OCC Releases Guidelines for Heightened Expectations for Bank Risk Governance

September 8, 2014

On September 2, 2014, the Office of the Comptroller of the Currency (the "OCC") issued final guidelines (the "Guidelines") establishing risk management standards for large national banks, insured federal savings associations, and insured federal branches of foreign banks (each, a "bank").[1] The Guidelines formalize and make enforceable five "heightened expectations" that the OCC developed and began communicating to large banks informally following the financial crisis, and which were eventually proposed as enforceable guidelines in January 2014. The five heightened expectations are:

- for the board of directors of a bank to preserve the "sanctity of the charter" by ensuring that the bank operates in a safe and sound manner rather than simply as an extension of its parent bank holding company and other group affiliates;
- to have a well-defined personnel management program that ensures appropriate staffing levels, provides for orderly succession, and provides for compensation tools to appropriately motivate and retain talent that does not encourage imprudent risk taking;
- to define and communicate an acceptable risk appetite across the organization;
- to have reliable oversight programs, including the development and maintenance of strong audit and risk management functions; and
- for the board to be willing to provide credible challenges to management's decision-making.

The Guidelines implement these standards by requiring banks to adopt a written risk governance framework to manage their risks in compliance with various substantive, procedural, and organizational structure requirements, and by imposing certain standards on their boards, including a requirement that two directors be independent of both the bank and its holding company.

SCOPE OF APPLICATION

Generally, the Guidelines apply to any bank (i) with average total consolidated assets of $50 billion or more, or (ii) whose parent company controls[2] a bank with average total consolidated assets of $50 billion or more (each, a "Covered Bank").

---

[1] The Guidelines will be included in a new Appendix D to the OCC's Part 30 regulations (12 C.F.R. Part 30, Appendix D).

[2] The term "parent company" means the top-tier legal entity in a bank's ownership structure. A parent company "controls" a bank if it owns or controls 25% or more of a class of voting securities of the bank or consolidates the bank for financial reporting purposes.

Notably, the Guidelines also reserve the OCC's right to apply the Guidelines to a bank whose average total consolidated assets do not meet the $50 billion threshold if the OCC determines such bank's operations are highly complex or otherwise present a heightened risk, based on the bank's complexity of products and services, risk profile, and scope of operations. In the preamble to the Guidelines, the OCC noted that this authority will only be used in "extraordinary circumstances," and is not intended to be used to apply the Guidelines to community banks.

COMPLIANCE DATES

The Guidelines phase in the date for compliance based on a bank's size:

- a Covered Bank with average total consolidated assets of $750 billion or more should comply with the Guidelines on November 10, 2014
- a Covered Bank with average total consolidated assets of $100 billion or more but less than $750 billion should comply by May 10, 2015
- a Covered Bank with average total consolidated assets of $50 billion or more but less than $100 billion should comply by May 10, 2016
- a Covered Bank with average total consolidated assets of less than $50 billion that is subject to the Guidelines by virtue of being a subsidiary of a parent company that controls another Covered Bank should comply with the Guidelines on the same date that the affiliated Covered Bank should comply
- a bank with average total consolidated assets of less than $50 billion on the effective date that subsequently becomes subject to the Guidelines should comply within 18 months of the as-of date of the most recent Call Report used to calculate the average

Once a Covered Bank is subject to the Guidelines, it would be required to comply with the Guidelines even if its average total consolidated assets were subsequently to fall below $50 billion, unless the OCC determines otherwise.

RISK GOVERNANCE FRAMEWORK

Under the Guidelines, a Covered Bank must establish and implement a written risk governance framework ("Framework") that manages and controls the Covered Bank's credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk, and reputation risk.

A. Governance Structure

The Framework should include three distinct units: front line units, independent risk management, and internal audit.

1. ***Front Line Units***

Front line units are broadly defined to include any organizational unit that is "accountable" for one of the risks enumerated above (whether or not it created the risk) *and* that also meets one of three additional criteria:

- engages in activities designed to generate revenue or reduce expenses for the parent company or Covered Bank,
- provides operational support or servicing to any organizational unit or function within the Covered Bank for the delivery of products or services to customers, or
- provides technological services to any organizational unit or function covered by the Guidelines.

