelines (Guidelines) that would apply to all insured state nonmember banks, state-licensed insured branches of foreign banks, and insured state savings associations that are subject to Section 39 of the Federal Deposit Insurance Act (FDI Act), with total consolidated assets of $10 billion or more on or after the effective date of the final Guidelines. These proposed Guidelines would be issued as Appendix C to FDIC's standards for safety and soundness regulations in part 364, pursuant to Section 39 of the FDI Act, and would be enforceable under Section 39. The FDIC also proposes to make corresponding amendments to parts 308 and 364 of its regulations to implement the proposed Guidelines.

DATES: Comments on the proposed Guidelines must be received by [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: The FDIC encourages interested parties to submit written comments. Please include your name, affiliation, address, email address, and telephone number(s) in your comment. You may submit comments to the FDIC, identified by RIN 3064-AF94, by any of the following methods:

Agency Website: https://www.fdic.gov/resources/regulations/federal-register-publications. Follow instructions for submitting comments on the FDIC's website.

Mail: James P. Sheesley, Assistant Executive Secretary, Attention: Comments/Legal OES (RIN 3064-AF94), Federal Deposit Insurance Corporation, 550 17th Street NW, Washington, DC 20429.

Hand Delivered/Courier: Comments may be hand-delivered to the guard station at the rear of the 550 17th Street NW building (located on F Street NW) on business days between 7 a.m. and 5 p.m.

Email: comments@FDIC.gov. Include RIN 3064-AF94 in the subject line of the message.

Public Inspection: Comments received, including any personal information provided, may be posted without change to https://www.fdic.gov/resources/regulations/federal-registerpublications/. Commenters should submit only information that the commenter wishes to make available publicly. The FDIC may review, redact, or refrain from posting all or any portion of any comment that it may deem to be inappropriate for publication, such as irrelevant or obscene material. The FDIC may post only a single representative example of identical or substantially identical comments, and in such cases will generally identify the number of identical or substantially identical comments represented by the posted example. All comments that have been redacted, as well as those that have not been posted, that contain comments on the merits of this notice will be retained in the public comment file and will be considered as required under all applicable laws. All comments may be accessible under the Freedom of Information Act.

FOR FURTHER INFORMATION CONTACT: Division of Risk Management Supervision: Judy E. Gross, Senior Policy Analyst, 202-898-7047, JuGross@FDIC.gov; Legal Division: Jennifer M. Jones, Counsel, 202-898-6768; Catherine Topping, Counsel, 202-898-3975; Nicholas A. Simons, Senior Attorney, 202-898-6785; Kimberly Yeh, Senior Attorney, 202-898-6514.

SUPPLEMENTARY INFORMATION:

I. Policy Objectives

Strong corporate governance is the foundation for an insured depository institution's safe and sound operations. An effective governance framework is necessary for an insured depository institution to remain profitable, competitive, and resilient through changing economic and market conditions. The board of directors serves a critical role in maintaining an insured depository institution's safety and soundness and continued financial and operational resilience.

The FDIC observed during the 2008 financial crisis and more recent bank[1] failures in 2023 that financial institutions with poor corporate governance and risk management practices were more likely to fail.[2] Reports reviewing the recent 2023 bank failures noted that poor corporate governance and risk management practices were contributing factors.[3] Failures of insured depository institutions (IDIs) impose costs on the Deposit Insurance Fund (DIF) and negatively affect a wide variety of stakeholders including the institution's depositors and shareholders, employees, customers (including consumers and businesses that rely on the institution's services and the availability of credit), regulators, and the public as a whole. Insufficient attention and responsiveness to

---

[1] The term "bank" is used to mean the same thing as "insured depository institution" as defined in Section 3 of the FDI Act.

[2] *Lessons Learned and a Framework for Monitoring Emerging Risks and Regulatory Response*, GAO Report to Congress, GAO-15-365, June 2015; FDIC OIG Reports – Bank Failures, https://www.fdicoig.gov/reports-publications/bank-failures; Remarks by Martin J. Gruenberg, Chairman, FDIC to the American Association of Bank Directors, May 12, 2015, https://archive.fdic.gov/view/fdic/1717; *Review of the Federal Reserve's Supervision and Regulation of Silicon Valley Bank,* April 2023, https://www.federalreserve.gov/publications/files/svb-review-20230428.pdf; *FDIC's Supervision of Signature Bank,* April 2023*,* https://www.fdic.gov/news/press-releases/2023/pr23033a.pdf.

[3] The FDIC report on the failure of Signature Bank in 2023 found that the root cause of the failure was poor management without adequate risk management practices and controls. The institution's management did not prioritize good corporate governance practices (*FDIC's Supervision of Signature Bank*, April 28, 2023, p. 2). The Federal Reserve Board's report on the failure of Silicon Valley Bank also identified governance and risk management failures that led to the failure. (*Review of the Federal Reserve's Supervision and Regulation of Silicon Valley Bank,* April 2023, p. 1).

internal controls and governance processes can result in noncompliance with laws and regulations going undetected or unaddressed.

The safety and soundness standards in part 364 currently include guidelines in Appendix A,[4] which contain operational and managerial standards for insured state nonmember banks, state-licensed insured branches of foreign banks, and insured state savings associations (together, "FDIC-supervised institutions").[5] In smaller, noncomplex institutions, risk management processes and internal controls that generally incorporate these standards may be adequate. However, as the recent bank failures show, corporate and risk governance structure and practices should keep pace with the bank's changes in size, business model, risk profile, and complexity. Larger or more complex institutions should have more sophisticated and formal board and management structures and practices to ensure appropriate corporate governance.

In order to strengthen the corporate governance and risk management practices of large institutions, the FDIC is proposing to issue Guidelines as a new Appendix C to part 364 to address corporate governance and risk management practices and board oversight. The proposed Guidelines would apply to all FDIC-supervised institutions with total consolidated assets of $10 billion or more on or after the effective date of the final Guidelines (together "covered institutions" and each, a "covered institution"). The proposed Guidelines would apply in addition to any other requirements established by law or regulation.[6] The FDIC's supervisory experience has shown that institutions with assets greater than $10 billion are larger, more complex and present a higher risk profile.

---

[4] *See* 12 CFR part 364, Appendix A; https://www.fdic.gov/regulations/laws/rules/2000-8630.html#fdic2000appendixatopart364.

[5] The FDIC is the federal banking regulator for such institutions set forth in Section 3(q)(1) of the FDI Act, 12 U.S.C. 1813(q)(1), and has the authority to promulgate safety and soundness regulations for such institutions pursuant to Section 39 of the FDI Act, 12 U.S.C. 1831p-1.

[6] All FDIC-supervised institutions, including covered institutions, may continue to utilize existing guidance in establishing appropriate corporate guidance processes. However, should an inconsistency exist between existing guidance and the proposed Guidelines, the proposed Guidelines will govern the activities of a covered institution since any final guidelines will be codified in Appendix C to part 364.

The proposed Guidelines are intended to raise the FDIC's standards for corporate governance, risk management, and control to help ensure these larger institutions effectively anticipate, evaluate, and mitigate the risks they face.

In developing the proposed Guidelines, the FDIC considered other statutory and regulatory authorities that impose requirements and expectations concerning corporate governance activities and risk management practices. For example, the Office of the Comptroller of the Currency (OCC) has developed heightened expectations to strengthen the corporate governance and risk management practices of large national banks with total consolidated assets of $50 billion or more. Under guidelines the OCC issued pursuant to Section 39 of the FDI Act, it expects larger national banks to establish and implement a risk governance framework for managing and controlling the bank's risk taking.[7] The Board of Governors of the Federal Reserve System (Federal Reserve Board) has incorporated corporate governance and risk management requirements in Regulation YY[8] and various Supervision and Regulation (SR) Letters for bank holding companies with total consolidated assets of $50 billion or more. The Federal Reserve Board has also noted that the risk management processes of a regional IDI, which it generally considers to be a midsize IDI with total consolidated assets between $10 and $100 billion, should typically contain detailed guidelines that set specific prudent limits on the principal types

---

[7] *See* OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations, 79 Fed. Reg. 54518 (Sept. 11, 2014), https://www.federalregister.gov/documents/2014/09/11/2014-21224/occ-guidelines-establishing-heightened-standards-for-certain-large-insured-national-banks-insured; OCC, Comptroller's Handbook - Corporate and Risk Governance, https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk-governance/index-corporate-and-risk-governance.html.

[8] 12 CFR 252.22, subpart C – Risk Committee Requirements for Bank Holding Companies with Total Consolidated Assets of $50 Billion or More and Less Than $100 Billion. The Federal Reserve Board initially set the application of risk committee requirements under Regulation YY, among other requirements, for banks with total consolidated assets of $10 billion or more pursuant to Section 165 of the Dodd-Frank Act of 2010. 79 Fed. Reg. 17239, 17248 (Mar. 27, 2014). This threshold was raised from $10 billion to $50 billion pursuant to changes made under the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018. 84 FR 59032, 59055 (Nov. 1, 2019).

of risks relevant to a regional IDI's consolidated activities.[9]

The proposed Guidelines are drawn from the principles set forth in the authorities noted above and would therefore align the FDIC's supervisory framework more closely with the other Federal banking agencies. Although the proposed Guidelines would apply more broadly to capture FDIC-supervised institutions with total assets of $10 billion or more, the FDIC believes that the proposed scope of application threshold is appropriate, as effective risk management practices should be tailored to the size of the institution and the nature, scope, and risk of its activities. These institutions are typically more complex and present a higher risk profile than community banking organizations with less than $10 billion in total assets.

II. Background

Prior supervisory guidance and guidelines

Over many years, the FDIC has issued 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. For example, in 1988, the FDIC issued the *Pocket Guide for Directors*[10] to provide guidance to community bank directors about long-standing, broad principles on corporate governance and fiduciary responsibilities. In 1992, the FDIC issued a "Statement Concerning the Responsibilities of Bank Directors and Officers."[11] In 2005, the FDIC issued a document, "Corporate Codes of Conduct: *Guidance on Implementing an Effective Ethics*

---

[9] *See* SR 16-11: *Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $100 Billion* (June 8, 2016; revised and reposted February 17, 2021, p. 3). SR letter 95-51, *Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies* (Nov. 14, 1995; revised Feb. 26, 2021) remains applicable to state member banks and bank holding companies with $100 billion or more in total assets. The Federal Reserve Board's Commercial Bank Examination Manual, Community Bank Supervision Process (Nov. 2020) applies the term "community bank" to generally describe a bank with $10 billion or less in total consolidated assets.

[10] https://www.fdic.gov/regulations/resources/director/pocket/.

[11] Financial Institution Letter (FIL--87--92) dated December 3, 1992, https://www.fdic.gov/regulations/laws/rules/5000-3300.html.

Program."[12] Further, in 2018 the FDIC published an issue of *Supervisory Insights* [13] as a resource specifically for community bank directors with an interest in bank governance and bank directors' responsibilities.

The FDIC's safety and soundness standards in part 364 currently include guidelines in Appendix A that contain operational and managerial standards.[14] Appendix A describes the fundamental governance and risk management standards the FDIC expects FDIC-supervised institutions to implement in a manner appropriate to the scope and complexity of their operations. In addition to Appendix A, the FDIC includes corporate governance and risk management expectations relevant to specific areas in topical rules, such as for appraisals[15] and stress testing,[16] and in guidance, such as the Interagency Guidance on Third-Party Relationships: Risk Management.[17]

Examinations for Safety and Soundness

Corporate governance and risk management practices are core considerations in evaluating management at IDIs as part of FDIC's examinations for safety and soundness. Section 4.1 of the FDIC's *Risk Management Manual of Examination Policies*[18] (Manual) reiterates the importance of good management:

> In the complex, competitive, and rapidly changing environment of financial institutions, it is extremely important for all members of bank management to be aware of their responsibilities and to discharge those responsibilities in a manner which will ensure stability and soundness of the institution, so that it may continue to

---

[12] https://www.fdic.gov/news/financial-institution-letters/2005/fil10505.html.
[13] This is an informational resource but is not regulatory guidance: Special Governance Issue; April 2016, revised October 2018, https://www.fdic.gov/regulations/examinations/supervisory/insights/sise16/si-se2016.pdf.
[14] 12 CFR part 364, Appendix A; https://www.fdic.gov/regulations/laws/rules/2000-8630.html#fdic2000appendixatopart364.
[15] 12 CFR part 323.
[16] 12 CFR part 325.
[17] 88 FR 37920 (Jun. 9, 2023).
[18] https://www.fdic.gov/regulations/safety/manual/.

