DEBEVOISE & PLIMPTON LLP | D&P

# CLIENT UPDATE

# OCC'S FINAL "HEIGHTENED EXPECTATIONS": AN OVERVIEW FOCUSING ON HOW THE OCC RESPONDED TO INDUSTRY COMMENTS


NEW YORK
Gregory J. Lyons
gjlyons@debevoise.com

Paul L. Lee
pllee@debevoise.com

Byungkwon Lim
blim@debevoise.com

Lee A. Schneider
lschneider@debevoise.com

David L. Portilla
dlportilla@debevoise.com

Samuel E. Proctor
seproctor@debevoise.com

Amelia J. Russell
ajrussel@debevoise.com

WASHINGTON, DC
Satish M. Kini
smkini@debevoise.com


## I. INTRODUCTION

On September 2, 2014, the Office of the Comptroller of the Currency ("OCC") issued final guidelines establishing heightened risk governance standards for OCC-regulated large financial institutions and their OCC-regulated affiliates ("Guidelines"). This update provides a broad overview of the scope, implementation timing, structure and requirements of the Guidelines, and highlights in chart form the way in which the OCC revised the proposed form of the Guidelines in response to industry concerns that were raised during the comment process.

As described below, the OCC responded to a number of industry comments by making revisions intended to make the Guidelines less prescriptive and to clarify that boards of directors are not responsible for "management" duties. However, the Guidelines also include a new, potentially burdensome, provision that require small (less than $50 billion in assets) banks that are under common control with a larger covered bank to be subject to the Guidelines on the same timeline as the larger, affiliated covered bank. The Final Guidelines also may be important for non-covered banking organizations as a guidepost for "best practices."

## II. SCOPE AND TIMING

The Guidelines apply to insured national banks, insured federal savings associations and insured federal branches of foreign banks (collectively, "banks") with $50 billion or more in average total consolidated assets ("covered bank"), or any such institution with less than $50 billion in assets if the institution's parent company controls at least one other covered bank. In justifying the broad scope of the Guidelines, the OCC stated that the $50 billion asset threshold is a well understood threshold that it and other regulatory agencies use to demarcate the larger, more complex banking institutions.[1] This statement, however, seems at odds with comments made by Federal Reserve Board Governor Daniel K. Tarullo, in which he questioned whether the $50 billion threshold for the application of certain "systemic risk" prudential regulations should be increased.

As detailed below, the Final Guidelines include a staggered implementation schedule based on the total consolidated assets of the bank.

- **$750 billion or more in assets**: 60 days after the Guidelines are published in the Federal Register (the "Effective Date").[2]
- **$100 billion to $750 billion in assets**: 6 months after the Effective Date.
- **$50 billion to $100 billion in assets**: 18 months after the Effective Date.
- ***New Category* – Less than $50 billion in assets (but controlled by a company that controls another covered bank)**: Same date as the other controlled covered bank.[3]

As indicated in the bullet immediately above, the proposed Guidelines did not apply to banks with less than $50 billion in assets. This new requirement, and application of the same effective date as applies to commonly controlled covered banks, could introduce substantial burdens for large banking organizations that have multiple national bank subsidiaries.

---

1 *Rethinking the Aims of Prudential Regulation*, The Federal Reserve Bank of Chicago Bank Structure Conference, May 8, 2014 *available at* http://www.federalreserve.gov/newsevents/speech/tarullo20140508a.htm.

2 As of the date of this memo, the Guidelines have not been published in the Federal Register. The asset sizes noted above are measured as of the Effective Date.

3 Guidelines I.6.B. In addition, a covered bank with less than $50 billion in average total consolidated assets on the Effective Date that subsequently becomes a covered bank is required to comply with the Guidelines within 18 months after the as-of date of the most recent Call Report used in the calculation of the average total consolidated assets.

## III. RISK GOVERNANCE FRAMEWORK AND LINES OF DEFENSE

### *Overview*

The core element of the Guidelines is the requirement for a formal, written risk governance framework approved by the board of directors or the risk committee of the board of directors.[4] Key required features of the risk governance framework include:

- **Annual reviewing and updating by independent risk management, or more frequently if needed to address improvements in risk management practices and changes in the covered bank's risk profile.**
- **Definitions of risk management roles and responsibilities for the "three lines of defense": (1) front line units, (2) independent risk management and (3) internal audit. Notably, as highlighted in the chart below, the roles and responsibilities for the three lines of defense were revised in a number of ways to make the Guidelines less prescriptive.**
- **A strategic plan that, at a minimum, covers a three-year period, is evaluated and approved by the board of directors.**
- **A comprehensive written risk appetite statement that serves as the basis for the risk governance framework and includes qualitative components and quantitative limits.**
- **Concentration risk limits and concentration risk management, as well as limits that apply to front line units.**
- **Risk appetite review, monitoring and communication processes.**
- **Processes governing risk limit breaches.**
- **Risk data aggregation and reporting policies, procedures and processes, including to support the reporting of material risks, concentrations and emerging risks to the board of directors and the OCC.**
- **Talent management processes, including processes for talent development, recruitment and succession planning.**
- **Compensation and performance management programs that are appropriate to ensure that the chief executive officer ("CEO") and three lines of defense implement and adhere to an effective risk governance framework.**

---

[4] Guidelines II.A.