Accountability for risks is a dynamic concept, and the preamble makes clear that accountability can arise once a unit has inherited or taken over a risk from another unit, such as when responsibility for a particular loan portfolio shifts from one unit to another. The organizational unit or function that assumes responsibility for the loan portfolio becomes a front line unit at the time accountability for the risk is transferred.

The Guidelines confirm that an entire organizational unit or just part of it can be a front line unit depending on the facts and circumstances. An example the OCC provides involves the CFO's organizational unit: such unit may be a front line unit with respect to its responsibility to set goals and provide oversight for enterprise-wide expense reduction initiatives (which have the potential to create risks if actions taken to achieve cost-saving goals inappropriately weaken risk management practices or internal controls), but not with respect to customary responsibilities, such as receiving reports from other units and preparing financial statements.

The final Guidelines contain a number of important changes from the proposed Guidelines. The first additional criterion has been expanded to include not only revenue-generating activities but also activities related to expense reduction. For the second criterion, the proposed Guidelines specifically included administration, finance, treasury, legal, and human resources services as front line units. The final Guidelines do not. Indeed, the Guidelines contain an explicit acknowledgment that a front line unit "does not ordinarily include" an organizational unit or function that provides legal services to the Covered Bank. Finally, the third criterion has been narrowed to include only "technology services," and no longer includes far-reaching references to "processing" and "other support."

Each front line unit should take responsibility and be held accountable by the CEO and the board of the Covered Bank for assessing and managing all of the risks associated with their activities. This requires each front line unit, either alone or in conjunction with another organizational unit that has the purpose of assisting the front line unit, to establish and adhere to written policies, procedures and processes to manage risk consistent with the Covered Bank's risk appetite statement. Front line units must also report to independent risk management at least quarterly on their risk limits.

2. *Independent Risk Management*

Independent risk management includes any organizational unit that has responsibility for identifying, measuring, monitoring, or controlling aggregate risks. Independent risk management should oversee the Covered Bank's risk-taking activities and assess risk independent of the CEO and front line units. This requires, among other things:

- taking primary responsibility and being held responsible by the CEO and the board for designing a comprehensive written risk governance framework;
- identifying and assessing, on an ongoing basis, the Covered Bank's material aggregate risks and using such assessments to determine if actions need to be taken to strengthen risk management or reduce risk;
- establishing and adhering to enterprise policies, procedures, and processes to manage concentration risk limits;
- ensuring that front line units meet their risk management responsibilities;
- identifying and communicating to the CEO and the board significant instances in which independent risk management's assessment of risk differs from that of a front line unit, and in which a front line unit is not adhering to the Framework;
- review and report to the board or its risk committee at least quarterly on the Covered Bank's risk profile in relation to its risk appetite statement and compliance with concentration limits (as discussed below); and
- identifying and communicating to the board significant instances in which independent risk management's assessment of risk differs from the CEO, and in which the CEO is not adhering to, or holding front line units accountable for adhering to, the Framework.

One or more chief risk executives ("CRE") are required to lead the independent risk management unit and must be one level below the CEO in the Covered Bank's organizational structure, but unlike the proposed Guidelines, the final Guidelines do not require the CEO to oversee the day-to-day activities of CAEs. Each CRE should have unrestricted access to the board and its committees to address risks and issues identified by the independent risk management unit.