> provide to the community the financial services for which it was created.

Section 4.2 of the Manual discusses the importance of risk assessment and management:

> Risk assessments are conducted in order to identify, measure, and prioritize risks so that attention is placed first on areas of greatest importance. Risk assessments should analyze threats to all significant business lines, the sufficiency of mitigating controls, and any residual risk exposures.

Although the FDIC has not previously issued supervisory guidelines or regulations specifically on corporate governance and risk management for covered institutions, the FDIC expects these larger IDIs to have more detailed and formal guidance frameworks, given their size and complexity. The FDIC has implemented a continuous examination process (CEP) for the largest IDIs that it supervises.[19] IDIs that are supervised under a CEP are not directly tied to an asset size; however, most FDIC-supervised IDIs with assets of $10 billion or more are supervised through a CEP since they are larger, more complex, or present a higher risk profile. The CEP includes onsite targeted reviews of areas the examiner determines are necessary to complete a full-scope examination; ongoing monitoring and assessment of institution risks, policies, procedures, and financial condition; and frequent communication with bank management. A dedicated or designated examiner-in-charge (EIC) oversees the continuous examination process and may be supported by additional dedicated examination staff. IDIs with assets of $10 billion or more are also subject to increased off-site review activities and more granular risk-based deposit insurance pricing due to their increased size and complexity.

The requirements in these proposed Guidelines generally reflect existing

---

[19] *See* Section 1.1 of the Manual.

principles and what examiners consider necessary for the safe and sound operation of a covered institution. In addition, these proposed Guidelines are intended to be generally consistent with the goals communicated through the OCC's and Federal Reserve Board's published issuances in an effort to harmonize corporate governance and risk management requirements for covered institutions that present a higher risk profile with those applicable to entities supervised by the other Federal banking agencies.

Most of the risk management practices to be established and maintained by a covered institution to meet these safety and soundness standards, including having appropriate loan review and credit underwriting and administration practices, are already components of the institution's risk governance framework. As discussed below in Section III, the FDIC is adding a requirement (consistent with the OCC and Federal Reserve Board standards) for covered institutions to establish a three-lines-of-defense model: business units (front line units), independent risk management unit, and internal audit unit.

Rulemaking Authority

The FDIC is issuing the proposed Guidelines pursuant to Section 39[20] of the FDI Act. Section 39 generally prescribes safety and soundness standards for insured depository institutions. Under subsection (a) of the statute, the FDIC, as the appropriate Federal banking agency for insured state nonmember banks, state-licensed insured branches of foreign banks, and insured state savings associations, may prescribe such standards, including other operational and managerial standards, by issuing a regulation or guideline. Pursuant to Section 39, if a covered institution fails to meet a standard prescribed by regulation, the FDIC must require the institution to submit a plan specifying the steps that it will take to comply with the standard. If a covered institution fails to meet a standard prescribed by guideline, the FDIC has the discretion to decide

[20] 12 U.S.C. 1831p-1.

whether to require the submission of a plan.[21] The issuance of these standards as Guidelines rather than as a regulation provides the FDIC with supervisory flexibility to pursue the course of action that is most appropriate given the specific circumstances of a covered institution's failure to meet one or more of the standards, and the covered institution's self-corrective and remedial responses.[22]

III. Description of the Proposed Guidelines

The proposed Guidelines contain standards for corporate governance and risk management for covered institutions. The proposed Guidelines include a description of the general obligations of the board to ensure good corporate governance.[23] The FDIC expects all FDIC-supervised institutions to have good corporate governance, including the key component of an active and involved board protecting the interests of the institution rather than the interests of the parent or affiliate of the institution. The proposed Guidelines for covered institutions emphasize the importance of developing a strategic plan and risk management policies and procedures and selecting and supervising senior management so that a covered institution will operate in a safe and sound manner. The proposed Guidelines also emphasize the importance for the board and management to adopt a code of ethics, to demonstrate high ethical standards in the covered institutions' operations, and to act to ensure the covered institution and its employees

---

[21] Pursuant to Section 39, if the FDIC determines that an IDI fails to meet any standard prescribed in the guidelines issued under subsection (a) or (b) of Section 39, the FDIC may require the IDI to submit a plan that specifies the steps that the institution will take to correct the deficiency (such plan is referred to as a "Section 39 Plan"). Further, Section 39 provides that if an IDI fails to submit an acceptable Section 39 Plan or fails in any material respect to implement an acceptable Section 39 Plan, the FDIC, by order shall require the institution to correct the deficiency and may take additional enumerated actions, including growth restrictions, increased capital requirements, and restrictions on interest rates paid on deposits.

[22] The FDIC's procedural rules implementing Section 39 are contained in 12 CFR part 308, subpart R. As part of this rulemaking, an amendment to 12 CFR 308.302(a) is being proposed to add a reference the proposed Guidelines. Similarly, a new paragraph (c) is being proposed to 12 CFR 364.101 to add a reference to the proposed Guidelines.

[23] Under the proposed Guidelines, the FDIC reserves authority to modify or extend the time for compliance for any IDI with $10 billion or more in assets and to modify the proposed Guidelines, as necessary, to address their applicability to insured branches of foreign banks because those institutions do not have a board.

adhere to applicable laws and regulations, including consumer protection laws and regulations, and the Community Reinvestment Act.

A. Section I – Introduction

This section describes the scope of FDIC-supervised institutions that would be subject to the proposed Guidelines. The proposed Guidelines would apply to all insured state nonmember banks, state-licensed insured branches of foreign banks, and insured state savings associations that are subject to the provisions of Section 39 of the FDI Act, with total consolidated assets of $10 billion or more on or after the effective date of the final Guidelines. The proposal defines "total consolidated assets" for purposes of meeting the $10 billion threshold as total assets reported on an institution's Consolidated Reports of Condition and Income (Call Report) for the two most recent consecutive quarters. The institutions which meet these criteria are "covered institutions" under the proposed Guidelines. As analyzed more fully in the discussion of the expected effects of the proposed Guidelines below, the FDIC believes this proposed $10 billion threshold will reduce the likelihood of failure and the magnitude of losses in the event of a failure. As of March 31, 2023, there are 57 covered institutions.[24]

The FDIC proposes to apply the Guidelines to institutions whose Call Report filings reflect two consecutive quarters of total assets above $10 billion to provide institutions an "on-ramp" for compliance. This provides a certain amount of time for institutions to develop the policies, procedures, and programs they need to comply with the proposed Guidelines before they become a "covered institution" on the as-of date of the Call Report for the second consecutive quarter in which their total consolidated assets exceed $10 billion. Additionally, it will allow institutions that may only briefly exceed the threshold to reduce their total consolidated assets over the following quarter without

[24] FDIC Call Report Data, March 31, 2023. Count excludes First Republic Bank, which was closed by the California Department of Financial Protection and Innovation and the FDIC was appointed Receiver on May 1, 2023.

needing to comply with the Guidelines. The FDIC expects that institutions would be well aware in advance if they would exceed the $10 billion threshold and develop compliance programs in advance or plan to reduce their assets. Finally, the FDIC proposes to consider an institution to no longer be a "covered institution" if its Call Report filings show total consolidated assets below $10 billion for four consecutive quarters. The FDIC believes that these asset thresholds based on quarterly Call Report filings strike a balance between application of the Guidelines for larger, more complex institutions, while not capturing less-complex institutions whose total assets only exceed $10 billion briefly or whose size is reduced over time. This proposed asset threshold, however, is subject to the FDIC's existing authority as described below.

The proposed Guidelines include preservation and reservation of the FDIC's existing authority to address unsafe or unsound practices of all FDIC-supervised institutions. The Guidelines preserve the FDIC's authority to bring any enforcement action available to it independently of, in conjunction with, or in addition to any action under Section 39 of the FDI Act. Further, the FDIC reserves the authority to apply the proposed Guidelines, in whole or in part, to institutions with less than $10 billion in total consolidated assets if the FDIC determines that the institution's operations are highly complex or present heightened risk. The FDIC also reserves the authority, for each covered institution, to extend the time for compliance with these Guidelines or modify these Guidelines, as necessary, and can determine that compliance should no longer be required for covered institutions, if the institution's operations are no longer highly complex or no longer present a heightened risk. The FDIC's reservation of authority is not restricted by the asset threshold, as described above.

The Introduction also includes Definitions for terms used throughout the proposed Guidelines and a description of the role, responsibility, and structure of certain positions and functions within a covered institution that have a role in the risk management and

corporate governance of the covered institution. This section defines both the Chief Audit Officer (CAO) and the Chief Risk Officer (CRO) within a covered institution, describing their responsibilities and reporting structure. The CAO and CRO lead the internal audit unit and the independent risk management unit, respectively. The internal audit unit and the independent risk management unit maintain independence from front line units through the structure outlined in their respective definitions and as further detailed throughout the proposed Guidelines. Front line units mean those units that, in general, generate revenue or reduce costs for the covered institution. This proposed section also defines a covered institution's parent company. Finally, this proposed section defines the risk appetite and risk profile for the covered institution.

B. Section II – Corporate Governance

The board of directors of a covered institution has the ultimate responsibility for the safe and sound operation of the institution, overseeing management, and fulfilling its fiduciary duties. Effective corporate governance depends upon a board of directors that is active and engaged. As noted elsewhere in the discussion of these proposed Guidelines, the FDIC has observed that institutions with weak corporate governance are more likely to fail and are more likely to experience significant losses upon failure. To ensure the safety and soundness of covered institutions and the stability of the financial system, the FDIC is proposing these Guidelines for the boards of covered institutions regarding their obligations, composition, duties, and committee structure to set expectations for corporate governance.

Subsection A – Board of Directors – General Obligations

Proposed Section II, Subsection A describes the general obligations of a covered institution's board of directors. The board is ultimately responsible for the affairs of the covered institution and each individual member must abide by certain legal duties. These legal duties flow from the myriad federal and state laws applicable to the covered

institution, securities law and bank regulation, common law, and other sources that may impose criminal or civil liability on directors that fail to discharge their duties. Boards should familiarize themselves with and refer to all applicable federal and state law requirements.

Subsection B – Board Composition

These proposed Guidelines also establish an expectation for the composition of the board of directors. There should be at least a majority of independent directors on the board. An appropriately sized, diverse board of directors promotes effective, independent oversight of a covered institution and is important to the overall risk management of the institution. Diversity of demographic representation, opinion, experience, and ownership level is key to a board composition that can oversee management, address a variety of risks, and challenge others when necessary. A board that includes multiple members with similar experiences, opinions, or interests in the covered institution may result in a lack of creativity or individual responsibility for decisions, or gaps in knowledge, experience, or oversight, increasing risk to the institution.

The covered institution's organizational documents or state chartering authority may have requirements for board members, including a requirement for a certain number of directors. The proposed Guidelines expand upon, but do not replace, these requirements by providing covered institutions various considerations for ensuring an effective board composition. In determining the appropriate number of directors and the board's composition in accordance with state law, the board should consider how the selection of, and diversity among board members collectively and individually, may best promote effective, independent oversight of the covered institution's management and satisfy all legal requirements for outside and independent directors.[25]

---

[25] For example, the Depository Institutions Management Interlocks Act (12 U.S.C. 3201 *et seq*.) that generally prohibits a management official from serving two nonaffiliated depository

Subsection C – Duties of the Board

The duties of the board of directors of a covered institution flow from their responsibilities to fulfill their fiduciary duties, oversee management, and ensure safe and sound operation of the institution. As these responsibilities ultimately lie with the board, the FDIC is proposing the following Guidelines for the minimum duties of the boards of covered institutions. Each of the following duties is an integral component of the board's overall responsibility for risk management of the covered institution, holding executives and management accountable, and ensuring ethical operations.

