New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 252—NO. 78
WEDNESDAY, OCTOBER 22, 2014

BANKING

Expert Analysis

Guidelines Establish Heightened Standards for Banks and Boards

By **Michael T. Escue**

On Sept. 2, 2014, the Office of the Comptroller of the Currency (OCC) finalized its "guidelines" to establish minimum standards for the design and implementation of risk governance frameworks by certain large banks and minimum standards for the boards of directors of those banks in overseeing the frameworks' design and implementation.[1]

The guidelines differ in certain important respects from the proposed guidelines published in a Notice of Proposed Rulemaking in January 2014,[2] (proposed guidelines) some of which are discussed below.

Following the financial crisis, the OCC developed a set of five "heightened expectations" intended to enhance the OCC's supervision and strengthen the governance and risk management practices of large national banks and to enhance the agency's supervision of those institutions. The OCC began communicating these heightened expectations informally to banks in the Large Bank program in 2010 and began examining banks for compliance in 2012. The guidelines state that they "will supersede the current heightened expectations program" and that prior informal guidance regarding the heightened expectations program will no longer be used to evaluate covered banks.

The guidelines apply to insured national banks, insured federal savings associations and insured federal branches of foreign banks with average total consolidated assets of $50 billion or more, as well as potentially smaller depository institutions.[3] The guidelines establish specific risk management-related roles and responsibilities for three designated functions: a bank's "front line" units, independent risk management and internal audit. The guidelines also impose substantial risk management-related and other responsibilities on the bank's board of directors as well as on the bank's CEO.

Risk Governance Framework

The guidelines require banks to establish and adhere to a formal, written risk governance framework, approved by the board (or the board's risk committee), which would encompass risks to the bank that arise from all its activities. Under the guidelines, a bank may theoretically use its parent's risk governance framework but only if that framework meets the minimum standards of the guidelines and the risk profiles of the bank and its parent are "substantially the same."[4] The framework would be implemented through the three-function process (i.e., front line units, independent risk management and internal audit) described below. The framework should cover eight categories of risk, which are described in existing OCC guidance: credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk and reputation risk.

Risk Appetite Statement

The guidelines define "risk appetite" as the aggregate level and types of risk the board and management are willing to assume to achieve the bank's strategic objectives and business plan, consistent with regulatory requirements. The bank's risk appetite statement should include both qualitative components, including a description of a safe and sound risk culture, and quantitative limits that include, as appropriate, stress testing processes described in the May 2012 interagency guidance on stress testing. If the bank's and its parent's risk profiles are substantially the same, the bank's board may tailor the parent's risk appetite statement to apply to the bank and document any needed adjustments or material differences between the risk profiles of the bank and its parent.

Risk-Related Roles

Fundamental to the design and implementation of the framework are the specific risk-related roles and responsibilities imposed by the guidelines on three functions: front line units, independent risk management and internal audit. The guidelines also impose some specific requirements on the CEO. Many of the roles and responsibilities are distinct to each function, although some are shared across multiple functions. Independent risk management and internal audit are required to have unfettered access to the board and to be afforded the stature within the bank needed to effectively carry out their respective roles and responsibilities.

> The guidelines establish specific risk management-related roles and responsibilities for three designated functions: a bank's 'front line' units, independent risk management and internal audit.

Front Line Units. Under the guidelines, a "front line unit" is broadly defined as any unit that (i) engages in activities designed to generate revenue or reduce expenses for the bank or its parent, (ii) provides operational support or servicing to any organizational unit or function within the bank in the delivery of products or services to customers or (iii) provides technology services to any organizational unit or function covered by the guidelines. The guidelines modified the definition of "front line unit" contained in the proposed guidelines in several respects, including by expanding the first prong of the

MICHAEL T. ESCUE *is a partner in the financial services group of Sullivan & Cromwell.* TAYLOR C. AUTEN, *an associate at the firm, assisted with the preparation of this article.*

definition to include units engaged in expense reduction activities and clarifying that certain support functions, such as human resources and legal, would ordinarily not be considered front line units. Each front line unit must assess, on an ongoing basis, material risks associated with its activities and implement policies that address unit risk limits and ensure that risks associated with the unit's activities are effectively identified, measured, monitored and controlled, consistent with the bank's risk appetite statement, concentration risk limits and policies established under the framework.

Independent Risk Management. The guidelines define "independent risk management" as the unit within the bank that is responsible for identifying, measuring, monitoring and controlling aggregate risks, independent of the front line units. The final guidelines clarify that independent risk management may be led by a single Chief Risk Executive (CRE) or multiple CREs, who must report directly to the CEO and who should have unrestricted access to the board and its committees with regards to risks and issues identified.