3. *Internal Audit*

Internal audit is the organizational unit of a Covered Bank that is designated to oversee the internal audit system set forth in the interagency standards for safety and soundness of the OCC, the Federal Reserve Board, and the FDIC. In addition to overseeing this system, internal audit should ensure that the Framework complies with the Guidelines and is appropriate for the size, complexity, and risk profile of the Covered Bank. This requires the internal audit unit to:

- establish and adhere to an audit plan that is periodically reviewed and updated and that takes into account the Covered Bank's risk profile, emerging risks, and issues, and establishes the frequency with which activities should be audited;

- maintain a current inventory of all the Covered Bank's material processes, product lines, and services, and assess the risks (including emerging risks) associated with each, which will provide a basis for the audit plan;
- report to the audit committee of the board in writing its conclusions, issues, and recommendations from work carried out under the audit plan, including (i) a determination of whether any issue will have an impact on one or multiple organizations within the Covered Bank and (ii) a determination of the effectiveness of front line units and independent risk management in responding to any identified issues;
- establish and adhere to processes for independently assessing the ongoing effectiveness of the Framework at least annually;
- identify and communicate to the audit committee significant instances in which front line units or independent risk management are not adhering to the Framework; and
- establish a quality assurance program that ensures the internal audit's policies, procedures, and processes (i) comply with applicable regulatory and industry guidance; (ii) are updated to reflect changes to internal and external risk factors, emerging risks, and improvement in industry internal audit practices; and (iii) are consistently followed.

A chief audit executive ("CAE") leads the internal audit unit and must be one level below the CEO in the Covered Bank's organizational structure. The CEO oversees the CAE's administrative activities, but unlike the proposed Guidelines, the final Guidelines do not require the CEO to oversee the day-to-day activities of the CAE. The CAE should have unrestricted access to the board and its committees to address risks and issues identified through independent audit's activities.

Independent risk management and internal audit units must be structurally independent from front line units. No front line unit executive may oversee independent risk management or internal audit units. The board or its risk committee should oversee independent risk management's Framework and all decisions regarding the appointment, removal, annual compensation, and salary adjustment of the CRE. The audit committee should oversee internal audit's charter and audit plans and all decisions regarding the CAE.

Each of these units may engage the services of, but may not delegate their risk management responsibilities to, external experts.

B. Strategic Plan

The Guidelines provide that the CEO—with input from the front line, independent risk management, and internal audit units—should be responsible for the development of a written strategic plan that contains a comprehensive assessment of risks that currently impact the Covered Bank or could impact the Covered Bank, an overall mission statement and strategic objectives for the Covered Bank, and an explanation of how the Covered Bank will achieve the objectives. The risk assessment should cover at least three years and should be updated as necessary due to any changes in the Covered Bank's risk profile or operating environment. At

least annually, the board should evaluate and approve the strategic plan and monitor management's efforts to implement it.

C. Risk Appetite Statement and Risk Limits

A Covered Bank should have a written statement articulating its risk appetite, meaning the aggregate level and types of risk that its board and management are willing to assume to achieve the Covered Bank's strategic objectives and business plan, consistent with applicable capital, liquidity, and other regulatory requirements. The risk appetite statement should have both qualitative components—that describe a safe and sound "risk culture" and articulate core values to guide risk-taking decisions—and quantitative limits—that incorporate sound stress testing processes, as appropriate, and address the Covered Bank's earnings, capital, and liquidity. The risk appetite statement should be communicated and reinforced throughout the Covered Bank.

The Framework should include concentration risk limits for the Covered Bank and, as applicable, front line risk units for the relevant risks of each front line unit. When aggregated across all units, the risks should not exceed the limits set forth in the risk appetite statement. Concentration risk limits should be accompanied by policies and processes to identify, measure, monitor, and control the Covered Bank's concentration of risk, and policies and processes designed to provide that the Covered Bank's risk data aggregation and reporting capabilities, including its information technology infrastructure, are appropriate for its size and risk profile.

A Covered Bank should establish escalation processes that require front line units and independent risk management to identify breaches of the various risk limits and inform the board, front line management, independent risk management, internal audit and/or the OCC, depending on the severity of the breach. A Covered Bank should also establish resolution processes that describe in writing how a breach will be resolved, taking into account the magnitude, frequency, and recurrence of breaches.

The risk appetite statement, concentration risk limits, and front line unit risk limits should be incorporated into the Covered Bank's other processes, including decisions regarding compensation, acquisitions and divestitures, and capital stress testing and liquidity stress testing matters.