The proposed Guidelines state that the board of a covered institution should set an appropriate tone for the institution. The "tone at the top" is integral to promoting a culture and environment of responsible and ethical behavior that discourages imprudent risk-taking in pursuit of profit. The proposed Guidelines include this responsibility for the board, in alignment with similar guidelines imposed by the Federal Reserve Board and the OCC. The tone set by the board is closely related to other concepts throughout the proposed Guidelines, including a Code of Ethics that encourages responsible behavior and a Compensation and Performance Management Program that does not incentivize imprudent risk-taking. By adhering to the law, these proposed Guidelines, and the board's own policies, the board sets the tone for the covered institution as a whole and reduces the likelihood or cost of failure.

The proposed Guidelines state that the board is responsible for the strategic plan and direction of the covered institution. Development and approval of a strategic plan is a common responsibility of a board of directors and its inclusion in these proposed Guidelines elaborates on the FDIC's expectations for such a plan to ensure the board of a covered institution is engaged with its business objectives while appropriately managing

---

organizations in situations where the management interlock likely would have an anticompetitive effect.

risk. A strategic plan developed by the Chief Executive Officer (CEO) with input from front-line units, independent risk management, and internal audit, and ultimately approved by the board, sets the direction of a covered institution to achieve business goals and manage the covered institution's risks. The strategic plan should cover at least a three-year period and be reviewed and approved annually to account for changing business conditions and risks to the covered institution.

The board of directors of a covered institution is also responsible for establishing the policies by which the institution operates, and these proposed Guidelines provide a high-level overview of such responsibility. Similar to a strategic plan, the adoption of policies ensures board engagement, prudent and proper risk management, and safe and sound operation. These proposed Guidelines do not prescribe the exact policies that the board of a covered institution may adopt; each institution varies in its business activities and unique risks and is responsible for making that determination itself. At a minimum, the covered institution should adopt policies and procedures to ensure safe and sound operation and fulfill the responsibilities outlined in Appendix A of part 364. For example, such policies and procedures may include a loan and/or credit policy, certain internal controls, and guides for assets and liabilities. Other statutes, regulations, or supervisory policies may require adoption of policies and procedures as well, such as compliance with the Bank Secrecy Act, consumer protection laws, the Community Reinvestment Act, and other legal requirements that may exist. The board should periodically review and revise its policies to ensure that they remain applicable and account for new or changing risks of the institution. Finally, compliance with the board's policies should be periodically reviewed by the internal audit function of the institution.

A Code of Ethics, written and adopted by the board, is integral to establishing an appropriate tone in a covered institution and setting expectations for behavior that manages risk. The proposed Guidelines state that the Code of Ethics should apply to all

directors, management, and employees. The proposed Guidelines also state, broadly, the areas that should be addressed by such a Code, including procedures and points of contact for reporting illegal or unethical behavior. A Code of Ethics should include topics addressing legal requirements, such as insider information, disclosure, and self-dealing.

The board of a covered institution should also provide active oversight of management. As the body that appoints and compensates the CEO (and possibly other management as well, either as a whole or by committee), it is the responsibility of the board of the covered institution to oversee the management that it has hired. Similarly, the board is responsible for overseeing compliance with the policies that it establishes, such as the strategic plan and the Code of Ethics, and is ultimately responsible for compliance with applicable laws and regulations. Under these proposed Guidelines, the board should hold management accountable and challenge and question management as necessary to ensure safe and sound operation of the covered institution.

The obligation of an individual board member to exercise independent judgment is included in the proposed Guidelines. Exercising sound, independent judgment is integral to a director's responsibility and duties to a covered institution. In addition, individual directors and the board as a whole should exercise independent judgment by ensuring that they are not excessively influenced by a single dominant policymaker, who may be a director, management, shareholder, or other individual. Such dominant policymakers present risks to the board and covered institutions by inhibiting board members' exercise of independent judgment, causing a power vacuum if they leave the institution, and presenting difficulty if mismanagement can be attributed to a single dominant individual.

The proposed Guidelines provide that the board of a covered institution must also select and appoint qualified executive officers. This typically includes the CEO, but may also include other officers appointed by the board as a whole or by committee. Such

selection and appointment is standard among boards of covered institutions; these proposed Guidelines provide a minimum expectation for selection criteria of personnel, grounds for dismissal, succession planning, and training.

The board of a covered institution should also provide ongoing training to each of its directors. To that end, the proposed Guidelines include examples of training that a board may conduct to ensure that it has the knowledge, abilities, and skills to understand industry trends, statutory and regulatory developments, and an understanding of the issues that affect the covered institution. The formal training program should include, at a minimum, the products, services, lines of business, and risks of the covered institution; laws, regulations, and supervisory requirements applicable to the covered institution; and other topics that the board may identify to ensure that the institution maintains safe and sound operation and the board can execute its duties appropriately.

A self-assessment at the board level is necessary for the directors of a covered institution to examine their own compliance, hold themselves accountable, and make plans to improve any gaps or deficiencies in their performance. Identifying and addressing deficiencies at the board level ensures one more layer of protection against risk. To that end, these proposed Guidelines state that the board should conduct such a self-assessment on a regular basis.

The board should also establish Compensation and Performance Management Programs. The proposed Guidelines include this as a component of the overall risk management of a covered institution; incentives and compensation programs may pose safety and soundness risks if they encourage noncompliance with laws, regulations, or internal policies to meet business objectives. To safeguard against those risks, these Guidelines propose that a Compensation and Performance Management Program be established by the board to ensure adherence to an effective risk management program, ensure issues identified by the risk management and internal audit functions are

addressed, and attract and retain competent staff.

Subsection D – Committees of the Board

The board of directors of a covered institution is expected to work through a committee structure that allows directors to stay informed, divide labor, and handle matters that require detailed review and in-depth consideration. These proposed Guidelines set the minimum expectations for committees of the board that oversee critical elements of the covered institution's overall risk management. The committees proposed in these Guidelines are in addition to, not in lieu of, any committees that may be required by other laws, regulations, or supervisory requirements.

An Audit Committee must be established as defined in these proposed Guidelines and as required by Section 36 of the FDI Act[26] and part 363 of the FDIC's regulations.[27] The Audit Committee, composed entirely of outside and independent directors as required by statute and regulation, oversees financial reporting, independent audits, the Chief Audit Officer, and the internal audit function. Furthermore, this Committee should report to the full board regarding the progress of the covered institution in addressing issues identified by the internal audit function and recommending further action.

A Compensation Committee established under these proposed Guidelines must comply with any exchange rules that may be applicable to publicly traded covered institutions and the FDIC's regulations, including Appendix A of part 364. The Compensation Committee assists in managing the risks of a covered institution by ensuring that compensation and performance management do not reward or encourage imprudent risk-taking or violations of legal requirements in pursuit of profit or business objectives. Furthermore, compensation that is excessive or that could lead to a material financial loss constitutes an unsafe and unsound practice that this Committee is also

[26] 12 U.S.C. 1831m.
[27] 12 CFR part 363.

designed to guard against.

These proposed Guidelines include the establishment of a Trust Committee if the covered institution has trust powers. This Committee oversees and manages the risks presented by the operation of a trust department by ensuring that the trust department is separate and apart from other departments of the covered institution, trust assets are separated from other assets of the covered institution, assets of each trust account are separated from the assets of other accounts, and ensuring overall compliance with applicable laws and regulations. These proposed Guidelines include these requirements as best practices for management of a trust department in a covered institution.

These proposed Guidelines also include requirements for a Risk Committee. The Risk Committee is responsible for approving and periodically reviewing the risk management policies of a covered institution and overseeing the risk management framework. To ensure that the Risk Committee is independent and able to effectively complete its mission, and to minimize the risk of failure and the magnitude of losses of a covered institution, these proposed Guidelines include requirements consistent with that of other Federal banking agencies. By requiring that the Committee has an independent director as its chair and be an independent committee of the board that reports directly to the board, these proposed Guidelines help to ensure that the individuals responsible for oversight of the covered institution's overall risks are free to make recommendations to the board and challenge management as necessary. At least one individual on the Committee should be experienced in managing the risks of a firm commensurate with the size, business model, complexity and risk profile of the covered institution to ensure that the Committee has the necessary expertise to fulfill its obligations. Reviewing reports from the CRO and meeting with the Committee not less than quarterly ensures that the Risk Committee can stay abreast of the risks of the covered institution, including any internal or external changes that may affect the institution, and make recommendations

accordingly. Finally, the Risk Committee overseeing the compensation and performance management of the CRO ensures that the CRO can maintain their independence and objectively assess the risks of the covered institution. The proposed Guidelines regarding the Risk Committee ensure proper oversight of the covered institution's independent risk management function and the risks of the institution itself. These requirements support the continued safety and soundness of large and complex institutions.

The board should also create other committees as required or appropriate for the board to perform its duties under these proposed Guidelines. While the Committees outlined in these proposed Guidelines represent the FDIC's minimum expectations for division of labor and expertise among the board of directors of a covered institution, it does not obviate the institution from creating board committees as necessary, commensurate with its risk profile and operations of the institution to ensure safety and soundness. For example, many institutions find it prudent to have a credit committee that establishes loan and credit policies of the covered institution and reviews and approves loans above a certain amount. Other institutions may be heavily involved in financial technology and determine that it is necessary to have committees addressing information technology, cybersecurity, or partnerships. A covered institution should consider its risk profile and complexity of operations to determine whether a board committee is necessary to ensure matters requiring detailed review and in-depth consideration are addressed appropriately.

C. Section III – Board and management responsibility regarding risk management and audit

Under Proposed Section III, the FDIC would expect a covered institution to have and adhere to a risk management program for managing and controlling the covered institution's risk taking. 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. The proposed Guidelines describe the responsibilities of each of these units in detail.

The proposed Guidelines provide that for a covered institution that has a parent company, if the risk profiles of each entity are substantially similar, the covered institution may adopt and implement all or any part of its parent company's risk management program that: satisfies the minimum standards in these Guidelines; ensures that the safety and soundness of the covered institution is not jeopardized by decisions made by the parent company's board and management; and ensures that the covered institution's risk profile is easily distinguished and separate from that of its parent for risk management and supervisory reporting purposes. Consideration of these factors may require the covered institution to have separate and focused governance and risk management practices.

Under these proposed Guidelines, a covered institution's risk management program should include a risk profile and a risk appetite statement. These documents form the foundation of an effective risk management program by providing an objective assessment of the institution's risks, and based on that risk profile, the board should establish written limits and levels of risks that the institution will accept. The independent risk management unit should develop the risk management program based on the risk profile of the institution and the risk appetite statement. At least annually and as the risks of the institution change, whether by internal or external factors, the risk management unit should review and update the risk management program. These proposed Guidelines provide the FDIC's expectations for the scope of the risk management program, including the risk categories, risk control infrastructure, and processes and systems for implementing and monitoring policies and procedures that govern, identify, and report risk. The risk management program should be effectively

communicated throughout the institution so that all units understand their respective responsibilities.

Under the three-lines-of-defense model in these proposed Guidelines, a covered institution should have three units, held accountable by the CEO and the board, for monitoring and reporting on compliance with the risk management program. The front line units, which are generally business units that generate revenue or save costs for the covered institution as defined in these Guidelines, are responsible for ensuring that their activities do not create excessive risks or exceed the risk appetite of the institution. The independent risk management unit, under direction of the CRO, should identify, assess, and oversee the covered institution's risk-taking activities on an ongoing basis. The independent risk management unit and CRO should be able to communicate with the CEO and the Risk Committee of the board of directors to identify and report risks and suspected instances of noncompliance. The internal audit unit, under direction of the CAO, should ensure that the covered institution complies with laws and regulations and adheres to the covered institution's risk management program. It should establish and adhere to an audit plan and report its findings, including any recommendations, to the Audit Committee of the board of directors. This three-lines-of-defense model, when taken as a whole with the duties and oversight of the board under proposed Section II of these Guidelines, ensures safety and soundness, reduces the likelihood of failure, and reduces the magnitude of any loss by preventing a single point of failure within an organization and providing for multiple checks within a covered institution's risk management.