### *Use of Parent Company's Risk Governance Framework*

A covered bank may use its parent company's risk governance framework in its entirety if the parent company's risk governance framework meets the Guideline's standards, and the risk profiles of the parent company and the covered bank are substantially the same, or the OCC otherwise approves the use of the covered bank's risk governance framework.[5] Under the Guidelines, the risk profiles of a covered bank and its parent company are substantially the same if the covered bank's average total consolidated assets represent 95% or more of the parent company's average total consolidated assets.[6]

In addition, a covered bank may incorporate or rely on components of its parent company's risk governance framework (after consulting with the OCC), to the extent those components are consistent with the objectives of the Guidelines.[7]

## IV. CONCLUSION

The Guidelines are the third significant risk management-focused rulemaking to be finalized this year, in addition to the Volcker Rule and the Federal Reserve's enhanced prudential standards (Regulation YY). Banking organizations that are subject to all three of these new standards, likely will find a number of ways in which the requirements overlap and are duplicative. We have prepared a summary chart that compares these three standards, and would be happy to provide a copy upon request. Further, the recently finalized liquidity coverage ratio, evolving capital and capital planning rules, and the liquidity standards of Regulation YY likely will be an important consideration for these various risk management requirements.

* * *

Please do not hesitate to contact us with any questions.

September 12, 2014

---

5 "Parent company" is defined as the top-tier legal entity in a covered bank's ownership structure. Thus, for a national bank that is a subsidiary of a foreign banking organization, it appears that the parent company would be the top-tier foreign holding company. Guidelines I.E.9.

6 Guidelines I.3-4.

7 Guidelines I.6.

## CHANGES FROM PROPOSED GUIDELINES

This summary chart sets out significant comments that the industry made regarding the OCC's proposed form of the Guidelines, and how the final Guidelines were revised, if at all, in response to these comments.

| Issue | Industry Comment | Industry Proposal | Final Guidelines |
|---|---|---|---|
| ***Use of parent risk governance framework*** | The proposal required that, in order for a covered bank to use the risk governance framework of its parent, the covered bank's average total consolidated assets would need to represent 95% or more of the parent company's average total consolidated assets.<br><br>Commenters argued that the proposal would rigidly compartmentalize the covered bank apart from its parent company's risk framework which could result in inconsistencies and inefficiencies. | The covered bank should be given more flexibility to draw upon certain aspects of its parent's risk governance framework. | The 95% asset standard remains unchanged.<br><br>However, the OCC eased some of the duplication for some banks to be able to use the expertise of the parent company, such as sharing a chief audit officer, under certain circumstances.<br><br>[Preamble p. 13; Guidelines I.4] |

| Issue | Industry Comment | Industry Proposal | Final Guidelines |
|---|---|---|---|
| ***Centralized internal audit function*** | The proposal seemed to require a banking organization to establish duplicative audit departments for its parent company and each of its banks. | The final Guidelines should allow a centralized audit function, as it is more effective and efficient, ensures consistent audit coverage, and enables enterprise-wide functional reviews that help to identify systemic issues quickly. | The final Guidelines generally provide that a covered bank may rely on components of its parent company's risk governance framework, including internal audit, to the extent those components are consistent with the objectives of the final Guidelines.<br>[Preamble p. 34; Guidelines I.6] |

| Issue | Industry Comment | Industry Proposal | Final Guidelines |
|---|---|---|---|
| ***Definition of front line unit*** | The proposal's definition of "front line unit" was overly broad and a departure from well-established principles regarding the three "lines of defense," which could unintentionally reduce the effectiveness of bank's risk programs.<br><br>Commenters were concerned that certain units that do not create risk, such as legal, compliance, finance, human resources or information technology, would be included and subject to the requirements of the front line units. | The final Guidelines should incorporate more flexibility for the covered bank to determine how service and support functions fit into the bank's risk governance framework. | The final Guidelines clarify that the front line would include anyone (1) involved in generating revenue (or reducing expenses) for the bank, (2) providing operational support or servicing to an organizational unit or function for the delivery of products or services to customers, or (3) providing technology services to any of the units or functions covered in (1) and (2).<br><br>The final Guidelines also specifically carve out legal services from the definition of front line unit.<br><br>[Preamble pp. 25-26; Guidelines I.E.6] |