Independent risk management is expected to identify and assess, on an ongoing basis, the bank's material aggregate risks and use those risk assessments as the basis for enterprise risk policies that address concentration risk limits and state how aggregate risks are effectively identified, measured, monitored and controlled, consistent with the bank's risk appetite statement, concentration risk limits and policies and processes established within the framework.

Independent risk management is also responsible for identifying material risks and significant instances in which independent risk management's assessment of risk differs from that of a front line unit or the CEO, there is a failure to adhere to the framework or the CEO is not holding front line units accountable for adhering to the framework. Where independent risk management identifies such material risks or significant instances, it is to communicate them to the board or CEO as specified in the guidelines.

Internal Audit. Internal audit is responsible for ensuring that a bank's framework complies with the guidelines. It must be led by the Chief Audit Executive (CAE), who must be one level below the CEO in the bank's organizational structure. Internal audit is expected to maintain a complete and current inventory of the bank's material processes, product lines, services and functions and to assess and rate the risks, including emerging risks, associated with each. These risk assessments and ratings are to provide a basis for an audit plan that takes into account the bank's risk profile and emerging risks and requires internal audit to evaluate the adequacy of and compliance with policies, procedures and processes established by front line units and independent risk management under the framework.

Internal audit is further tasked with identifying and communicating to the board's audit committee significant instances in which front line units or independent risk management are not adhering to the framework. The CAE should have unrestricted access to the board's audit committee with regard to risks and issues identified.

> The guidelines define 'independent risk management' as the unit within the bank that is responsible for identifying, measuring, monitoring and controlling aggregate risks, independent of the front line units.

CEO. Under the guidelines, the CEO is responsible for the development of, with input from the three functions described above, a minimum three-year strategic plan that includes a comprehensive assessment of risks to the bank, currently and during the time period covered by the plan, and an explanation of how the bank will update the framework to account for changes in the bank's risk profile as projected under the strategic plan. The strategic plan must be approved by the board and reviewed, updated and approved to reflect changes in the bank's risk profile or operating environment. The CEO is also required to oversee the CRE in a manner similar to the oversight the CEO provides to her or his other direct reports. The CEO, or the board's audit committee, must also oversee the CAE's administrative activities, such as routine personnel matters, expense account management and other departmental matters.[5]

Board of Directors

The guidelines impose a number of new requirements relating to the composition of the board of directors and the responsibilities of the board and individual directors. These include the following:

• At least two members of a bank's board must be "independent."[6]

• The board's basic duty of oversight is described as the requirement for the board to "actively" oversee the bank's risk-taking activities and hold management accountable for adhering to the framework, including by questioning, challenging and opposing management decisions that could cause the bank's risk profile to exceed its risk appetite or jeopardize the safety and soundness of the bank.

• The board must "require" management to establish and implement an effective framework. The board must also approve significant changes to the framework.

• The final guidelines impose specific requirements on the board with respect to talent development, recruitment and succession planning, with certain modifications from the proposed guidelines designed to reduce the operational burdens on the board. The board is required to appoint a CEO and to appoint or approve the appointment of a CAE and one or more CREs. The board should review and approve a written talent management program, require management to assign individuals specific responsibilities within the talent management program and hold those individuals accountable for the program's effectiveness.

• The board is expected to conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting the minimum standards.

• The final guidelines modified the proposed guidelines to require that a formal training program apply to all directors (rather than just independent directors) and that the program should consider the directors' knowledge and experience and the bank's risk profile. The formal training program should include training on (1) complex products, services, lines of business and risks that have a significant impact on the bank and (2) laws, regulations and supervisory requirements applicable to the bank.

1. 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. 54,518 (Sept. 11, 2014).

2. 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. 4282 (Jan. 27, 2014).

3. The guidelines also apply to any bank with less than $50 billion in total consolidated assets when such bank's parent company controls at least one covered bank. Moreover, the OCC reserved its authority to apply the guidelines to a bank whose average total consolidated assets are less than $50 billion "if the OCC determines that such bank's operations are highly complex or otherwise present a heightened risk as to require compliance with the Guidelines." The guidelines state that this reserved authority is expected to be used only in "extraordinary circumstances."

4. Substantial similarity under the guidelines requires that a bank's average total consolidated assets represent 95 percent or more of the parent company's average total consolidated assets.

5. The final guidelines modified the proposed guidelines to clarify that the CEO is not expected to oversee the "day-to-day" activities of the CRE or CAE.

6. The final guidelines' independence rules require that at least two members of the board (1) are not, and have not been within the last three years, an officer or employee of the bank or its parent company, (2) are not a member of the immediate family (as defined in 12 C.F.R. §225.41(b)(3)) of a person who is, or has been within the last three years, an executive officer of the bank or its parent company and (3) qualify as an independent director under the listing standards of a national securities exchange, as demonstrated to the satisfaction of the OCC.