The proposed Guidelines also provide the FDIC's expectations regarding the board's establishment of, and the covered institution's adherence to, processes governing breaches to risk limits and violations of law or regulations. The front line units and independent risk management unit, consistent with their respective responsibilities,

should identify breaches of the institution's risk appetite and other risk limits, distinguish breaches based on severity, report on the breach, its impact, and resolution, and establish consequences for breaches of risk limits. Similarly, the front line units and risk management unit should identify known or suspected violations of law or regulations. All violations of law or regulations and documentation regarding efforts to return to compliance should be documented in writing, distributed to relevant parties within the institution, and records should be retained for FDIC review. Known or suspected violations of law involving dishonesty, misrepresentation, or willful disregard for legal requirements must be promptly reported as required by law and on a timetable acceptable to the agency with jurisdiction.

IV. Expected Effects of Implementing the Proposed Guidelines

As previously discussed, if approved, the proposed rule would establish proposed Guidelines that include standards for corporate governance and risk management for covered institutions. As of the quarter ending March 31, 2023, the FDIC supervises 3,012 IDIs, of which 57 reported total consolidated assets of $10 billion or more.[28] Therefore, the FDIC estimates that 57 FDIC-supervised IDIs will be directly affected by the proposed rule, if approved.

The proposed Guidelines contain expectations for roles and responsibilities of the board, size and makeup of the board, organization of the board, committee structures of the board, development and maintenance of a strategic plan, development and maintenance of risk management policies, hiring and oversight of senior management, development and maintenance of processes for responding to violations of laws, regulations, or breaches of internal risk limits or other internal policies and procedures.

As previously discussed, all FDIC-supervised institutions have existing

[28] FDIC Call Report Data, March 31, 2023. Count excludes First Republic Bank, which was closed by the California Department of Financial Protection and Innovation and the FDIC was appointed Receiver on May 1, 2023.

requirements to establish operational and management standards to ensure the safe and sound operation of the IDI appropriate to the size of the IDI and the nature, scope and risk of its activities.[29] Additionally, certain FDIC-supervised institutions are subject to audit requirements, including the establishment of an audit committee as well as its makeup.[30] Finally, as previously discussed the FDIC has issued several guidance items related to appropriate risk management and ethics.[31]

The FDIC believes that the proposed rule will benefit covered institutions by reducing the likelihood and magnitude of losses and the likelihood of failure. The FDIC does not have access to information that would enable a quantitative estimate of the benefits of the proposed rule. Although there are existing regulations and guidance related to corporate governance and risk management, the FDIC has not previously issued supervisory guidelines or regulations specifically on corporate governance and risk management for covered institutions. The FDIC believes that adoption of the proposed Guidelines would benefit covered institutions by establishing clear expectations for covered institutions and strengthening corporate governance and risk management. Additionally, by adopting the proposed Guidelines in Appendix C to part 364, the FDIC could require a compliance plan or take other corrective action if warranted further reducing the likelihood and magnitude of loss, and the likelihood of failure.

The proposed Guidelines would result in some compliance costs for covered institutions. As previously discussed, FDIC-supervised IDIs have an existing requirement to establish operational and management standards to ensure the safe and sound operation of the IDI appropriate to the size of the IDI and the nature, scope and risk of its activities. Additionally, the FDIC has issued a number of guidance items related to appropriate risk management and ethics. However, while the FDIC has communicated through the

---

[29] 12 CFR 364.101, Appendix A.
[30] 12 CFR 363.2.
[31] *See* footnotes 10-15.

supervisory process for larger, more complex institutions an expectation that corporate governance and risk management frameworks need to be more robust and suitable for the IDI's risk profile and business model, the FDIC has not previously issued supervisory guidance specifically on corporate governance and risk management for covered institutions. Based on the foregoing information, the FDIC estimates that the proposed rule, if adopted, would compel covered institutions to expend 91,375 labor hours in the first year, and 90,365 labor hours each additional year, to comply with the recordkeeping, reporting, and disclosure requirements. At an estimated wage rate of $139.33[32] per hour, this would amount to total additional estimated reporting, recordkeeping, and disclosure costs of $12.73 million in the first year, and $12.59 million each additional year. This estimated annual cost is less than 0.03 percent of annual noninterest expense for all covered institutions. Additionally, the FDIC believes that covered institutions are likely to incur other regulatory costs to achieve compliance with the proposed rule, if adopted, such as hiring additional staff and changes to internal systems and processes.

If adopted, the FDIC believes that the proposed rule would benefit the financial sector and customers by reducing the likelihood of failure and associated costs. Bank failures impose costs on the DIF and negatively affect a wide variety of stakeholders, and reduce public confidence in the financial system. The FDIC believes that adoption of the proposed rule would help to limit such costs.

V. Alternatives Considered

The FDIC considered three alternatives: (1) maintaining the status quo with no

---

[32] The recordkeeping, reporting, and disclosure compliance burden is expected to be distributed between executives, lawyers and financial analysts. The estimated weighted average hourly compensation cost of these employees are found by using the 75th percentile hourly wages reported by the Bureau of Labor Statistics (BLS) National Industry-Specific Occupational Employment and Wage Estimates for the relevant occupations in the Depository Credit Intermediation sector, as of May 2022. These wages are adjusted to account for inflation and compensation rates for health and other benefits, as of March 2023, to provide an estimate of overall compensation.

specific guidance for covered institutions; (2) issuing guidance specific to covered institutions; and (3) issuing regulations on corporate governance for covered institutions. The FDIC believes that the proposed Guidelines, if adopted, would improve upon the status quo by consolidating and codifying the FDIC's expectations for a covered institution's effective corporate governance and risk management practices and potentially reducing future losses or bank failures and that these benefits outweigh the potential costs. Additionally, the FDIC believes that the proposed Guidelines are more appropriate than the status quo alternative because they would further codify the FDIC's expectations for effective corporate governance and risk management practices of a covered institution while still allowing the FDIC to consider appropriate variances in an individual covered institution's risk profile. The FDIC also considered the alternative of issuing guidance for covered institutions. However, such guidance would not provide an enforcement framework to ensure compliance such as compliance plans under 12 CFR part 308, subpart R, or other actions.

VI. Request for Comments

The FDIC requests comment on all aspects of the proposed rule and proposed Guidelines, including the following:

1. *Should the proposed Guidelines apply to FDIC-supervised institutions with $10 billion or more in total consolidated assets, or would a higher or lower threshold be appropriate? Alternatively, should the proposed Guidelines only apply to FDIC-supervised institutions that are examined under the FDIC's Continuous Examination Process? Please explain.*
2. *Is there a need to differentiate corporate governance and risk management requirements for covered institutions with $50 billion or more in total consolidated assets (or some other threshold)? Please explain.*
3. *Should the proposed Guidelines apply to any insured state nonmember bank or*

insured state savings association with total consolidated assets less than $10 billion if that institution's parent company controls at least one covered institution?

4. *The proposed Guidelines include a reservation of authority enabling the FDIC to determine that compliance with the proposed Guidelines should not be, or no longer be, required for a covered institution based on risk and complexity. Should there be an application process in accordance with subpart A of part 303 of the FDIC's regulations for a covered institution to request exemption from the requirements of these proposed Guidelines? If so, what criteria would be appropriate for FDIC to establish to consider such a request?*
5. *Should the covered institution and its parent holding company with other affiliates be required to have separate risk management officers and staff? Please explain.*
6. *The proposed Guidelines provide that a covered institution may use its parent company's risk governance framework to satisfy the Guidelines based on certain factors. What other factors, if any, should the FDIC consider?*
7. *Should the proposed Guidelines include more specific suggestions for corporate governance? If so, what additional suggestions should be included?*
8. *Should the proposed Guidelines include more specific requirements for risk management? If so, what additional requirements should be included?*
9. *Do the proposed Guidelines provide sufficient and appropriate requirements regarding the role of the board for corporate governance and risk management? Please explain.*
10. *Do the proposed Guidelines provide sufficient and appropriate requirements regarding the role of executive management for managing the covered institution and its risks? Please explain.*

11. *Should the CRO or the CAO report to the board or solely to a board committee? Please explain.*

12. *Do the CRO or the CAO and their associated functions have sufficient independence under the proposed Guidelines? Please explain.*

13. *Would the proposed Guidelines have any costs or benefits that the FDIC has not identified? If so, please identify and discuss.*

14. *Are there alternative ways to achieve the objectives of these proposed Guidelines that would impose lower burdens and costs on covered institutions? If so, what alternatives would be appropriate?*

VII. Regulatory Analysis

A. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) generally requires an agency, in connection with a proposed rule, to prepare and make available for public comment an initial regulatory flexibility analysis that describes the impact of the proposed rule on small entities.[33] However, an initial regulatory flexibility analysis is not required if the agency certifies that the proposed rule will not, if promulgated, have a significant economic impact on a substantial number of small entities. The Small Business Administration (SBA) has defined "small entities" to include banking organizations with total assets of less than or equal to $850 million.[34] Generally, the FDIC considers a significant economic impact to be a quantified effect in excess of 5 percent of total annual salaries

---

[33] 5 U.S.C. 601 *et seq*.

[34] The SBA defines a small banking organization as having $850 million or less in assets, where an organization's "assets are determined by averaging the assets reported on its four quarterly financial statements for the preceding year." *See* 13 CFR 121.201 (as amended by the SBA [87 FR 69118 (Nov. 17, 2022]), effective December 19, 2022). In its determination, the "SBA counts the receipts, employees, or other measure of size of the concern whose size is at issue and all of its domestic and foreign affiliates." *See* 13 CFR 121.103. Following these regulations, the FDIC uses an insured depository institution's affiliated and acquired assets, averaged over the preceding four quarters, to determine whether the insured depository institution is "small" for the purposes of RFA.

and benefits or 2.5 percent of total noninterest expenses. The FDIC believes that effects in excess of one or more of these thresholds typically represent significant economic impacts for FDIC-supervised IDIs. The proposed rule would only apply to FDIC-supervised state nonmember banks, savings associations, and state branches of foreign banks having total consolidated assets of $10 billion or more. As of the quarter ending March 31, 2023, the FDIC supervised 3,012 depository institutions, of which 2,306 are considered "small" for the purposes of RFA. As of the quarter ending March 31, 2023, there are no small, FDIC-insured institutions with $10 billion or more in total consolidated assets. In light of the foregoing, the FDIC certifies that the proposed rule would not have a significant economic impact on a substantial number of small entities. Accordingly, an initial regulatory flexibility analysis is not required.

The FDIC invites comments on all aspects of the supporting information provided in this RFA section. In particular, would this proposed rule have any significant effects on small entities that the FDIC has not identified?

B. Paperwork Reduction Act

Certain provisions of the proposed rule contain "collection of information" requirements within the meaning of the Paperwork Reduction Act of 1995 (PRA).[35] In accordance with the PRA, the FDIC may not conduct or sponsor, and an organization is not required to respond to this information collection, unless the information collection displays a currently valid Office of Management and Budget (OMB) control number. The FDIC will request approval from the OMB for this proposed information collection. OMB will assign an OMB control number.

OMB Number: 3064-NEW

Frequency of Response: Periodic – see table below.

Affected Public: FDIC-supervised IDIs.

---

[35] 44 U.S.C. 3501-3521.

Total Estimated Annual Burden: 91,375 hours.

The FDIC estimates that a covered institution that currently has strong corporate governance and risk management programs may not need to significantly increase the number of hours it spends on corporate governance and risk management to comply with the proposed Guidelines.