| Issue | Industry Comment | Industry Proposal | Final Guidelines |
|---|---|---|---|
| ***Independent risk management and CEO*** | Under the proposal, independent risk management should oversee the bank's risk-taking activities and assess risks and issues independent of the CEO, with the Chief Risk Executive ("CRE") reporting to the CEO. | The final Guidelines should clarify that although the CRE is responsible for overseeing the bank's risk-taking activities, the CRE is still subject to CEO oversight. | The final Guidelines removed the provision that independent risk management acts independently of the CEO. The OCC clarified that it did not intend to suggest that independent risk management should not be subject to CEO oversight with respect to the assessment of risks and issues.<br>[Preamble p. 46; Guidelines II.C.2] |
| ***Chief Audit Executive reporting*** | The reporting line requirements of the Chief Audit Executive ("CAE") were too narrow. The proposal provided for the CAE to report only to the Audit Committee or the CEO, rather than any other senior executive (*e.g.*, the general counsel) for day-to-day matters. | The final Guidelines should permit alternative senior management reporting on day-to-day issues. | Final Guidelines clarify that the CEO or the audit committee oversees the CAE's administrative activities (*e.g.*, routine personnel matters), rather than the CAE's day-to-day activities.<br>[Preamble pp. 35-36; Guidelines I.E.8] |

| Issue | Industry Comment | Industry Proposal | Final Guidelines |
| --- | --- | --- | --- |
| ***Materiality threshold for internal audit reporting*** | The proposal required that internal audit report to the audit committee in writing all conclusions and issues from audit work carried out including the identification of the root cause of any issue. | The final Guidelines should require only material issues to be reported. | The final Guidelines clarify that only material issues and the root causes of such material issues need to be reported.<br>[Preamble p. 51; Guidelines II.C.3.(c)] |
| ***CEO: strategic plan*** | The proposal included language that the CEO develop a strategic plan. Commenters argued that this placed too onerous of a burden on the CEO. | The final Guidelines should require the CEO to be responsible for the development of the strategic plan, rather than actually develop such plan. | The final Guidelines clarify that the CEO is responsible for the development of a strategic plan, indicating that the CEO is not responsible for writing the plan.<br>[Preamble p. 57; Guidelines II.D] |

| Issue | Industry Comment | Industry Proposal | Final Guidelines |
| --- | --- | --- | --- |
| ***Board of directors: obligation to challenge management*** | The proposal mandated that boards of directors must "question, challenge, and, when necessary oppose" management on certain actions related to risk. Commenters argued that such language could create an unnecessary rift between management and the board of directors, and inhibit an open dialogue. | The final Guidelines should place less emphasis on opposition to management and provide more clarity that the OCC will look to how credible challenge by the board of directors is exercised in practice. | The OCC kept such language in the final Guidelines, emphasizing that by challenging management, members of the board of directors will have more information about the risk-taking activities of the bank and whether management is adhering to the risk governance framework.<br>[Preamble p. 74; Guidelines III.B] |

| Issue | Industry Comment | Industry Proposal | Final Guidelines |
|---|---|---|---|
| ***Board of directors: management functions*** | The proposal required the board of directors to oversee the talent development, recruitment, and succession planning processes for independent risk management, internal audit and individuals two levels down from the CEO. Commenters asserted that these provisions would impose administrative burdens on a bank's board of directors and inappropriately place operational management responsibilities on the board of directors. | This requirement should be removed in the final Guidelines. | The OCC clarified that it did not intend to impose managerial responsibilities on the board of directors. The final Guidelines provide that a covered bank's board of directors or an appropriate committee of the board of directors should appoint a CEO and appoint or approve the appointment of a CAE and one or more CREs with the skills and abilities to carry out their roles and responsibilities within the risk governance framework. This provision clarifies that the board of directors need not be involved in the hiring process for these individuals. |

| Issue | Industry Comment | Industry Proposal | Final Guidelines |
| --- | --- | --- | --- |
| | | | The final Guidelines also provide that the board of directors or an appropriate committee of the board of directors should review and approve a written talent management program that provides for development, recruitment, and succession planning regarding only the CEO, CAE, CRE(s), their direct reports, and other potential successors.<br><br>The requirement to oversee the talent development, recruitment and succession planning processes for individuals two levels down from the CEO was removed.<br><br>[Preamble pp. 66-67; Guidelines II.L] |

| Issue | Industry Comment | Industry Proposal | Final Guidelines |
|---|---|---|---|
| ***Board of directors: ensuring management action*** | The proposal stated that the board of directors has a duty to "ensure that the bank establishes and implements an effective" risk governance framework. Commenters argued that the expansive use of the word "ensure" seemingly requires bank directors to "guarantee" outcomes that would impact the ability of banks to attract qualified board of director candidates and creates a new fiduciary duty. | The final Guidelines should more precisely describe the action the OCC expects bank directors to take. | The OCC clarified that it did not intend to suggest that the board of directors must guarantee results under the risk governance framework. The final Guidelines provide that the board of directors should require management to establish and implement an effective risk governance framework that meets the minimum standards described in the final Guidelines.<br>[Preamble p. 72; Guidelines III.A] |

| Issue | Industry Comment | Industry Proposal | Final Guidelines |
|---|---|---|---|
| ***Independent directors*** | The proposal required that the bank have at least two independent directors. Some commenters argued that the bank should retain its flexibility in board of directors composition or that the definition of independence should be clarified. | The final Guidelines should conform the definition of independence to be consistent with the Federal Reserve Board's enhanced prudential standards (Regulation YY). | The final Guidelines continue to require that at least two directors be independent, but the OCC incorporated the definition of "independence" from Federal Reserve Board's enhanced prudential standards (Regulation YY).<br>[Guidelines III.D] |