D. Staffing Levels, Talent Management and Compensation

The Guidelines include a number of requirements relating to a Covered Bank's employment decisions. Front line units, independent risk management, and internal audit must develop, attract, and retain talent and maintain staffing levels required to carry out properly each unit's risk management responsibilities. Additionally, the Covered Bank must establish and adhere to processes for talent development, recruitment, and succession planning to ensure that employees who are responsible for or influence material risk decisions have the knowledge, skill, and abilities to effectively manage relevant risks. The board or an appropriate board committee should:

- appoint a CEO and appoint or approve the appointment of the CAE and one or more CREs with the skills and abilities to carry out their roles and responsibilities within the Framework;
- review and approve a written talent management program that provides for development, recruitment, and succession planning regarding the CEO, CAE, and CREs; and
- require management to assign individuals specific responsibilities within the talent management program, and hold those individuals accountable for the program's effectiveness.

As noted above, the Covered Bank's risk limits should be incorporated into its compensation performance decisions. Additionally, compensation programs should prohibit any incentive-based payment arrangement that encourages inappropriate risks by providing excessive compensation or that could lead to material financial loss.

E. Approval and Other Considerations

A Covered Bank's board or its risk committee must review and approve its Framework and, at least annually, its risk appetite statement. The board or its risk committee should approve any significant changes to the Framework and monitor compliance with the Framework. Independent risk management must review, and at least annually update, the Framework.

Other than in limited circumstances, a Covered Bank must develop its own Framework independent of that of its parent company. However, the OCC clarified in the preamble that a Covered Bank may use components of its parent company's Framework as long as the Covered Bank determines, upon consultation with OCC examiners, that the Framework complies with the Guidelines. The preamble encourages Covered Banks to leverage appropriate components of their parent company's Frameworks to the extent appropriate, such as having the same individual serve as the CRE or CAE of both entities.

A Covered Bank may use all of its parent company's Framework if such Framework complies with the Guidelines and the Covered Bank can annually document that its risk profile and its parent company's risk profile are "substantially the same," meaning that the Covered Bank's average total consolidated assets (as reported on the Covered Bank's Call Report for the four most recent quarters) represent 95% or more of the parent company's average total consolidated assets (as reported on the parent company's Form FR Y-9C for the four most recent quarters). A Covered Bank that does not satisfy this test can submit to the OCC an analysis that otherwise demonstrates that the Covered Bank's risk profile is substantially the same as that of its parent company. If the Covered Bank uses its parent company's Framework, it may tailor the parent company's risk appetite statement to the Covered Bank, as appropriate, and the board must document any material differences between the risk profiles of the parent company and the Covered Bank.

STANDARDS FOR BOARD OF DIRECTORS

The Guidelines impose a number of governance standards on a Covered Bank's board. Most significantly, the Guidelines require that at least two directors be independent, meaning that they:

- are not, and have not been in the last three years, an officer or employee of the parent company or Covered Bank;
- are not a member of the "immediate family" (as defined in Section 225.41(b)(3) of Regulation Y) of a person who is, or has been within the last three years, an "executive officer" (as defined in Section 215.2(e)(1) of Regulation O) of the parent company or Covered Bank; and
- qualify as independent directors under the listing standards of a national securities exchange, as demonstrated to the OCC's satisfaction.

The board should establish and adhere to an ongoing training program for all directors, considering their knowledge and experience and the Covered Bank's risk profile. This program should cover (i) complex products, services, lines of business, and risks that have a significant impact on the Covered Bank; (ii) laws, regulations, and supervisory requirements applicable to the Covered Bank; and (iii) other topics identified by the board.

The Guidelines require the board to actively oversee the Covered Bank's risk-taking activities and hold management accountable for adhering to the Framework. Active oversight includes questioning, challenging, and when necessary, opposing recommendations and decisions made by management that could cause the Covered Bank's risk profile to exceed its risk appetite or jeopardize the Covered Bank's safety and soundness. The board may rely on risk assessments and reports prepared by independent risk management and internal audit to support its active oversight role. In the preamble to the Guidelines, the OCC stated that the board should take action to hold appropriate parties accountable when management is not adhering to the Framework.