ESTIMATED HOURLY BURDEN - 2023 Part 364, Appendix C NPR							
Number	**Information Collection Description and Citation**	**Type of Burden**	**Frequency**	**Number Respondents**	**Number of Responses Per Respondent**	**Time Per Response**	**Total Estimated Annual Burden**
1	Audit Committee, Review and Approval of the Internal Audit Unit's Charter Section I(D)(7)(b) One-Time	Recordkeeping	One-Time	1	1	40	40
2	Audit Committee, Annual Review and Approval of the Internal Audit Unit's Charter Section I(D)(7)(c) Ongoing	Recordkeeping	Annually	1	1	20	20
3	Development of a Written Strategic Plan Section II(C)(2) One-Time	Recordkeeping	One-Time	1	1	120	120
4	Annual Evaluation and Approval of Strategic Plan Section II(C)(2) Ongoing	Recordkeeping	Annually	57	1	60	3,420
5	Board, Establishment and Approval of Policies Governing Operations Section II(C)(3) One-Time	Recordkeeping	One-Time	1	1	40	40
6	Board, Annual Review Policies Governing Operations Section II(C)(3) Ongoing	Recordkeeping	Annually	57	1	20	1,140
7	Establishment of a Written Code of Ethics Section II(C)(4) One-Time	Recordkeeping	One-Time	1	1	40	40
8	Annual Review Written Code of Ethics Section II(C)(4) Ongoing	Recordkeeping	Annually	57	1	20	1,140
9	Establishment of a Management Performance Review Process Section II(C)(7) One-Time	Recordkeeping	One-Time	1	1	40	40
10	Annual Review of Management Performance Review Process Section II(C)(7) Ongoing	Recordkeeping	Annually	57	1	20	1,140
11	Development of a Succession Plan Section II(C)(7) One-Time	Recordkeeping	One-Time	1	1	40	40
12	Annual Review Succession Plan Section II(C)(7) Ongoing	Recordkeeping	Annually	57	1	20	1,140
13	Establishment of a Training Program for Directors Section II(C)(8)	Recordkeeping	One-Time	1	1	50	50

	One-Time						
14	Annual Review Training Program for Directors Section II(C)(8) Ongoing	Recordkeeping	Annually	57	1	25	1,425
15	Board Annual Self-Assessment Section II(C)(9) Ongoing	Recordkeeping	Annually	57	1	20	1,140
16	Establishment of a Compensation and Performance Management Program Section II(C)(10) One-Time	Recordkeeping	One-Time	1	1	100	100
17	Annual Review of Compensation and Performance Management Program Section II(C)(10) Ongoing	Recordkeeping	Annually	57	1	50	2,850
18	Establishment of a Written Charter for Board Committees Section II(D) One-Time	Recordkeeping	One-Time	1	1	40	40
19	Annual Review of Written Charter for Board Committees Section II(D) Ongoing	Recordkeeping	Annually	57	1	20	1,140
20	Board Approval of Charter of Internal Audit Function Section II(D)(1)(e) One-Time	Recordkeeping	One-Time	1	1	20	20
21	Board Annual Review of Charter of Internal Audit Function Section II(D)(1)(f) Ongoing	Recordkeeping	Annually	57	1	10	570
22	Audit Committee, Approval of all Audit Services Section II(D)(1)(b) Ongoing	Recordkeeping	On Occasion	57	1	40	2,280
23	Audit Committee, Approval all Decisions Regarding the Appointment or Removal and Annual Compensation and Salary Adjustment for the CAO Section II(D)(1)(d) Ongoing	Recordkeeping	On Occasion	57	1	40	2,280
24	Risk Committee, Approval of Risk Management Policies Section II(D)(4) One-Time	Recordkeeping	One-Time	1	1	40	40
25	Risk Committee, Annual Review of Charter of Internal Audit Function Section II(D)(4) Ongoing	Recordkeeping	Annually	57	1	20	1,140
26	Risk Committee, Quarterly Review of CRO Reports Section II(D)(4)(e) Ongoing	Recordkeeping	Quarterly	57	4	40	9,120
27	Risk Committee, Quarterly Documentation of Proceedings and Risk Management Decisions Section II(D)(4)(f) Ongoing	Recordkeeping	Quarterly	57	4	40	9,120
28	Risk Committee, Approval of Decisions Regarding Appointment or Removal of CRO Section II(D)(4)(g) Ongoing	Recordkeeping	On Occasion	57	1	40	2,280

29	Board Establishment of a Comprehensive Risk Management Program Section III(A) One-Time	Recordkeeping	One-Time	1	1	100	100
30	Board Annual Review of Comprehensive Risk Management Program Section III(A) Ongoing	Recordkeeping	Annually	57	1	50	2,850
31	Board Establishment of a Risk Profile Section III(B) One-Time	Recordkeeping	One-Time	1	1	40	40
32	Board Quarterly Review of Risk Profile Section III(B) Ongoing	Recordkeeping	Quarterly	57	4	40	9,120
33	Establishment of a Comprehensive Written Statement that Establishes Risk Appetite Limits Section III(B) One-Time	Recordkeeping	One-Time	1	1	40	40
34	Board Quarterly Review and Approval of Risk Appetitive Statement Section III(B) Ongoing	Recordkeeping	Quarterly	57	4	20	4,560
35	Report Risk Limit Breaches to the FDIC Section III(C)(2)(c)(iii) Ongoing	Reporting	On Occasion	57	1	20	1,140
36	Front Line Unit, Establishment of Written Policies that Include Risk Limits Section III(C)(3)(a)(ii) One-Time	Recordkeeping	One-Time	1	1	40	40
37	Front Line Unit, Annual Review of Written Policies that Include Risk Limits Section III(C)(3)(a)(ii) Ongoing	Recordkeeping	Annually	57	1	20	1,140
38	Front Line Unit, Establish Procedures and Processes, as Necessary to Ensure Compliance with Board Policies Section III(C)(3)(a)(iii) One-Time	Recordkeeping	One-Time	1	1	40	40
39	Front Line Unit, Annual Review of Procedures and Processes, as Necessary to Ensure Compliance with Board Policies Section III(C)(3)(a)(iii) Ongoing	Recordkeeping	Annually	57	1	20	1,140
40	Front Line Unit, Quarterly Monitor and Report Compliance with Respective Risk Limits Section III(C)(3)(a)(v) Ongoing	Recordkeeping	Quarterly	57	4	40	9,120
41	Independent Risk Management Unit, Quarterly Monitor and Report on the Covered Institution's Risk Profile Relative to Risk Appetite and Concentration Limits Section III(C)(3)(b)(iii) Ongoing	Recordkeeping	Quarterly	57	4	40	9,120
42	Independent Risk Management Unit, Establishment of Policies Relative to Concentration Risk Limits Section III(C)(3)(b)(iv) One-time	Recordkeeping	One-Time	1	1	40	40
43	Independent Risk Management Unit, Review and Update of Policies Relative to Concentration Risk Limits Section III(C)(3)(b)(iv) Ongoing	Recordkeeping	Annually	57	1	40	2,280

44	Independent Risk Management Unit, Establishment of Procedures and Processes to Ensure Compliance with Board Risk Management Policies Section III(C)(3)(b)(v) One-time	Recordkeeping	One-Time	1	1	20	20
45	Independent Risk Management Unit, Review and Update of Procedures and Processes to Ensure Compliance with Board Risk Management Policies Section III(C)(3)(b)(v) Ongoing	Recordkeeping	Annually	57	1	10	580
46	Independent Risk Management Unit, Quarterly Monitor and Report to CEO and Risk Committee Front Line Units' Compliance with Risk Limits Section III(C)(3)(b)(vii) Ongoing	Recordkeeping	Quarterly	57	4	10	2,280
47	Internal Audit Unit, Establishment of an Audit Plan Section III(C)(3)(c)(ii) One-Time	Recordkeeping	One-Time	1	1	40	40
48	Internal Audit Unit, Quarterly Report Changes to Audit Plan Section III(C)(3)(c)(ii) Ongoing	Recordkeeping	Quarterly	57	4	10	2,280
49	Board, Establishment of Processes that Require the Front Line and Independent Risk Management Units to Identify and Distinguish Breaches, as well as Establishment of Accountability for Reporting and Resolving Breaches Section III(E) One-Time	Recordkeeping	One-Time	1	1	40	40
50	Board, Annual Review Processes that Require the Front Line and Independent Risk Management Units to Identify and Distinguish Breaches, as well as Establish Accountability for Reporting and Resolving Breaches Section III(E) Ongoing	Recordkeeping	Annually	57	1	20	1,140
51	Front Line and Independent Risk Management Units Report to the FDIC Breach of a Risk Limit or Noncompliance with the Risk Appetite Statement or Risk Management Program Section III(E)(3) Ongoing	Reporting	On Occasion	57	1	20	1,140
52	Board, Establishment of Processes that Require Front Line and Independent Risk Management Units to Identify, Distinguish, Document and Report Violations of Law or Regulations Section III(F) One-Time	Recordkeeping	One-Time	1	1	40	40
53	Board, Annual Review of Processes that Require Front Line and Independent Risk Management Units to Identify, Distinguish, Document and Report Violations of Law or Regulations Section III(F) Ongoing	Recordkeeping	Annually	57	1	20	1,140
					TOTAL HOURLY BURDEN		**91,375 hours**

General Description

Section 39 of the FDI Act requires the FDIC to issue certain safety and soundness

standards by regulation or guideline. In this instance, the FDIC is proposing guidelines to address corporate governance and risk management by covered institutions. The FDIC estimates that most, if not all covered institutions, as part of their standard governance and risk management practices, maintain procedures discussed in the proposed Guidelines, so the FDIC is assigning a one placeholder for implementation burden. However, the FDIC is estimating the burden associated with what covered institutions need to do going forward to comply with the proposed Guidelines.

This information collection includes the need for a strategic plan, a risk committee, board review of information and policies, formal training program for directors, self-assessments, compensation and performance management programs, risk profile and risk appetite statement, a written risk management program, front line units, an independent risk management unit, an internal audit unit, and processes for governing risk limit breaches and noncompliance with laws or regulation.

Comments are invited on:

(a) Whether the proposed collection of information is necessary for the proper performance of the functions of the FDIC, including whether the information will have practical utility;

(b) The accuracy of the FDIC's estimate of burden of the proposed collection of information, including the validity of the methodology and assumptions used, including the FDIC's estimated implementation burden;

(c) Ways to enhance the quality, utility, and clarity of the information to be collected;

(d) Ways to minimize the burden of the information collection on those who are to respond, including appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology (e.g., permitting electronic submission of responses); and

(e) Estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to provide information.

All comments will become a matter of public record. Comments on the collection of information should be sent to the address listed in the ADDRESSES section of this document. A copy of the comments may also be submitted to the OMB desk officer by mail to: U.S. Office of Management and Budget, 725 17th Street NW, #10235, Washington, DC 20503, or by facsimile to 202-395-6974; or email to oira_submission@omb.eop.gov, Attention, Federal Banking Agency Desk Officer.

C. Riegle Community Development and Regulatory Improvement Act of 1994

Pursuant to Section 302(a) of the Riegle Community Development and Regulatory Improvement Act of 1994[36] (RCDRIA), in determining the effective date and administrative compliance requirements for new regulations that impose additional reporting, disclosure, or other requirements on insured depository institutions, each Federal banking agency must consider, consistent with principles of safety and soundness and the public interest, any administrative burdens that such regulations would place on affected depository institutions, including small depository institutions, and customers of depository institutions, as well as the benefits of such regulations. In addition, Section 302(b) of RCDRIA requires new regulations and amendments to regulations that impose additional reporting, disclosures, or other new requirements on insured depository institutions generally to take effect on the first day of a calendar quarter that begins on or after the date on which the regulations are published in final form.[37] The FDIC invites comments that will further inform its consideration of RCDRIA.

D. Plain Language

---

[36] 12 U.S.C. 4802(a).
[37] 12 U.S.C. 4802(b).

Section 722 of the Gramm-Leach-Bliley Act[38] requires the Federal banking agencies to use plain language in all proposed and final rules published after January 1, 2000. The FDIC invites your comments on how to make the proposed rule and Guidelines easier to understand. For example:

• Has the FDIC organized the material to suit your needs? If not, how could this material be better organized?

• Are the requirements in the proposed rule and proposed Guidelines clearly stated? If not, how could the proposed rule and proposed Guidelines be more clearly stated?

• Do the proposed rule and proposed Guidelines contain language or jargon that is not clear? If so, which language requires clarification?

• Would a different format (grouping and order of sections, use of headings, paragraphing) make the proposed rule and proposed Guidelines easier to understand? If so, what changes to the format would make the proposed rule and proposed Guidelines easier to understand?

• What else could the FDIC do to make the proposed rule and proposed Guidelines easier to understand?

E. Providing Accountability Through Transparency Act of 2023

The Providing Accountability Through Transparency Act of 2023 (12 U.S.C. 553(b)(4)) requires that a notice of proposed rulemaking include the Internet address of a summary of not more than 100 words in length of a proposed rule, in plain language, that shall be posted on the Internet website under section 206(d) of the E-Government Act of 2002 (44 U.S.C. 3501 note).

In summary, the FDIC is proposing to issue Guidelines as a new Appendix C to part 364 (part 364) to strengthen the corporate governance and risk management practices and board oversight of FDIC-supervised institutions with total consolidated assets of $10

[38] Pub. L. 106-102, sec. 722, 113 Stat. 1338, 1471 (1999).

billion or more. The proposed Guidelines are intended to raise the FDIC's standards for corporate governance, risk management, and control to help ensure these larger institutions effectively anticipate, evaluate, and mitigate the risks they face. The proposal and the required summary can be found at https://www.fdic.gov/resources/regulations/federal-register-publications/.

List of Subjects

12 CFR Part 308

Administrative practice and procedure, Bank deposit insurance, Banks, Banking, Claims, Crime, Equal access to justice, Fraud, Investigations, Lawyers, Penalties, Safety and soundness compliance plans, Savings associations.

12 CFR Part 364

Banks, Banking, Information, Safety and soundness guidelines.

Authority and Issuance

For the reasons set forth in the preamble, the Federal Deposit Insurance Corporation proposes to amend parts 308 and 364 of chapter III of title 12 of the Code of Federal Regulations as follows:

PART 308—RULES OF PRACTICE AND PROCEDURE

1. The authority citation for part 308 continues to read as follows:

Authority: 5 U.S.C. 504, 554–557; 12 U.S.C. 93(b), 164, 505, 1464, 1467(d), 1467a, 1468, 1815(e), 1817, 1818, 1819, 1820, 1828, 1829, 1829(b), 1831i, 1831m(g)(4), 1831o, 1831p–1, 1832(c), 1884(b), 1972, 3102, 3108(a), 3349, 3909, 4717, 5412(b)(2)(C), 5414(b)(3); 15 U.S.C. 78(h) and (i), 78o(c)(4), 78o–4(c), 78o–5, 78q–1, 78s, 78u, 78u–2, 78u–3, 78w, 6801(b), 6805(b)(1); 28 U.S.C. 2461 note; 31 U.S.C. 330, 5321; 42 U.S.C. 4012a; Pub. L. 104–134, sec. 31001(s), 110 Stat. 1321; Pub. L. 109–351, 120 Stat. 1966; Pub. L. 111–203, 124 Stat. 1376; Pub. L. 114–74, sec. 701, 129 Stat. 584.

2. Revise § 308.302 (a) to read as follows:

§ 308.302 Determination and notification of failure to meet a safety and soundness standard and request for compliance plan.

* * * * *

(a) *Determination.* The FDIC may, based upon an examination, inspection or any other information that becomes available to the FDIC, determine that a covered institution has failed to satisfy the safety and soundness standards set out in part 364 of this chapter and in the Interagency Guidelines Establishing Standards for Safety and Soundness in appendix A, the Interagency Guidelines Establishing Standards for Safeguarding Customer Information in appendix B, and the Guidelines Establishing Standards for Corporate Governance and Risk Management for Covered Institutions with Total Consolidated Assets of $10 Billion or More in appendix C to part 364 of this chapter.

* * * * *

PART 364—STANDARDS FOR SAFETY AND SOUNDNESS

3. The authority citation for part 364 continues to read as follows:

Authority: 12 U.S.C. 1818 and 1819 (Tenth), 1831p–1; 15 U.S.C. 1681b, 1681s, 1681w, 6801(b), 6805(b)(1).

4. Add paragraph (c) to § 364.101 to read as follows:

§ 364.101 Standards for safety and soundness.

* * * * *

(c) *Guidelines Establishing Standards for Corporate Governance and Risk Management for Covered Institutions with Total Consolidated Assets of $10 Billion or More.* The Guidelines Establishing Standards for Corporate Governance and Risk Management for Covered Institutions with Total Consolidated Assets of $10 Billion or More pursuant to Section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p-1), as set forth as appendix C to this part, apply to all insured state nonmember banks, state-

licensed insured branches of foreign banks that are subject to the provisions of Section 39 of the Federal Deposit Insurance Act, and state savings associations with $10 billion or more in total consolidated assets.

5. Add Appendix C to part 364 to read as follows:

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

Table of Contents

I. INTRODUCTION.

Section 39 of the Federal Deposit Insurance Act (FDI Act) authorizes the Federal Deposit Insurance Corporation (FDIC) to establish safety and soundness standards by regulation or by guidelines. The following Guidelines address standards for corporate governance, risk management, and boards of directors' oversight for covered institutions. These standards are in addition to other standards or requirements in law or regulation.[39]

[39] The roles and responsibilities provided for in these Guidelines are in addition to those set forth in existing laws, regulations, and regulatory guidelines, including in Appendices A and B in part 364. Many of the risk management practices established and maintained by a covered institution

A. *Scope.* These Guidelines apply to all insured state nonmember banks, state-licensed insured branches of foreign banks, and insured state savings associations that are subject to the provisions of Section 39 of the FDI Act, with total consolidated assets of $10 billion or more on or after the effective date of these Guidelines (together "covered institutions" and each, a "covered institution"). Total consolidated assets means the covered institution's total assets, as reported on the covered institution's Consolidated Reports of Condition and Income (Call Report)[40] filing, for the two most recent consecutive quarters. An insured state nonmember bank, state-licensed insured branch of a foreign bank, or an insured state savings association that does not come within the scope of these Guidelines on the effective date, but subsequently becomes subject to the Guidelines because total consolidated assets are $10 billion or more after the effective date, as reported on the Call Report for the two most recent consecutive quarters, shall be considered a covered institution and subject to the Guidelines. If a covered institution under the Guidelines reports consolidated assets of less than $10 billion in its Call Report filings for four consecutive quarters, the covered institution will be classified as a non-covered institution beginning the following quarter.

B. *Preservation of Existing Authority*. Neither Section 39 of the FDI Act (12 U.S.C. 1831p-1) nor these Guidelines in any way limits the authority of the FDIC to address unsafe or unsound practices, unsafe or unsound conditions, or violations of law. Action under Section 39 and these Guidelines may be

---

to meet these standards, including loan review and credit underwriting and administration practices, should be components of its risk governance framework, within the construct of the three distinct units identified herein: front line unit, independent risk management unit, and internal audit unit.

[40] For insured branches of foreign banks, the term "Call Report" means the branch's FFIEC 002 filing.

taken independently of, in conjunction with, or in addition to any other enforcement action available to the FDIC.

C. *Reservation of Authority.*

1. Upon notice to the institution, the FDIC reserves the authority to apply these Guidelines, in whole or in part, to an institution that has total consolidated assets less than $10 billion, if the FDIC determines such institution's operations are highly complex or present a heightened risk that warrants the application of these Guidelines.
2. The FDIC reserves the authority, for each covered institution, to extend the time for compliance with these Guidelines or modify these Guidelines as necessary.
3. The FDIC reserves the authority to determine that compliance with these Guidelines should not be, or should no longer be, required for a covered institution. The FDIC would generally make the determination under this paragraph if a covered institution's operations are not or are no longer highly complex or no longer present a heightened risk. In determining whether a covered institution's operations are highly complex or present a heightened risk, the FDIC will consider factors such as: nature, scope, size, scale, concentration, interconnectedness, and mix of the activities of the institution.

D. *Definitions.*

1. *Chief Audit Officer* (CAO) means an individual who leads the covered institution's internal audit unit, possesses the skills and abilities to effectively implement the internal audit program, and reports directly to either the covered institution's board of directors (the board) or the board's audit committee and chief executive officer (CEO).

2. *Chief Risk Officer* (CRO) means an individual who leads a covered institution's independent risk management unit and is experienced in identifying, assessing, and managing risk exposures of large financial firms, with unrestricted access to the board and its committees, and reports directly to the board or the board's risk committee and, solely for administrative matters, the CEO.
3. *Control* means the power, directly or indirectly, to direct the management or policies of a covered institution or to vote 25 percent or more of any class of voting securities of a covered institution.
4. *Corporate governance* means the set of processes, customs, policies, and laws affecting the way a corporation[41] is directed, administered, and controlled and how it manages risks and ensures compliance with laws and regulations, including consumer protection laws and regulations and the Community Reinvestment Act. Corporate governance also includes the relationships among the many stakeholders involved and the corporation's goals.
5. *Front line unit* means any organizational unit within the covered institution that:
    a. Engages in activities designed to generate revenue or reduce expenses for the covered institution;
    b. Provides operational support or servicing to any organizational unit or function within the covered institution for the delivery of products or services to customers;[42] or

[41] As used in these Guidelines, the term "corporate" and "corporation", where appropriate, includes alternative forms of business enterprises, such as limited liability companies.
[42] Notwithstanding the foregoing, "front line unit" does not ordinarily include an organizational unit or function thereof within a covered institution when it is providing solely legal services to the covered institution.

c. Provides technology services to any organizational unit or function covered by these Guidelines.

6. *Independent risk management unit* means any organizational unit within the covered institution that is directed by the CRO and which has responsibility for identifying, measuring, monitoring, or controlling aggregate risks. Such unit maintains independence from front line units through the following reporting structure:

    a. The CRO has unrestricted access to the board of directors and its committees, including the risk committee, to address risks and issues identified through the independent risk management unit's activities;

    b. The board of directors or the risk committee reviews and approves the risk governance framework;

    c. The independent risk management unit adheres to compensation and performance management programs that ensure that the covered institution provides incentives to the independent risk management unit staff that ensure their independence, are consistent with providing an objective assessment of the risks taken by the covered institution, and comply with laws and regulations regarding excessive or incentive compensation, and complies with the covered institution's compensation policies; and

    d. No front line unit executive oversees the independent risk management unit.

7. *Internal audit unit*[43] means the organizational unit within the covered institution that is designated to fulfill the role and responsibilities outlined in part 364, Appendix A, II.B. The internal audit unit should maintain independence from the front line and independent risk management units through the following reporting structure:
    a. The CAO has unrestricted access to the board's audit committee to address risks and issues identified through the internal audit unit's activities;
    b. The board's audit committee, in accordance with Section II.6.a. of these Guidelines, reviews and approves the internal audit unit's charter, audit plans, and decisions regarding appointment, removal, and compensation of the CAO;
    c. The board's audit committee, in accordance with Section II.6.a. of these Guidelines, at least annually or more frequently, as necessary, reviews the internal audit unit's charter, audit plans, and decisions regarding appointment, removal, and compensation of the CAO;
    d. The CEO or the audit committee oversees the internal audit unit's administrative activities; and
    e. No front line unit executive oversees the internal audit unit.
8. *Parent company* means any legal entity that controls the covered institution as defined in these Guidelines.
9. *Risk appetite* means the aggregate level and types of risk the board and management are willing to assume to achieve the covered institution's

[43] *See* 12 CFR part 364, Appendix A - Section II.B.

strategic objectives and business plan, consistent with safe and sound operation and compliance with applicable laws and regulations.

10. *Risk profile* means a point-in-time assessment of the covered institution's risks aggregated within and across each relevant risk category, using methodologies consistent with the risk appetite.

II. CORPORATE GOVERNANCE.

A. *Board of Directors – General Obligations.* The board of directors is ultimately responsible for the affairs of a covered institution. Each member of the board has a duty to safeguard, through the lawful, informed, efficient, and able administration of the covered institution, the interests of the covered institution and to oversee and confirm that the covered institution operates in a safe and sound manner, in compliance with all laws and regulations. The board, in supervising the covered institution, should consider the interests of all its stakeholders, including shareholders, depositors, creditors, customers, regulators, and the public.

1. *Governing laws*. In the exercise of their duties, directors are governed by federal and state banking, securities, and antitrust statutes and by common law (all of which may impose potential liability on all directors). Directors who fail to discharge their duties may be subject to removal from office, criminal prosecution, civil money penalties imposed by covered institution regulators, and civil liability.