The board should conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting these standards. In the preamble, the OCC stated that any opportunities for improvement identified in self-assessments should lead to specific changes, including, for example, changing the board composition and structure, meeting frequency and agenda items, board report design or content, ongoing training program design or content, and other process and procedure topics.

Because federal branches of foreign banks do not have a U.S. board and their risk governance frameworks may vary depending on the activities taking place in the branches, the OCC will consult with the branches to adapt the guidelines in a flexible and appropriate manner to the branches' operations. OCC examiners will also consult with branches to determine the appropriate person or committee to undertake the responsibilities assigned to the board under the Guidelines.

ENFORCEMENT

The Guidelines are promulgated pursuant to Section 39 of the Federal Deposit Insurance Act, which authorizes the OCC to issue and enforce safety and soundness standards by regulations or guidelines. If the OCC were to determine, by examination or otherwise, that a Covered Bank failed to meet the standards set forth in the Guidelines, the OCC retains *discretion* whether to require the Covered Bank to submit a remedial plan specifying the steps the Covered Bank will take to comply with the standards, or to require other self-corrective or remedial measures (by contrast, if the Guidelines were formulated as regulations, the OCC *must* require a Covered Bank to submit a remedial plan).

If a Covered Bank did not comply with a required remedial plan, the OCC could initiate a public enforcement order, which would be enforceable in federal court and could result in civil monetary penalties to the Covered Bank.

OBSERVATIONS

The Guidelines are significant because they are part of a larger trend, following the enactment of the Dodd-Frank Act, by the U.S. federal banking agencies to more intensely scrutinize the risk management practices and procedures of large banking organizations. Below are some key observations:

- Identifying front line units will be an arduous initial task for Covered Banks. While the final Guidelines narrow the "front line unit" definition that had been in the proposed Guidelines (and which would have picked up nearly every conceivable unit of a Covered Bank), they will require a factual (and ongoing) analysis of nearly every business unit in the Covered Bank, including operational functions within business units.

- Many aspects of the Guidelines are already reflected in the practices of large national banks, but the Guidelines are nevertheless important in that examiners will have substantial discretion to assess compliance and identify specific weaknesses, including in Covered Banks' exam reports.

- The OCC expects a Covered Bank's board to credibly challenge the recommendations and decisions of management. This is somewhat reminiscent of the Federal Reserve Board's guidance on capital planning from August 2013, which noted that large bank holding companies with "stronger documentation practices had board minutes that described how [capital planning] decisions were made and what information was used," and "provided evidence that the board challenged results and recommendations."[3] Although the OCC's Guidelines do not include any specific documentation requirements, Covered Banks will need to consider how to demonstrate to examiners

[3] Federal Reserve Board, "Capital Planning at Large Bank Holding Companies: Supervisory Expectations and Range of Current Practice" (August 2013), *available at* http://www.federalreserve.gov/bankinforeg/bcreg20130819a1.pdf.

that their boards questioned and challenged management. In the preamble to the Guidelines, the OCC indicated that it "does not expect the board of directors to evidence opposition to management during each board meeting," but "only when necessary."

- The Guidelines provide that directors should oversee the Covered Bank's compliance with safe and sound banking practices. Unlike the proposed Guidelines, the final Guidelines do not frame this responsibility in terms of a "duty" of directors. The OCC has noted that the Guidelines are not intended to impose managerial responsibilities on the board, or that the board must guarantee results under the Framework to be established.

* * *

For more information about the Guidelines and how they may impact your organization, please contact any of the members of our Financial Institutions group listed below.

Lee Meyerson
(212) 455-3675
lmeyerson@stblaw.com

Mark Chorazak
(212) 455-7613
mchorazak@stblaw.com

Maripat Alpuche
(212) 455-3971
malpuche@stblaw.com

Elizabeth Cooper
(212) 455-3407
ecooper@stblaw.com

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
2 Houston Center
909 Fannin Street
Houston, TX 77010
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
1155 F Street, N.W.
Washington, D.C. 20004
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3919 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
West Tower, Mirae Asset Center 1
26 Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000