B. *Board Composition*. The covered institution's organizational documents or state chartering authority may have requirements for board members, including the appropriate number of members on its board of directors. However, in determining the appropriate number of directors and the board's composition, 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.[44]

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 (for example, directors who own only the amount of stock required by state law or those who share ownership interests with family members, but are not employed by the covered institution).

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.[45]

C. *Duties of the Board.*

1. *Set an Appropriate Tone.* The board should establish a corporate culture and work environment that promotes responsible, ethical behavior. This culture and environment should not condone or encourage imprudent risk-taking, unethical behavior, or violations of law, regulation, or policy in

[44] For example, 12 CFR part 348 implements the Depository Institution Management Interlocks Act. That Act prohibits interlocking relationships of management officials of various nonaffiliated depository institutions, depending on the asset size and geographical proximity of the organizations.

[45] 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.

pursuit of profit or other business objectives, and the board should hold directors, officers, and employees accountable for such conduct. By adhering to the requirements of law, regulation, these Guidelines, and the covered institution's own policies and procedures (including a Code of Ethics and a Compensation and Performance Management Program under these Guidelines), the board's actions should reflect its commitment to integrity, honesty, and ethical conduct.

2. *Approve Strategic Plan for the Covered Institution.* The board is responsible for providing clear objectives within which the covered institution's management can operate and administer the covered institution's affairs. The board should direct the CEO to develop a written strategic plan with input from front-line units, independent risk management, and internal audit. The strategic plan should implement operating budgets and encompass the covered institution's philosophy and mission. At least annually, the board should evaluate and approve the strategic plan, monitor management's efforts to implement the strategic plan and respond to unanticipated external developments, and ensure the strategic plan is consistent with policies the board has approved. The strategic plan should discuss the covered institution's goals and objectives over, at a minimum, a three-year period and:
    a. Articulate an overall mission statement and strategic objectives for the covered institution, including an explanation of how the covered institution will achieve those objectives;
    b. Contain a comprehensive assessment of risks that currently affect the covered institution or that could affect the covered institution during the period covered by the strategic plan;

c. Explain how the covered institution will update, as necessary, its risk management program to account for changes in the covered institution's risks projected under the strategic plan; and

d. Explain how the covered institution will review, update, and approve the strategic plan, as necessary, if the covered institution's risk profile, risk appetite, or operating environment changes in ways not considered in the strategic plan.

3. *Approve Policies*. The board is responsible for establishing and approving the policies that govern and guide the operations of the covered institution in accordance with its risk profile and as required by law and regulation. These policies ensure that the board has a fundamental understanding of the business of banking and the covered institution's associated risks, the risks undertaken by the institution are prudently and properly managed, and the covered institution is operating in a safe and sound manner. Such policies may include, but are not limited to, applicable internal controls, loan and credit policies, asset and liability management, and other operational and managerial standards to fulfill the responsibilities outlined in part 364, Appendix A, II. Such policies should also address other legal requirements, including but not limited to statutes and regulations regarding real estate lending, Anti Money Laundering/Countering the Financing of Terrorism (AML/CFT) compliance, consumer protection laws, anti-fraud, and the Community Reinvestment Act (CRA). Policies should be written and reviewed at least annually to ensure that they remain applicable and up-to-date as the covered institution's risks may change based on internal or external circumstances. Compliance with the covered institution's policies and procedures should be periodically reviewed by

internal audit.

4. *Establish a Code of Ethics.* The board should establish a written code of ethics for the covered institution, covering directors, management, and employees, addressing areas such as:
    a. Conflicts of interest, self-dealing, protection and proper use of covered institution assets, integrity of financial recordkeeping, and compliance with laws and regulations;
    b. How to report illegal or unethical behavior, and forbidding retaliation for such reporting (also known as a whistleblower policy); and
    c. Identifying officials, such as an ethics officer or the covered institution's counsel, employees can contact to seek advice in the event ethical issues arise and to whom and under what circumstances (including those that do not disclose the employee's identity) the ethics officer or counsel must report ethical issues affecting the covered institution to senior management and the board.

    At least annually, the board should review and update, as necessary, the code of ethics.
5. *Provide active oversight of management*. The board should actively oversee the covered institution's activities, including all material risk-taking activities. The board should hold management accountable for adhering to the strategic plan and approved policies and procedures to ensure the covered institution's compliance with safe and sound banking practices and all applicable laws and regulations. In providing active oversight, the board should question, challenge, and when necessary,

oppose recommendations and decisions made by management that are not in accordance with the covered institution's risk appetite, could jeopardize the safety and soundness of the covered institution, or undermine compliance with applicable laws or regulations. The board also must ensure that management corrects deficiencies that auditors or examiners identify in a timely manner.

6. *Exercise independent judgment.* When carrying out his or her duties, each director should exercise sound, independent judgment. 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. Risks inherent in such a situation include, but are not limited to:
    a. A dominant policymaker may inhibit the directors' exercise of independent judgment or prevent the board from fulfilling its responsibilities;
    b. Loss of a dominant officer with concentrated authority may deprive the covered institution of competent management; and
    c. Problems resulting from mismanagement are more difficult to solve because the covered institution's problems are often attributed to the one individual that dominates the covered institution.
7. *Select and Appoint Qualified Executive Officers*. The board must select and appoint executive officers who are qualified to administer the covered institution's affairs effectively and soundly. The selection criteria should include integrity, technical competence, character, and experience in financial services. In addition, the board should implement a formal

appraisal process to periodically review management performance. If any executive officer, including the CEO, is unable to meet reasonable standards of executive ability or ethical standards, the board should dismiss and replace that officer. The board should develop a succession plan to address the possible or eventual loss of the CEO and other key personnel, and at least annually, such plan should be reviewed and updated, as necessary, by the board. The board should also require the covered institution to implement adequate training and personnel activities so that there is continuity of qualified management and competent staff.

8. *Provide Ongoing Training to 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 Guidelines, the board should establish and adhere to a formal, ongoing training program for directors. This program should include training on:
    a. Products, services, lines of business, and risks that have a significant impact on the covered institution;
    b. Laws, regulations, and supervisory requirements applicable to the covered institution; and
    c. Other topics identified by the board.
9. *Self-assessments.* The board should conduct an annual self-assessment evaluating its effectiveness in meeting the standards of these Guidelines.
10. *Compensation and Performance Management Programs.* If not properly structured, incentive compensation arrangements for executive and non-executive employees may pose safety and soundness risks by providing incentives to take imprudent risks that are not consistent with the long-

term health of the organization. Some incentive programs may inadvertently encourage noncompliance with laws or regulations. To avoid these risks, the board should establish, and the covered institution should adhere to compensation and performance management programs that are consistent with applicable laws and regulations and are appropriate to:

a. Ensure the CEO, front line, independent risk management, and internal audit units implement and adhere to, an effective risk management program;
b. Ensure front line unit compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by the independent risk management and internal audit units, even if the covered institution has not or will not realize a loss; and
c. Attract and retain competent staff needed to design, implement, and maintain an effective risk management program.

At least annually, the board should review and update, as necessary, the compensation and performance management programs.

D. *Committees of the Board*. The board should implement an organizational structure to keep members informed and provide an adequate framework to oversee the covered institution. Establishing board committees allows for a division of labor and enables directors with expertise to handle matters that require detailed review and in-depth consideration. In addition, certain laws and regulations or supervisory policies may require the covered institution to establish certain board committees. Each committee should have a board-approved written charter outlining its purpose and responsibilities:

1. *Audit Committee:* The covered institution must have an Audit Committee that complies with Section 36 of the Federal Deposit Insurance Act and part 363 of the FDIC's regulations.[46] The audit committee of a covered institution must be composed entirely of outside and independent directors. The audit committee:
    a. Oversees the covered institution's accounting and financial reporting processes and audits of its financial statements and its internal control over financial reporting;
    b. Approves all audit services; assists board oversight of the integrity of the covered institution's financial statements and disclosures;
    c. Appoints, compensates, and retains any public accounting firm to prepare any audit report and oversees the work of such firms in preparing or issuing any audit report;
    d. Approves all decisions regarding the appointment or removal and annual compensation and salary adjustment for the CAO;
    e. Approves the charter of and oversees the covered institution's internal audit function, including reviewing and approving audit plans and reports of the internal audit function regarding the effectiveness of the risk management program and identified or suspected violations of law or regulations, determining whether and how identified issues are being addressed, and making recommendations, as necessary, to the board for further corrective action;

---

[46] *See* 12 CFR part 363 Annual Independent Audits and Reporting Requirements**;** *see also* part 364, Appendix A - Section II.B. If permitted under Section 36 and part 363 of the FDIC's regulations, the audits of the financial statements and of internal control over financial reporting may be done at the consolidated holding company level and not the covered institution level.

f. At least annually, reviews and updates, as necessary, the charter of the covered institution's internal audit function; and

g. Satisfies all other requirements of law, regulation, and applicable exchange rules.

2. *Compensation Committee:* A covered institution's Compensation Committee must comply with applicable laws and regulations,[47] including the FDIC's regulations.[48] The committee should monitor adherence to a compensation and performance management program, review compensation packages for executives, and consider executive officer performance evaluations. Compensation includes all direct and indirect payments or benefits, both cash and non-cash as defined in part 364, Appendix A, I.B.3. A covered institution is prohibited from paying compensation that constitutes an unsafe and unsound practice (including excessive compensation or compensation that could lead to material financial loss) and should ensure that their incentive compensation arrangements do not encourage imprudent risk-taking behavior or create incentives for violations of legal requirements.

3. *Trust Committee:* If the covered institution has trust powers, it should have a trust committee to ensure that operation of the trust department is separate and apart from every other department of the covered institution, trust assets are separated from assets owned by the covered institution, assets of each trust account are separated from the assets of every other

[47] For example, any covered company that has securities registered with the Securities and Exchange Commission (SEC) must have a compensation committee composed entirely of independent directors, 15 U.S.C 78j–3; 17 CFR parts 229 and 240; *see, e.g.*, NYSE Listed Company Manual Section 303A.04(a), Nasdaq Equity Rule 5605(e), and any other or successor corporate governance rules prescribed by the exchange's governing body.

[48] *See* 12 CFR part 364, Appendix A - Section II.B.

trust account, and the trust department otherwise complies with all applicable laws and regulations.

4. *Risk Committee:* The covered institution must have a risk committee that approves and at least annually reviews and updates, as necessary, the risk management policies of the covered institution's operations and that oversees the operation of the covered institution's risk management framework. The risk committee must:
    a. Be chaired by an independent director;
    b. Be an independent committee of the board that has, as its sole function, responsibility for the risk management policies of the covered institution and oversight of the covered institution's risk management framework;
    c. Report directly to the covered institution's board of directors;
    d. Include at least one member experienced in identifying, assessing, and managing risk exposures of large firms;
    e. Receive and review regular reports on not less than a quarterly basis from the CRO;
    f. Meet at least quarterly, or more frequently as necessary, and fully document and maintain records of its proceedings, including risk management decisions;
    g. Review and approve all decisions regarding the appointment or removal of the CRO, and ensure that the CRO's compensation is consistent with providing an objective assessment of the risks taken by the covered institution.
5. *Other Committees as Required to Perform Duties:* The covered institution should establish other committees, as necessary, in

accordance with its risk profile such as compliance, lending, information technology, cybersecurity, and investments.

At least annually, the board should review and update, as necessary, the written charter for each committee.

III. BOARD AND MANAGEMENT RESPONSIBILITIES REGARDING RISK MANAGEMENT AND AUDIT.

The board of a covered institution 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.

A. *Risk Management Program*. The covered institution should have and adhere to a risk management program that identifies, measures, monitors, and manages risks of the covered institution through a framework appropriate for the current and forecasted risk environment and that meets the minimum standards of these Guidelines. The risk management program 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. The risk management program should ensure that the covered institution's activities are conducted in compliance with applicable laws and regulations. At least annually, the board should review and update, as necessary, the risk management program.

For a covered institution that has a parent company, if the risk profiles of each entity are substantially similar, the covered institution may adopt and implement all or any part of its parent company's risk management program that:

1. Satisfies the minimum standards in these Guidelines;
2. Ensures that the safety and soundness of the covered institution is not jeopardized by decisions made by the parent company's board and management;
3. Ensures that the covered institution's risk profile is easily distinguished and separate from that of its parent for risk management and supervisory reporting purposes; and
4. Consideration of these factors may require the covered institution to have separate and focused governance and risk management practices.

B. *Risk Profile and Risk Appetite Statement*. The covered institution should create and quarterly review and update, as necessary, a risk profile that identifies its current risks. Based upon its risk profile, the covered institution should have a comprehensive written statement, that is reviewed quarterly and updated, as necessary, that establishes risk appetite limits for the covered institution, both in the aggregate and for lines of business and material activities or products. The risk appetite statement should:
   1. Reflect the level of risk that the board and management are willing to accept.
   2. Include both qualitative components and quantitative limits:
      a. The qualitative components should describe a safe and sound risk culture and how the covered institution will assess and accept risks, including those that are difficult to quantify.
      b. Quantitative limits should explicitly constrain the size of risk exposures relative to the covered institution's earnings, capital, and liquidity position that management may accept without board approval.

3. Set limits at levels that take into account appropriate capital and liquidity buffers and that prompt management and the board to reduce risk before the covered institution's risk profile jeopardizes the adequacy of its earnings, liquidity, or capital.

The board should review and approve the 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 covered institution's business model, strategy, risk profile, or market conditions. The covered institution's management, front line units, and independent risk management unit should incorporate the risk appetite statement, concentration risk limits, and front line unit risk limits into:

a. Strategic and annual operating plans;
b. Capital stress testing and planning processes;
c. Liquidity stress testing and planning processes;
d. Product and service risk management processes, including those for approving new and modified products and services;
e. Decisions regarding acquisitions and divestitures; and
f. Compensation and performance management programs.

C. *Risk Management Program Standards.*

1. *Governance.* The independent risk management unit should design a formal, written risk management program that implements the 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 covered institution's risk profile caused by 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.

2. *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. The risk management program should be commensurate with the covered institution's structure, risk profile, complexity, activities, and size and should include:

    a. Policies and procedures establishing risk-management governance, risk management procedures, and risk control infrastructure for its operations; and

    b. Processes and systems for implementing and monitoring compliance with such policies and procedures, including those for:

        i. Identifying and reporting risks (including emerging risks) and risk management deficiencies and ensuring effective and timely implementation of actions to address emerging risks and risk management deficiencies for its operations;

        ii. Identifying and reporting to the Risk Committee and to the internal audit unit known or suspected noncompliance with applicable laws or regulations;

        iii. Establishing managerial and employee responsibility for risk management;

        iv. Ensuring the independence of the risk management

function;

v. Integrating risk management and associated controls with management goals and its compensation structure for operations; and

vi. Identifying, measuring, monitoring, and controlling the covered institution's concentration of risk.

c. Policies, procedures, and processes designed to ensure that the covered institution's risk data aggregation and reporting capabilities are appropriate for its size, complexity, and risk profile and support supervisory reporting requirements. Collectively, these policies, procedures, and processes should provide for:

i. The design, implementation, and maintenance of a data architecture and information technology infrastructure that supports the covered institution's risk aggregation and reporting needs during normal and stressed times;

ii. The capturing and aggregating of risk data and reporting of material risks, concentrations, breaches of risk limits, and emerging risks in a timely manner to the board and the CEO;

iii. The establishment of protocols for when and how to inform board, front line unit management, independent risk management, and the FDIC of a risk limit breach that takes into account the severity of the breach and its impact on the bank, with a requirement to provide a written description of how a breach will be resolved; and

iv. The distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.

3. *Responsibilities.* 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.[49] Monitoring and reporting should be performed, as often as necessary, based on the size and volatility of risks and any material change in the covered institution's business model, strategy, risk profile, or market conditions.

   The responsibilities for each of these units are:

   a. *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 covered institution's risk appetite statement. In fulfilling this responsibility, each front line unit should:

      i. Assess, on an ongoing basis, the material risks associated with its activities and products and use such risk assessments as the basis for fulfilling its responsibilities under this paragraph 3(a) and for determining needed actions to strengthen risk

[49] These roles and responsibilities are in addition to any roles and responsibilities set forth in Appendices A and B to part 364.

management or reduce risk because of changes in the unit's risk profile, products, or other conditions.

ii. Establish and adhere to a set of written policies that include front line unit risk limits as approved by the board. Such policies should ensure risks associated with the front line unit's activities are effectively identified, measured, monitored, and controlled, consistent with the covered institution's risk appetite statement, concentration risk limits, and all policies established within the risk management program.

iii. Establish and adhere to procedures and processes, as necessary, to ensure compliance with board policies, including risk policies and applicable laws and regulations, and at least annually, update, as necessary, such procedures and processes.

iv. Adhere to all applicable policies, procedures, and processes established by independent risk management.

v. Monitor compliance with their respective risk limits and report at least quarterly to the independent risk management unit.

vi. Develop, attract, train, retain, and maintain competent staff at levels required to carry out the unit's role and responsibilities effectively.

vii. Adhere to compensation and performance management programs that comply with laws and regulations regarding excessive or incentive compensation and

covered institution compensation policies.

At least annually, each front line should review and update, as necessary, the written policies that include risk limits.

b. *Independent Risk Management Unit.* Under the direction of the CRO, the independent risk management staff should oversee the covered institution's risk-taking activities and assess risks and issues independent of the CEO and front line units. In fulfilling these responsibilities, independent risk management should:

   i. Take primary responsibility and be held accountable by the CEO and the board for designing a comprehensive written risk management program that meets these Guidelines.

   ii. Identify and assess, on an ongoing basis, the covered institution's material risks, in the aggregate and for lines of business and material activities or products, and use such risk assessments as the basis for fulfilling its responsibilities under these Guidelines and for determining needed actions to strengthen risk management or reduce risk given changes in the covered institution's risk profile, products, or other conditions.

   iii. Monitor the covered institution's risk profile relative to the covered institution's risk appetite and compliance with concentration risk limits and report on such monitoring to the Risk Committee at least quarterly.

   iv. Establish and adhere to policies that include concentration risk limits. Such policies should ensure that risks, both in the aggregate and for lines of business and material

activities or products, within the covered institution are effectively identified, measured, monitored, and controlled, and are consistent with the covered institution's risk appetite statement and all policies and processes established within the risk management program. At least annually, such policies should be reviewed and updated, as necessary.

v. Establish and adhere to procedures and processes, as necessary, to ensure compliance with the board risk management policies and with applicable laws and regulations. At least annually, such procedures and processes should be reviewed and updated, as necessary.

vi. Ensure that front line units meet the standards in paragraph 3(a).

vii. When necessary due to the level and type of risk, monitor front line units' compliance with front line unit risk limits, engage in ongoing communication with front line units regarding adherence to these limits, and report at least quarterly any concerns to the CEO and the Risk Committee.

viii. Identify and communicate to the CEO and the Risk Committee:

    a. Material risks and significant instances where independent risk management's assessment of risk differs from that of a front line unit;

    b. Significant instances where a front line unit is not adhering to the risk governance program;

and

c. Identified or suspected instances of noncompliance with laws or regulations.

ix. Identify and communicate to the Risk Committee:

a. Material risks and significant instances where independent risk management's assessment of risk differs from the CEO's assessment; and

b. Significant instances where the CEO is not adhering to, or holding front line units accountable for adhering to, the risk governance program.

x. Develop, attract, train, retain, and maintain competent staff at levels required to carry out the unit's role and responsibilities effectively.

xi. Adhere to compensation and performance management programs that ensure that the covered institution provides compensation and other incentives to the independent risk management unit staff that ensure their independence, are consistent with providing an objective assessment of the risks taken by the covered institution, and comply with applicable laws and regulations regarding excessive or incentive compensation, and covered institution compensation policies.

c. *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 covered institution's risk

management program complies with these Guidelines and is appropriate for the size, complexity, and risk profile of the covered institution. In carrying out its responsibilities the internal audit unit should:

i. Maintain a complete and current inventory of all of the covered institution's material businesses, product lines, services, and functions, and assess the risks associated with each, which collectively provide a basis for the audit plan required in paragraph 3(c)(ii).

ii. Establish and adhere to an audit plan, updated quarterly or more often, as necessary, that takes into account the covered institution's risk profile and emerging risks and issues. The audit plan should require the internal audit unit to evaluate the adequacy of and compliance with policies, procedures, and processes established by front line units and the independent risk management unit under the risk management program. Changes to the audit plan should be communicated to the Audit Committee as they occur.

iii. Report in writing, conclusions, issues, recommendations, and management's response from audit work carried out under the audit plan described in paragraph 3(c)(ii) to the Audit Committee. The internal audit unit's reports to the Audit Committee should identify the root cause of any investigated issue and include:

    1. A determination of whether the root cause creates an issue that has an impact on one

organizational unit or multiple organizational units within the covered institution; and

2. A determination of the effectiveness of the front line units and the independent risk management unit in identifying and resolving issues in a timely manner.

iv. 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. The assessment should include a conclusion regarding the covered institution's compliance with the standards set forth in these Guidelines.

v. 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.

vi. Establish and adhere to a quality assurance process that ensures internal audit's policies, procedures, and processes comply with applicable regulatory and industry guidance, are appropriate for the size, complexity, and risk profile of the covered institution, are updated to reflect changes to internal and external risk factors, and are consistently

followed.

vii. Develop, attract, train, retain, and maintain competent staff at levels required to carry out the unit's role and responsibilities effectively.

viii. Adhere to compensation and performance management programs that comply with applicable laws and regulations regarding excessive or incentive compensation and covered institution compensation policies.

D. *Communication Processes.* The risk management program should require that the covered institution initially communicate and provide ongoing communication and reinforcement of the covered institution's risk appetite statement and risk management program throughout the covered institution in a manner that ensures management and all employees align their risk-taking decisions with applicable aspects of the risk appetite statement.

E. *Processes Governing Risk Limit Breaches.*

The board should establish, and the covered institution should adhere to, processes that require front line units and the independent risk management unit, consistent with their respective responsibilities to:

1. Identify breaches of the risk appetite statement, concentration risk limits, and front line unit risk limits.
2. Distinguish breaches based on the severity of their impact on the covered institution.
3. 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 covered institution, and how the breach will be, or has been, resolved.

4. 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 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.

F. *Processes Governing Identification of and Response to Violations of Law or Regulations.*

The board should establish, and the covered institution should adhere to, processes[50] that require front line units and the independent risk management unit, consistent with their respective responsibilities to:

1. Identify known or suspected violations of law or regulations applicable to the activities conducted by their units.
2. Distinguish between violations of law or regulations that appear largely technical, inadvertent, or insignificant and those that appear willful or may involve dishonesty or misrepresentation.
3. Document all violations of law or regulations in writing and notify the CEO, Audit Committee, and the Risk Committee, including information about actions that are being taken to return the institution to compliance with the applicable law or regulatory requirement.
4. Ensure that known or suspected violations of law involving dishonesty,

[50] The covered institution may seek legal advice (from in-house or outside legal advisors) regarding any breach, including known or suspected violation of law, but the covered institution's policies and processes should state that seeking legal advice does not abrogate the requirement to report any breach.

misrepresentation or willful disregard for requirements, whether by a customer or by any covered institution's director, manager, employee, or person or entity performing services for the covered entity, are promptly reported as required by law or regulation[51] and to relevant law enforcement and federal and state agencies, and take prompt action to cease such activity and prevent its recurrence.

5. Report all violations of law or regulation in a manner and on a timetable acceptable to the agency with jurisdiction over that law or regulation and establish accountability for resolving violations, even if the covered institution did not realize a loss from such violations.

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.

Federal Deposit Insurance Corporation.

By order of the Board of Directors.

Dated at Washington, DC, on October 3, 2023.

James P. Sheesley,

Assistant Executive Secretary.

BILLING CODE 6714-01-P

[FR Doc. 2023-22421 Filed: 10/10/2023 8:45 am; Publication Date: 10/11/2023]

[51] *See, e.g.*, 12 CFR part 353.